Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Organo direzione informatica della Confederazione ODIC
Servizio delle attività informative della Confederazione SIC

Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI
https://www.melani.admin.ch/

SICUREZZA DELLE INFORMAZIONI

LA SITUAZIONE IN SVIZZERA E A LIVELLO INTERNAZIONALE

Rapporto semestrale 2019/1 (gennaio–giugno)

29 OTTOBRE 2019

CENTRALE D'ANNUNCIO E D'ANALISI PER LA SICUREZZA DELL'INFORMAZIONE MELANI
https://www.melani.admin.ch/

1 Indice

2 Editoriale

Il ransomware è una minaccia anche per le amministrazioni

Martin Müller è responsabile della sicurezza della tecnologia dell'informazione e della comunicazione dell'amministrazione comunale di Berna nonché membro di vari gruppi di lavoro nazionali sul tema della sicurezza TIC e Swiss Certified ICT Leader.

Ransomware, trojan di crittografia o trojan a scopo di estorsione, non è importante come li si chiama, questo tipo di software nocivi che, dopo essersi annidati nel dispositivo, fanno comparire una richiesta di riscatto, sono balzati all'onore della cronaca con la diffusione di WannaCry. Le cifre richieste per poter decifrare i file colpiti variano da poche centinaia fino a svariate centinaia di migliaia di dollari statunitensi, da versare in bitcoin. Tuttavia non vi è mai la garanzia di poter ripristinare effettivamente i propri dati.

Anche l'amministrazione comunale di Berna ha subito simili attacchi nel 2017 e nel 2019. Gli aggressori non hanno colpito miratamente l'amministrazione comunale, bensì hanno operato su vasta scala con lo scopo di ottenere quanto più denaro possibile. Il fatto che oggi attacchi di questo tipo possono essere sferrati senza disporre di particolari conoscenze o mezzi è fonte di grande preoccupazione per i responsabili della sicurezza. Difatti, il cosiddetto modello Ransomware-as-a-Service (RaaS) è offerto nel Darknet da vari fornitori a cifre modeste. Questo tipo di attacco, dunque, non è più appannaggio esclusivo dei professionisti della cibercriminalità, bensì è accessibile a tutti, dagli script kiddie in cerca di visibilità agli hacktivisti mossi da motivazioni politiche.

Oltre a dotarsi di tutte le possibili misure tecniche di sicurezza come firewall, sistemi per il riconoscimento e la prevenzione degli attacchi, antivirus, soluzioni per la sicurezza delle e-mail nonché aggiornare costantemente software e hardware, è molto importante generare regolarmente copie dei propri dati (backup), che vanno conservate fisicamente o logicamente separate dal resto della rete aziendale. In tal modo, in caso di attacco è possibile ripristinare rapidamente l'esercizio e minimizzare la perdita dei dati. La gestione dei backup dell'amministrazione comunale si è dimostrata molto efficace per contrastare gli attacchi.

Nonostante tutti i mezzi tecnici oggi a nostra disposizione nell'universo TIC, tutto ruota ancora necessariamente intorno all'individuo. Per questo riteniamo che la formazione e la sensibilizzazione dei collaboratori rappresentino la misura più importante nonché il fondamento della sicurezza nel settore TIC. Di pari passo con la trasformazione digitale dell'amministrazione, occorre gettare le basi affinché i collaboratori siano in grado di utilizzare i nuovi mezzi in modo sicuro, responsabile e con fiducia. Anche una buona dose di diffidenza e buon senso contribuisce alla sicurezza. Per questo l'amministrazione comunale di Berna, nell'ambito della propria Strategia digitale 2021 e della campagna per la sicurezza TIC 2019–2020, ha posto volutamente al centro le capacità digitali delle persone e consigliamo anche a voi di fare altrettanto.

Martin Müller

3 Tema principale: ransomware

Il ransomware (malware con scopo estorsivo, trojan di crittografia) è uno strumento di attacco consolidato nel cosmo della criminalità informatica. I trojan di crittografia mirano a rendere indisponibili i dati delle vittime, con l'obiettivo di ricattarle. Ma un altro scopo, sebbene in misura minore, può essere quello di danneggiare un'azienda. Nel corso degli anni i trojan di crittografia si sono evoluti sul piano tecnico e tattico, diventando una delle minacce più pericolose per le aziende. Nel primo semestre del 2019 si è osservato in tutto il mondo un aumento degli attacchi contro le organizzazioni e delle richieste di riscatto.

3.1 Sviluppo storico

Già otto anni fa, MELANI aveva descritto la comparsa di un software maligno in grado di bloccare i computer a scopo estorsivo.[1] All'epoca si trattava di una delle prime versioni di ransomware in grado di bloccare gli schermi e di far comparire una comunicazione, proveniente apparentemente dalla polizia federale, nella quale veniva intimato il pagamento di una pena pecuniaria a causa della presenza di presunto materiale illegale sul dispositivo colpito. Questo tipo di malware era relativamente innocuo e nella maggior parte dei casi poteva essere rimosso attraverso una semplice analisi del computer con un live-CD antivirus.

Due anni più tardi Cryptolocker è stato il primo software nocivo con funzioni di crittografia a conquistare i titoli di giornale.[2] Esso era in grado di cifrare i dati presenti sia sul disco rigido sia sui supporti dati collegati. Per ogni vittima veniva creata una chiave di codifica specifica su un server C2, rendendo così il ripristino dei dati più difficile rispetto ad altri trojan di crittografia dotati di una chiave programmata in maniera fissa e quindi estraibile. Cryptolocker si diffondeva tramite allegati e-mail infetti (malspam) e infezioni drive-by (siti web manipolati) o veniva scaricato mediante un dropper (file di programma eseguibile autonomamente) già installato sul dispositivo. La propagazione mediante dropper è attualmente molto diffusa.

Nel 2014 fu propagato il trojan di crittografia Synolocker che sfruttava una falla nella sicurezza dei dispositivi NAS dell'azienda Synology.[3] La lacuna utilizzata era nota e pochi mesi prima era stato pubblicato un update per la sicurezza. Questo caso mostrò la necessità di aggiornare con regolarità i programmi e i sistemi operativi non solo dei computer, ma anche di router, dispositivi NAS e componenti simili. Nel 2014 i programmatori di ransomware iniziarono a elaborare misure per ostacolare il riconoscimento e l'analisi dei server C2. Ad esempio il trojan di crittografia CTB-Locker, che veniva diffuso tramite i siti web hackerati della stampa online, comunicava in modo cifrato con i propri server C2 e utilizzava il servizio di anonimizzazione Tor per cancellare le proprie tracce, ostacolando così il riconoscimento e l'analisi da parte degli attori della sicurezza.

---

1 MELANI rapporto semestrale 2011/2, cap. 3.5.
2 MELANI rapporto semestrale 2013/2, cap. 3.1.
3 MELANI rapporto semestrale 2014/2, cap. 3.6.

I criminali, alla costante ricerca di nuovi bersagli, hanno cominciato a prendere di mira le banche dati di siti web scarsamente protetti, crittografandole per poi chiedere un riscatto agli amministratori.[4] Nel 2015 le famiglie di ransomware più attive sono state Teslacrypt e Cryptowall.[5]

Nel 2016 si è assistito a un vero e proprio boom del fenomeno ransomware.[6] Per la prima volta sono state colpite infrastrutture critiche di interesse pubblico, in particolare alcuni ospedali in Germania e negli Stati Uniti. Il settore sanitario, oltre a dover mantenere aggiornati i sistemi TIC e la tecnologia medica e a installare gli update di sicurezza, deve anche essere in grado di reagire agli attacchi più rapidamente delle altre vittime, perché un'infrastruttura TIC non funzionante può mettere in pericolo vite umane. Perciò la pressione verso il pagamento del riscatto è relativamente alta, nella speranza di ripristinare quanto prima l'operatività. Tuttavia, cedere alle richieste dei ricattatori non è necessariamente una soluzione efficace, come dimostra l'esempio del Kansas Heart Hospital che ha ricevuto dai ricattatori la chiave per decifrare soltanto una parte dei dati e si è visto costretto a pagare un secondo riscatto per ottenere la decodifica dei dati restanti.[7]

Locky, diffuso anche in Svizzera dal febbraio 2016, ha rappresentato un'evoluzione tecnica del ransomware.[8] Questo malware crittografa i file salvati sui dispositivi di rete collegati (drive su cloud, condivisioni di risorse in rete ecc.). La crescita esponenziale del fenomeno ha spinto le autorità di sicurezza a rafforzare le misure preventive. MELANI, in collaborazione con vari uffici federali, associazioni e organizzazioni svizzere così come produttori di software, ha organizzato una giornata di sensibilizzazione sul tema del ransomware.[9] L'Ufficio federale per la sicurezza informatica della Germania (BSI) ha pubblicato un dossier per fare il punto sul tema ransomware.[10]

Nel primo semestre del 2017 due attacchi ransomware internazionali hanno mostrato chiaramente il potenziale di rischio di simili attacchi: WannaCry ha colpito almeno 200 000 computer in 150 Paesi. Le vittime più rilevanti sono state l'azienda spagnola di telecomunicazioni Telefonica, alcuni ospedali in Gran Bretagna e la società ferroviaria tedesca Deutsche Bahn. Anche in Svizzera sono state rilevate alcune centinaia di infezioni, ma nessuna riguardante un'infrastruttura critica. Poco dopo il malware NotPetya ha causato gravi danni, innanzitutto in Ucraina dove ha colpito l'aeroporto di Kiev, la banca centrale ucraina e la stazione di misurazione della radioattività di Chernobyl. Il ransomware si è poi propagato a livello globale attraverso le filiali ucraine di aziende multinazionali. Vittime di rilievo sono state la danese Maersk (il più grande armatore di navi mercantili al mondo) e il gigante farmaceutico USA Merck. NotPetya ha colpito anche in Svizzera, ad esempio la società pubblicitaria Admeira.[11] L'elemento comune degli

---

4 MELANI rapporto semestrale 2014/2, cap. 5.3.

5 MELANI rapporto semestrale 2015/1, cap. 4.6.1.5 e 2015/2, cap. 4.5.1.

6 MELANI rapporto semestrale 2016/1, cap. 5.4.3.

7 https://www.csoonline.com/article/3073495/kansas-heart-hospital-hit-with-ransomware-paid-but-attackers-demanded-2nd-ransom.html

8 MELANI rapporto semestrale 2016/1, cap. 4.6.3.

9 https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/ransomwareday.html; https://www.switch.ch/news/ransomware-day/; https://www.ebas.ch/it/securitynews/509-giornata-nazionale-di-sensibilizzazione-contro-il-ransomware

10 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Lagedossier_Ransomware.pdf

11 MELANI rapporto semestrale 2017/1, cap. 3.

attacchi WannaCry e NotPetya è il modo di propagazione: in entrambi i casi il malware si è diffuso come un verme informatico, quindi in modo autonomo, sfruttando una lacuna nel protocollo SMB delle reti. Ma se per WannaCry la propagazione appariva casuale, il bersaglio principale di NotPetya erano probabilmente le aziende ucraine. In entrambi i casi gli esperti di sicurezza dubitano dell'esistenza di una motivazione puramente criminale. Sebbene non siano stati accertati né gli aggressori né le loro motivazioni, si ritiene che in entrambi i casi il principale obiettivo fosse il sabotaggio e la diffusione del panico.

Nella seconda metà del 2017 il ransomware BadRabbit è stato autore di attacchi geolocalizzati, principalmente in Russia, ma anche in Ucraina, Germania e Turchia. BadRabbit si è diffuso mediante falsi aggiornamenti di Adobe Flash e utilizzando l'exploit EternalRomance per infiltrarsi nei sistemi delle aziende colpite e ottenere i dati di accesso da diffondere, come era accaduto con Mimikatz.[12]

Finché non vengono ripristinati, i sistemi colpiti da ransomware possono implicare perdite di produttività, come è capitato nel 2018 al produttore taiwanese di microchip TSMC (Taiwan Semiconductor Manufacturing Company): una variante di WannaCry ha costretto l'azienda ad arrestare la produzione in svariati impianti.[13]

Fino al 2018 la maggior parte degli attacchi di ransomware non erano mirati. Unicamente il gruppo SamSam era noto per attacchi con trojan di crittografia sferrati principalmente contro le organizzazioni USA. Nel 2018 è comparso un altro ransomware utilizzato apparentemente per estorcere denaro a specifiche organizzazioni, si tratta di Ryuk, già tematizzato nell'ultimo rapporto semestrale[14] ed ancora molto attivo nel 2019 (cfr. cap. 3.4.1). Ci sono inoltre ransomware impiegati in modo sia mirato sia opportunistico, come ad esempio GandCrab e Dharma.[15]

3.2 I casi più recenti

Il numero degli attacchi ransomware mirati è aumentato nel primo semestre del 2019. Ai già citati Ryuk, GandCrab e Dharma si sono aggiunti LockerGoga, MegaCortex e RobbinHood. Quest'ultimo ha paralizzato a fine maggio l'amministrazione comunale di Baltimora.[16] Gli attacchi con ransomware sono tra le minacce cibernetiche più pericolose per le aziende, le organizzazioni e le amministrazioni. Un attacco riuscito, oltre a richiedere l'impiego di tempo, personale e denaro per la pulizia dei sistemi e il ripristino dei dati perduti, può anche danneggiare la reputazione di un'azienda o causare perdite di produttività per un certo periodo di tempo.[17] Come è accaduto al produttore di alluminio Norsk Hydro, costretto da un attacco ransomware a proseguire in modalità manuale la produzione, fondamentalmente automatizzata,[18] o ai poliziotti di Jackson County, nello stato federato USA della Georgia, che hanno dovuto scrivere a mano i loro rapporti perché i sistemi dell'amministrazione comunale erano

12 MELANI rapporto semestrale 2017/2, cap. 5.4.2.
13 MELANI rapporto semestrale 2018/2, cap. 5.3.5.
14 MELANI rapporto semestrale 2018/2, cap. 4.5.4.
15 https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat
16 https://www.tripwire.com/state-of-security/featured/ransomware-baltimore-network/
17 https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat
18 https://www.bleepingcomputer.com/news/security/lockergoga-ransomware-sends-norsk-hydro-into-manual-mode/

stati paralizzati da Ryuk.[19] In Svizzera Offix Holding SA, vittima di Ryuk (cfr. anche cap. 3.4.1), ha potuto evitare il peggio riuscendo a allestire in poche ore un funzionamento di emergenza che le ha permesso di avvertire i clienti e di proseguire la propria attività finché non sono stati risolti i problemi informatici. L'azienda non ha ceduto alla richiesta di versare un riscatto di 45 bitcoin (c. fr. 330'000).[20]

Nel periodo oggetto del rapporto ci sono stati anche casi di impiego contemporaneo di due tipologie di minacce informatiche: il ransomware e il phishing. Il trojan di crittografia utilizzato in questi casi non si limita a codificare i file ma cerca anche di sottrarre dati sensibili alle vittime, a cui viene chiesto se preferiscano pagare il riscatto in bitcoin o tramite PayPal. Scegliendo questa opzione, vengono indirizzate su una pagina di phishing in cui devono inserire i dati della carta di credito e dell'accesso all'account di PayPal oltre ad altri dati personali.[21]

Temendo che i loro piani possano essere vanificati dai backup, gli aggressori hanno cambiato approccio. Difatti ora si procurano prima i dati di accesso e le password necessari per poter eliminare o crittografare anche i backup e poi bloccano i sistemi operativi.

Non sorprende dunque che le aziende senza backup o i cui backup sono resi inutilizzabili, e che quindi si trovano in una situazione che mette a rischio la loro esistenza, cedano all'estorsione. Già nel 2014 MELANI ha affermato che il ransomware avrà successo fintanto che le vittime sono propense a pagare il riscatto.[22] Nei primi sei mesi del 2019 hanno fatto notizia i casi di due città della Florida, Riviera City e Lake City, disposte a pagare rispettivamente le cifre esorbitanti di 65 bitcoin (c. 600 000 $ US) e 42 bitcoin (c. 500 000 $ US). Nel caso di Lake City il pagamento del riscatto è stato negoziato direttamente con la società che assicura la città.[23] Questa tendenza potrebbe affermarsi anche in Svizzera.[24] Ma nel lungo termine, il pagamento dei riscatti si dimostrerà essere un «cattivo investimento», perché tanto più le imprese saranno disposte a pagare quanto più i cibercriminali saranno incentivati a sferrare questo tipo di attacchi.[25]

3.3 Ransomware-as-a-Service

Con l'affermarsi, nell'ambiente della cibercriminalità, della ripartizione del lavoro e della tendenza a specializzarsi, anche il mercato clandestino si evolve. Già da molto tempo nel Darknet si trovano ciberattacchi preconfigurati.[26] Questa offerta è definita «Cybercrime-as-a-Service» (CaaS) o, nel caso del ransomware, RaaS. Così anche senza particolari conoscenze informatiche è possibile lanciare un attacco digitale.[27] Questo tipo di servizio offre a un determinato

19 https://statescoop.com/georgia-county-paid-400k-to-ransomware-hackers/

20 https://www.inside-it.ch/articles/54898

21 https://www.bleepingcomputer.com/news/security/new-ransomware-bundles-paypal-phishing-into-its-ransom-note/

22 MELANI rapporto semestrale 2014/2, cap. 5.3.

23 https://www.zdnet.com/article/second-florida-city-pays-giant-ransom-to-ransomware-gang-in-a-week/

24 https://www.nzz.ch/wirtschaft/ransomware-warum-zahlreiche-firmen-loesegeld-zahlen-duerften-ld.1489507

25 https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat

26 Cfr. MELANI rapporto semestrale 2009/2, cap. 4.7: «A livello di criminalità informatica l'anno scorso è stato sviluppato il modello commerciale Crimeware-as-a-Service (CaaS). Nel caso di questo modello i criminali informatici che non hanno dimestichezza con le questioni tecniche possono "affittare" un servizio corrispondente.»

27 Maggiori dettagli in MELANI rapporto semestrale 2016/2, cap. 6.1.

prezzo gli elementi necessari per un attacco: le istruzioni per generare il malware, il management panel (dashboard) che fornisce tutte le informazioni necessarie sulle infezioni andate a buon fine, la chiave di decifratura ed eventualmente un tutorial per l'uso degli strumenti messi a disposizione. Grazie a questo pacchetto di base, il «cliente» è in grado di adeguare il ransomware e l'attacco alle proprie esigenze.[28]

3.4 Ransomware oggi particolarmente attivi

3.4.1 Ryuk

Il ransomware Ryuk è attivo dalla seconda metà del 2018 ed è già stato trattato nell'ultimo rapporto semestrale.[29] Con Ryuk a dicembre è stata attaccata la tipografia Tribune Publishing di Los Angeles. Gli aggressori hanno crittografato il server che supportava la piattaforma di produzione per la stampa e la distribuzione di vari quotidiani statunitensi. Il guasto ha ritardato o in parte impedito la pubblicazione delle edizioni del sabato del Los Angeles Times e della San Diego Union Tribune così come delle edizioni dello Wall Street Journal e del New York Times destinate alla costa occidentale.[30]

Ryuk viene utilizzato per lanciare attacchi mirati contro computer e server delle reti aziendali. La crittografia dei dati è spesso la fase finale di un attacco sferrato su tre livelli, che ha inizio con l'infezione con il trojan Emotet. Generalmente Emotet è diffuso mediante e-mail contenenti un link o un allegato infetti (malspam). Cliccando ingenuamente sul link o sull'allegato, Emotet si installa nel computer e invia e-mail ai contatti presenti in rubrica per propagarsi ulteriormente. Emotet può fungere da dropper per altri software nocivi. In alcuni casi, ad esempio, viene scaricato Trickbot (cfr. cap. 4.6) che esegue un'analisi della rete colpita per scoprire se appartiene a un privato o a un'azienda. In quest'ultimo caso cerca di diffondersi nella rete sfruttando la lacuna di sicurezza nei protocolli SMB. In tal modo sono raccolte ulteriori informazioni sulla potenziale vittima. Per lo più Ryuk viene scaricato solo se la vittima è ritenuta sufficientemente appetibile.[31]

Nell'anno in corso sono stati condotti attacchi mirati con Ryuk per estorcere somme esorbitanti. Tra le vittime si annoverano le amministrazioni di alcune città negli Stati Uniti, che hanno pagato tra i 130 000 e i 600 000 dollari di riscatto.[32]

In Svizzera sono stati segnalati casi nel settore delle costruzioni, nel traporto pubblico e nell'industria. Ad esempio a metà maggio Offix Holding SA, azienda che fornisce articoli da ufficio e cancelleria, è stata pesantemente colpita «da un massiccio attacco hacker mirato, pianificato e accuratamente orchestrato»[33].[34] Il varco di entrata è stato un documento di Word, inviato per e-mail, che ha installato il malware Emotet mediante una macro. Successivamente sono stati scaricati Trickbot e Ryuk. Due giorni dopo gran parte dei sistemi dell'azienda hanno smesso

---

28 https://securityaffairs.co/wordpress/84273/breaking-news/inpivx-ransomware-service.html

29 MELANI rapporto semestrale 2018/2, cap. 4.5.4

30 https://www.heise.de/newsticker/meldung/Cyber-Attacke-verzoegert-Druck-grosser-Tageszeitungen-in-den-USA-4260103.html

31 MELANI rapporto semestrale 2018/2, cap. 4.5.4

32 https://www.bleepingcomputer.com/news/security/la-porte-county-pays-130-000-ransom-to-ryuk-ransomware/

33 Comunicazione alla clientela di Offix Holding SA riportata da Inside-IT: https://www.inside-it.ch/articles/54898

34 https://www.nzz.ch/wirtschaft/cyber-angriff-auf-schweizer-firma-offix-ein-kampf-ums-ueberleben-ld.1492862

di funzionare: registrazione degli orari di lavoro, contabilità salariale, banche dati delle immagini, server telefonico, server Citrix, server Exchange e altri.[35] Sono stati risparmiati soltanto i webshop ospitati sui server Linux e il sistema di gestione merci.

3.4.2 LockerGoga e MegaCortex

LockerGoga è comparso per la prima volta nel mese di gennaio 2019 quando ha colpito l'azienda multinazionale francese di consulenza ingegneristica e industriale Altran Technologies.[36] LockerGoga è viene principalmente utilizzato in attacchi a due fasi, in cui viene scaricato, su un dispositivo precedentemente infettato, da uno strumento chiamato PsExec. I criminali informatici utilizzano tool di hacking disponibili in rete per ottenere l'accesso al sistema e i diritti di amministratore con cui poter disattivare il software di sicurezza e i backup prima di installare il ransomware. Questa tecnica, abbinata all'utilizzo di certificati legittimi, permette di aggirare le misure di protezione adottate.[37] Dopo essere stato installato, LockerGoga modifica i dati di accesso al sistema e tenta di chiudere la sessione dell'utente collegato con questi dati. LockerGoga cerca di criptare contemporaneamente quanti più dispositivi possibili. Tuttavia, per ogni file da criptare il ransomware genera un proprio processo; si tratta di un aspetto piuttosto insolito che rallenta notevolmente la cifratura.[38]

A marzo sono state almeno tre le vittime prestigiose di LockerGoga: Hexion e Momentive, due aziende statunitensi che possiedono il fondo d'investimento Apollo Global Management e che producono resine, siliconi e altri materiali,[39] e il produttore norvegese di alluminio Norsk Hydro. In quest'ultimo caso, prima è stata infettata una filiale statunitense dell'azienda, da cui il malware si è propagato «lateralmente» attraverso la rete (lateral movement) annidandosi in quasi tutte le postazioni di lavoro. In alcuni casi è stato necessario avviare l'esercizio manuale poiché il sistema di produzione non era più funzionante. Apparentemente i cibercriminali hanno modificato le password degli account Active Directory. Probabilmente mediante Mimikatz o un tool simile hanno ottenuto i cosiddetti Kerberos ticket con cui hanno ingannato il sistema spacciandosi per utenti abilitati.[40]

MegaCortex opera in modo simile a LockerGoga. Questo ransomware attacca in modo mirato aziende e organizzazioni. Stando a diverse fonti, in sole 48 ore sono state infettate con MegaCortex quasi 50 aziende negli Stati Uniti, in Europa e in Canada.[41] Secondo i ricercatori di Sophos non vi sono similitudini di codici tra MegaCortex e LockerGoga, tuttavia in entrambi i casi viene utilizzato un domain controller compromesso per inviare il malware ai dispositivi collegati alla rete bersaglio. Sono eseguiti comandi PowerShell per contattare i server C2 controllati in modo fraudolento e per avviare la cifratura. Almeno uno dei server C2 è stato utilizzato sia per MegaCortex sia per LockerGoga, spiegano i ricercatori.[42] Come per Ryuk, anche

---

35 https://www.inside-it.ch/articles/54898

36 https://ml.globenewswire.com/Resource/Download/0663f8d4-0acf-4463-b0fd-bb05042d1373, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware

37 https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat

38 https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware

39 https://www.chemistryworld.com/news/hexion-momentive-and-norsk-hydro-all-hit-by-ransomware-cyber-attacks/3010328.article

40 https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware

41 https://www.darkreading.com/perimeter/lockergoga-megacortex-ransomware-share-unlikely-traits/d/d-id/1334696

42 https://news.sophos.com/en-us/2019/05/10/megacortex-deconstructed-mysteries-mount-as-analysis-continues/

la presenza di MegaCortex è stata spesso rilevata presso le aziende già infettate con Emotet e Qbot.[43] Attività perpetrate con questi trojan di crittografia sono state segnalate anche in Svizzera.

3.4.3 GandCrab

Nel secondo semestre del 2018 GandCrab ha monopolizzato il 50 per cento del mercato dei ransomware a livello globale. Ciò è possibile in quanto i suoi sviluppatori operano secondo il modello ransomware-as-a-service. È cioè possibile acquistare GandCrab su forum specifici nel Dark Web pagando il 40 per cento dei profitti ricavati dagli attacchi sferrati con questo strumento.[44] Questo spiega anche la molteplicità di vettori utilizzati per la diffusione del malware: diverse varianti di e-mail di massa (malspam), dossier di candidatura manomessi e siti web con infezioni drive-by, sia appositamente registrati dai criminali sia legittimi ma hackerati.[45]

Dalla sua comparsa nel gennaio 2018, GandCrab ha conosciuto varie versioni e rielaborazioni del codice che rendono gli attacchi sempre più efficaci e difficili da contrastare. Anche gli autori di malware puntano sulla ridondanza: in alcuni attacchi lanciati nel corso di quest'anno si è osservato l'impiego di GandCrab abbinato a BetaBot o AzorUlt. BetaBot dispone di funzioni che disattivano i programmi antivirus e i firewall per non essere riconosciuti. Successivamente BetaBot analizza il dispositivo della vittima e raccoglie informazioni come i dati di accesso e di login al servizio e-banking. Nel frattempo, il secondo malware (ad es. GandCrab) garantisce la ridondanza dell'infezione del sistema colpito, anche in caso di crash del sistema.[46]

Il provider di servizi cloud Meta10, con sede a Zugo, il 22 febbraio 2019 ha subito un attacco con il ransomware GandCrab v5.2 che ha colpito alcuni server di banche dati, di applicazioni e di backup.[47] La pulizia dei sistemi e il ripristino della documentazione hanno causato sensibili perdite di efficienza per circa il dieci per cento dei clienti dell'azienda. L'azienda ha deciso subito di attuare una comunicazione proattiva informando i propri clienti su quanto avvenuto e dando loro la possibilità di restare costantemente aggiornati consultando la pagina dedicata allo stato del servizio. Anche l'amministrazione comunale di Berna ha subito nel 2019 un attacco GandCrab da cui tuttavia si è ripresa velocemente grazie alla sua esemplare gestione dei backup.[48]

A fine maggio 2019 i gestori di GandCrab hanno reso noto di aver estorto con il loro ransomware 2 miliardi di dollari e di volersi ritirare dall'attività. Hanno richiesto ai loro partner di arrestare la diffusione di GandCrab entro 20 giorni esortando le vittime a pagare il riscatto quanto prima, onde evitare di perdere i loro dati per sempre.[49]

---

43 https://www.darkreading.com/perimeter/lockergoga-megacortex-ransomware-share-unlikely-traits/d/d-id/1334696

44 https://www.europol.europa.eu/newsroom/news/just-released-fourth-decryption-tool-neutralises-latest-version-of-gandcrab-ransomware

45 MELANI rapporto semestrale 2018/2, cap. 4.5.4.

46 https://www.scmagazineuk.com/gandcrab-returns-trojans-redundency/article/1523389

47 https://www.computerworld.ch/security/hacking/cyberangriff-legt-zuger-cloud-provider-meta10-lahm-1684975.html

48 Si veda in merito l'editoriale del responsabile della sicurezza della tecnologia dell'informazione e della comunicazione dell'amministrazione comunale di Berna nel precedente capitolo 2.

49 https://securityaffairs.co/wordpress/86438/malware/gandcrab-shutdown-operations.html

Da metà giugno 2019, su https://www.nomoreransom.org/ è disponibile un tool in grado di decifrare le versioni attualmente in circolazione (1, 4 e 5–5.2) del ransomware GandCrab. Il programma, sviluppato in collaborazione con le autorità di perseguimento penale di vari Paesi e con il supporto dell'azienda Bitdefender, premette alle vittime di ripristinare i loro dati crittografati.[50] Una settimana prima del rilascio di questo strumento un padre siriano aveva comunicato su Twitter di non disporre del denaro per pagare il riscatto e che quindi non avrebbe potuto recuperare le foto del figlio deceduto. Gli amministratori di GandCrab hanno mostrato compassione decidendo di mettere a disposizione un codice di decifratura per le vittime siriane del ransomware.[51]

È probabile che l'annuncio di voler mandare in pensione GandCrab fosse solo una trovata dei suoi amministratori per dirottare altrove l'attenzione e riorganizzarsi. Secondo alcuni esperti di sicurezza, essi sarebbero infatti di nuovo attivi e utilizzerebbero software di crittografia chiamati REvil e Sodinokibi.[52] Il malware Sodinokibi ha già fatto le sue prime vittime in Svizzera.

3.5 Prospettive

Nel campo del ransomware, nei prossimi anni vi saranno ulteriori sviluppi tecnici e metodologici. Gli attacchi diventeranno prevedibilmente ancora più mirati e i vettori di attacco saranno tecnicamente più evoluti. Sarà quindi necessario rimuovere le vulnerabilità e mantenere alto il livello di protezione nella rete. L'approccio dei criminali è tipicamente opportunista: se l'impegno è troppo oneroso e non vi sono prospettive di successo in tempo utile, l'obiettivo diventa inappetibile e i criminali desistono.

Da alcuni anni si osserva come la crescita esponenziale di apparecchi collegati a Internet (Internet delle cose) rappresenti per i criminali un'area d'attacco in continua espansione in cui agire.[53] A seguito di questa evoluzione, la maggior parte degli apparecchi elettronici che utilizziamo quotidianamente è collegata alla rete domestica o addirittura direttamente a Internet e quindi è potenzialmente vulnerabile. Sono vari gli scenari in cui i criminali possono rendere temporaneamente inutilizzabile un apparecchio per ricattare il proprietario.

Anche l'azione di perseguimento penale si fa più evoluta e collabora con le autorità di sicurezza e le aziende private su vari livelli per porre un freno ai criminali. Il coordinamento dei vari soggetti a livello nazionale e internazionale ha dato i primi frutti.[54]

---

50 https://www.europol.europa.eu/newsroom/news/just-released-fourth-decryption-tool-neutralises-latest-version-of-gandcrab-ransomware

51 https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/

52 https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/ e https://www.tesorion.nl/aconnection-between-the-sodinokibi-and-gandcrab-ransomware-families/

53 MELANI rapporto semestrale 2014/2, cap. 5.3.

54 https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public; https://www.maketecheasier.com/man-arrested-for-spreading-shame-driven-ransomware/

3.6 Guest article: Insieme contro i cibercriminali

di Daniel Nussbaumer, capo del reparto cibercriminalità della polizia cantonale di Zurigo e responsabile NEDIK

Per combattere i cibercriminali servono autorità di perseguimento penale digitalmente abili. In questa lotta è essenziale lo scambio costante tra Confederazione e Cantoni che devono essere in grado di reagire rapidamente. Per questo i corpi di polizia svizzeri si sono riuniti nella rete NEDIK per svolgere, in collaborazione con MELANI, un'azione comune repressiva e preventiva.

Attacchi informatici professionali, mirati contro le aziende, possono minarne l'esistenza. Le aziende colpite si ritrovano a lottare per la loro sopravvivenza e conseguentemente hanno nuove, mutate esigenze nei confronti delle autorità. Per un'azienda che viene attaccata è importante sapere come i criminali sono penetrati nei sistemi e quali di questi sono stati compromessi, come deve comportarsi in caso di richieste di riscatto e se è stata l'unica ad essere danneggiata.

In tali situazioni sono d'aiuto i corpi di polizia svizzeri e MELANI. Tutti i corpi di polizia della Svizzera si sono riuniti nella rete intercantonale di sostegno alle indagini nella lotta contro la criminalità informatica NEDIK per poter reagire rapidamente insieme in caso di ciberattacchi. Grazie allo scambio regolare a livello operativo nell'ambito di questa rete e alla diffusione diretta di informazioni sui nuovi casi e di aggiornamenti sull'evoluzione degli eventi, oggi siamo in grado di riconoscere le interazioni molto velocemente – anche grazie all'intensa attività di scambio con MELANI – di reagire in modo adeguato e di fornire raccomandazioni appropriate. Grazie alla partecipazione dell'Ufficio federale di polizia (fedpol) nella rete NEDIK e alla sua collaborazione con Europol siamo in grado di agire immediatamente oltre i confini nazionali anche in caso di nuovi attacchi.

NEDIK offre un valore aggiunto, non solo per risolvere i casi di attacco. Insieme a MELANI produciamo nell'ambito di NEDIK dei rapporti sulla situazione nel settore informatico e sviluppiamo insieme consigli di prevenzione e strategie per impedire e contrastare la cibercriminalità. Queste best practice sono rese disponibili a tutti i corpi di polizia per offrire a tutti i soggetti coinvolti in ogni Cantone la migliore assistenza possibile nel settore della protezione contro i rischi informatici, a livello sia preventivo sia repressivo.

Raccomandazioni:

MELANI consiglia di adottare le seguenti misure protettive contro i ransomware:

- **effettuate regolarmente delle copie di sicurezza (backup) dei vostri dati, ad esempio su un disco rigido esterno. Utilizzate un programma che permetta di effettuare il backup regolarmente (giornalmente, settimanalmente, mensilmente / minimo due gerarchie). Al termine del backup, assicuratevi di scollegare dal computer o dalla rete il dispositivo su cui sono conservate le copie. Altrimenti gli aggressori potrebbero accedere anche alla copia di sicurezza, cifrando o eliminando i dati;**

- assicuratevi che i provider che offrono soluzioni cloud generino al meno due gerarchie, analogamente ai salvataggi di dati classici. L'accesso ai backup su cloud deve essere protetto dai ransomware, ad esempio tramite l'utilizzo di un secondo fattore di autenticazione per operazioni sensibili;
- sia il sistema operativo sia tutte le applicazioni installate sui computer o sul server (ad es. Adobe Reader, Adobe Flash, Java ecc.) devono essere mantenute costantemente aggiornate, preferibilmente mediante la funzione di update automatico;
- proteggete con un secondo fattore anche tutte le risorse accessibili da Internet (in particolare i terminal server, gli accessi RAS e VPN). Mettete unterminal server dietro a un portale VPN;
- bloccate nel gateway della vostra casella di posta elettronica la ricezione di allegati e-mail pericolosi, compresi i documenti di Office contenenti macro;
- accertatevi che non vi siano irregolarità nei file log del vostro antivirus.

4 La situazione a livello nazionale

4.1 Spionaggio

4.1.1 Lazarus attacca le banche svizzere

Nel marzo 2019 il produttore di software di sicurezza McAfee ha pubblicato un follow-up del rapporto di dicembre 2018 sulla campagna Sharpshooter, che lo scorso anno ha interessato 87 aziende in tutto il mondo, in particolare negli Stati Uniti d'America. Le aziende coinvolte erano operative nei settori della difesa, dell'energia, del nucleare e della finanza.[55] Nel secondo rapporto, McAfee conferma il primo sospetto: dietro gli attacchi si celerebbe il gruppo Lazarus, noto per aver attaccato i sistemi di varie banche[56] e che molti esperti collegano al regime nordcoreano.

Già nel primo rapporto McAfee aveva riferito di tentativi di attacco contro gli istituti finanziari svizzeri. Come già citato nell'ultimo rapporto semestrale,[57] MELANI è in contatto con varie banche. Ora come allora non sono state rilevate tracce di infezioni presso le aziende potenzialmente interessate in Svizzera.

4.1.2 APT40

L'attuale strategia della Cina per migliorare le relazioni commerciali tra l'Asia e l'Europa si basa sullo sviluppo di infrastrutture per la logistica e i trasporti. Il fornitore di servizi di sicurezza TIC FireEye ha scoperto un'operazione di spionaggio in atto almeno dal 2013 e mirata contro i

55 MELANI rapporto semestrale 2018/2, cap. 4.1.2.

56 https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks

57 MELANI rapporto semestrale 2018/2, cap. 4.1.2; https://www.tagesanzeiger.ch/sonntagszeitung/nordkorea-greift-schweizer-banken-an/story/15090344

Paesi strategicamente rilevanti per la nuova Via della seta (Belt and Road Initiative, BRI),[58] tra cui anche la Svizzera.[59] Dietro questa operazione si cela il gruppo APT40 (noto anche come Leviathan e TEMP.Periscope), che FireEye sospetta essere legato al governo cinese. L'obiettivo dell'operazione era acquisire informazioni per supportare la modernizzazione del settore marittimo in generale e delle capacità di cantieristica navale in particolare.

Il gruppo utilizza e-mail di phishing con allegati nocivi e infezioni drive-by per attaccare i settori della difesa, dei trasporti e della tecnologia navale. Già nel 2017 è stata utilizzata abusivamente l'identità di un produttore di sottomarini autonomi per infiltrarsi nelle università che svolgono ricerca nel settore dell'ingegneria navale. Questo settore è di fondamentale importanza per il governo cinese, sia sul piano commerciale che su quello della difesa.[60] Per questo la ricerca è finita anche nel mirino di altre campagne di spionaggio per le quali si sospettano legami con Pechino (cfr. anche cap. 4.1.4).

Oltre alle campagne di spionaggio nel settore della ricerca e dell'industria, APT40 svolge attività di spionaggio contro le organizzazioni del Sud-est asiatico ed è inoltre coinvolto nei conflitti territoriali nel Mar Cinese. Nel 2018 sono state compromesse svariate autorità cambogiane coinvolte nello svolgimento delle elezioni locali.[61] La Cambogia è tra i Paesi di rilevanza strategica per la nuova Via della seta.

Finora non sono state rilevate tracce di infezioni presso le aziende potenzialmente interessante in Svizzera.

4.1.3 VPN Filter

Nel mese di maggio dello scorso anno, Talos − la divisione di sicurezza dell'azienda di telecomunicazioni Cisco − ha riferito della botnet VPN Filter, comprendente almeno mezzo milione di router e dispositivi NAS in 54 Paesi, soprattutto in Ucraina.[62]

Il malware VPN Filter dispone di una struttura modulare con varie funzionalità. Ad esempio il software dannoso può rendere inutilizzabile un dispositivo, ma è anche in grado di diffondersi nella rete e di infettare altri sistemi (lateral movement). Può rubare informazioni (in particolare dati di accesso) e dirottare il traffico Internet verso un diverso destinatario. Inoltre un modulo cerca e controlla l'eventuale traffico di rete Modbus.[63] Modbus è un protocollo di comunicazione spesso impiegato dai sistemi di controllo industriali.

La botnet di VPN Filter avrebbe potuto essere utilizzata anche per azioni di sabotaggio ma, non appena è stata resa nota, l'FBI ha preso il controllo di una parte dell'infrastruttura *command & control*. Grazie a questa misura è stato possibile non solo identificare i dispositivi infettati, ma anche impedire l'invio dei comandi dei gestori della botnet agli apparecchi.

---

58 https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html

59 Sulla Belt and Road Initiative vedi http://english.www.gov.cn/beltAndRoad/ e http://english.www.gov.cn/archive/publications/2015/03/30/content_281475080249035.htm

60 Cfr. con la strategia «Made in China 2025» su http://english.www.gov.cn/2016special/madeinchina2025/; http://en.people.cn/n/2015/0522/c98649-8895998.html

61 https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html

62 MELANI rapporto semestrale 2018/1, cap. 5.1.2.

63 https://blog.talosintelligence.com/2019/05/one-year-later-vpnfilter-catastrophe.html

Sebbene siano stati pubblicati update che consentono ai software di sicurezza di identificare e arrestare il malware, MELANI è a conoscenza della presenza di alcune centinaia di infezioni ancora attive in Svizzera. Per eliminare il software nocivo e colmare le lacune di sicurezza è necessario ripristinare le impostazioni di fabbrica degli apparecchi e poi aggiornarli.

Raccomandazione:

Sempre più frequentemente l'infrastruttura di rete viene presa di mira da criminali informatici. Router e switch sono obiettivi allettanti perché sono spesso collegati a Internet ma allo stesso tempo non sono sempre sufficientemente protetti. Perciò possono rappresentare un facile varco per penetrare in una rete domestica o aziendale.

Ogni dispositivo collegato direttamente a Internet necessita di una protezione specifica contro gli accessi non autorizzati. Oltre all'uso di una password forte è necessario installare rapidamente ogni update.

4.1.4 APT10

Nel primo semestre del 2019, la campagna di spionaggio informatico APT10 ha fatto nuove vittime. Il gruppo attivo dal 2006 ha raggiunto la notorietà a seguito dell'operazione Cloud Hopper con cui dal 2015 ha attaccato Managed Services Provider (MSP) in tutto il mondo.[64] Il dipartimento di giustizia statunitense (Department of Justice, DoJ) e gli altri quattro Paesi del gruppo Five Eyes hanno preso ufficialmente posizione accusando apertamente il governo cinese di partecipare a questa operazione di spionaggio.[65]

Il 20 dicembre 2018 il DoJ ha accusato di truffa e furto d'identità due cittadini cinesi sospettati di aver partecipato all'operazione Cloud Hopper. Vittime della campagna di spionaggio sono risultati due grandi provider di servizi informatici: Hewlett Packard Enterprise (HPE) e IBM. Il sospetto è che, per lo meno nel caso di HPE, l'aggressore fosse penetrato nella rete già da vari anni.

Nel giugno 2019 l'agenzia di stampa Reuters ha pubblicato i nomi di altre sei vittime di APT10.[66] Si tratta di Fujitsu, Tata Consultancy Services, Dimension Data, NTT, Computer Sciences Corporation e DXC Technology. A seguito di questa nuova scoperta il numero delle possibili vittime è aumentato drasticamente. Difatti i Managed Services Provider non sono il bersaglio reale ma servono da vettore per penetrare nelle grandi aziende di cui gestiscono o supportano l'infrastruttura della tecnologia dell'informazione e della comunicazione. L'infezione HPE, ad esempio, è stata scoperta dal team di sicurezza TIC di Ericsson. Il gigante

---

64 MELANI rapporto semestrale 2018/2, cap. 5.1.1 e 2017/1, cap. 5.1.1.

65 https://www.securityweek.com/five-eyes-nations-blame-china-apt10-attacks;
USA: https://www.justice.gov/opa/press-release/file/1121706/download;
Gran Bretagna: https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign;
Canada: https://cse-cst.gc.ca/en/media/media-2018-12-20;
Australia: https://foreignminister.gov.au/releases/Pages/2018/mp_mr_181221.aspx;
Nuova Zelanda: https://www.ncsc.govt.nz/newsroom/cyber-campaign-attributed-to-china/

66 https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/

svedese delle telecomunicazioni era alla ricerca del vettore d'ingresso di varie infezioni malware verificatesi tra il 2014 e il 2017. È impossibile dire quante aziende siano state infiltrate tramite questo vettore. I service provider sono un bersaglio molto vantaggioso perché dispongono di diritti di accesso diretto ai sistemi dei loro clienti e talvolta trattano anche dati per loro.

Gli attacchi puntano a rubare la proprietà intellettuale. Le vittime sono attive, ad esempio, nei settori dell'ingegneria navale militare o della tecnica dei sottomarini nucleari. La modernizzazione della tecnologia marittima e navale è di fondamentale rilevanza per la Cina.[67] Un altro obiettivo degli attacchi è il controllo della concorrenza: Ericsson ad esempio è un concorrente dei produttori cinesi nel settore della telefonia mobile. Inoltre il furto di informazioni riservate relative alla cifra d'affari permette di valutare se un'azienda è appetibile per una futura acquisizione.

Tuttavia la campagna di spionaggio potrebbe avere anche obiettivi diversi da quelli meramente commerciali. Tra le vittime confermate spicca l'azienda Sabre Corp. che gestisce i sistemi di prenotazione per migliaia di hotel in tutto il mondo, così come i biglietti aerei di centinaia di compagnie aeree. Sebbene pare non vi sia stata alcuna fuga di dati di viaggio, tramite questo canale gli aggressori avrebbero potuto impossessarsi di informazioni sugli spostamenti dimolte persone.

Nel documento pubblicato dal DoJ, tra gli Stati in cui sono presenti organizzazioni prese di mira figura anche la Svizzera. Sebbene non vi siano prove concrete di infezioni presso le organizzazioni con sede in Svizzera, in generale le aziende potenzialmente interessanti per le acquisizioni devono sempre essere considerate possibili bersagli dello spionaggio informatico.

4.2 Sistemi di controllo industriali

Spesso le comodità della vita moderna sono rese possibili grazie ai sistemi di controllo industriali. Se l'energia elettrica prodotta dalle turbine dei bacini idroelettrici giunge in modo affidabile alla presa elettrica domestica lo dobbiamo, tra l'altro, ai sistemi di controllo dei distributori locali. Uno studio presentato nel capitolo 4.2.1 illustra le dotazioni di sicurezza informatica di queste aziende elettriche di medie e piccole dimensioni. I sistemi di controllo sono impiegati anche nel settore dei trasporti, permettendoci di giungere comodamente e velocemente a destinazione. Le sfide che devono essere superate, ad esempio nel campo dell'atterraggio strumentale, sono illustrate nel capitolo 4.2.2.

4.2.1 Sfide per le piccole e medie imprese elettriche

Nell'ambito dell'energia elettrica fanno notizia soprattutto gli eventi che riguardano le centrali atomiche, idroelettriche e le linee di alta tensione. Ma per i clienti finali è piuttosto il distributore locale a svolgere un ruolo decisivo in termini di affidabilità del servizio. La sicurezza informatica di queste aziende elettriche di medie e piccole dimensioni è stata oggetto di uno studio[68] dell'associazione Electrosuisse.

---

[67] Cfr. con la strategia «Made in China 2025» su http://english.www.gov.cn/2016special/madeinchina2025/; http://en.people.cn/n/2015/0522/c98649-8895998.html

[68] https://www.electrosuisse.ch/wp-content/uploads/2019/03/Electrosuisse_Cybersecurity-Erhebung-EVU_.pdf

Nonostante la sicurezza informatica sia al centro dell'attenzione in ogni azienda, dallo studio emerge che lo stato di implementazione e l'approccio sistematico verso le misure atte a garantire la sicurezza delle informazioni denotano ancora un potenziale di ampliamento, soprattutto nelle centrali elettriche più piccole. Sulla base del NIST Cybersecurity Framework[69] lo studio ha individuato un focus sulle misure protettive preventive mentre vengono trascurati altri elementi del framework.

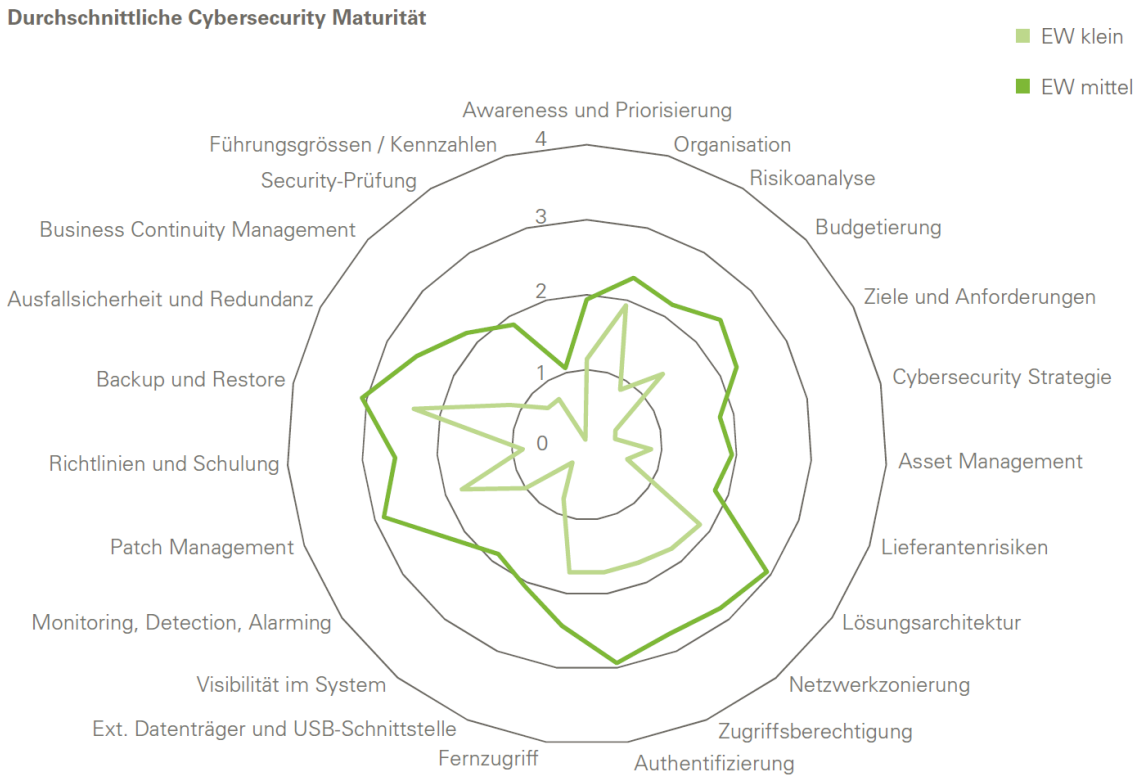

Figura 1: Riepilogo dei risultati dello studio nei settori della cibersicurezza presi in esame.

In molte aziende è stata rilevata un'inventariazione insufficiente (asset management) unita a una scarsa visibilità nella rete. Insieme alla bassa capacità di reazione e alla mancanza di esercitazioni di emergenza sono emerse sfide rilevanti sul piano del rilevamento e della risoluzione degli eventi. Per quanto riguarda gli aspetti organizzativi generali d'organizzazione è stata attestata una scarsissima considerazione dei rischi nella definizione della priorità delle differenti misure e della impostazione del bilancio. In questo ambito emergono la scarsa attenzione rivolta al rischio fornitori e alla gestione del fattore umano quale punto debole. Queste carenze sono spesso dovute alla mancanza di competenze specialistiche e risorse, soprattutto tra le aziende più piccole che hanno partecipato all'indagine, con il risultato che la cibersicurezza non è gestita attivamente come processo a sé stante.

Un modo per colmare queste lacune da parte delle aziende elettriche di medie e piccole dimensioni consiste nella cooperazione nei settori identici per ogni azienda. Un progetto degno di nota in quest'ambito è l'iniziativa promossa da Swisspower, l'alleanza strategica delle

69 https://www.nist.gov/cyberframework

aziende municipali svizzere per favorire la cooperazione tra le imprese sul fronte della cibersicurezza.[70] Grazie a questa rete, tutti i partner della cooperazione possono approfittare delle esperienze degli altri e insieme aumentare costantemente il livello della sicurezza informatica.

4.2.2 Anche i sistemi di atterraggio strumentale sono vulnerabili

Nella maggior parte degli aeroporti civili del mondo, nelle manovre di avvicinamento i piloti sono coadiuvati da un sistema di atterraggio strumentale (in inglese instrument landing system, ILS). Questi sistemi sono stati progettati in un'epoca in cui la tecnologia radio impiegata era disponibile o accessibile solo per una cerchia ristretta di utenti. Tra le condizioni quadro un tempo individuate, le misure crittografiche di protezione e autenticazione non erano una priorità. Nella scorsa conferenza Usenix[71] i ricercatori della Northeastern University di Boston hanno dimostrato un metodo poco costoso per falsificare i segnali radio di un ILS e per mostrare a un velivolo un orientamento errato.[72] Il dispositivo descritto nel documento di ricerca[73] utilizza componenti disponibili in commercio per simulare i segnali ILS. Perché l'attacco riesca, il dispositivo viene collocato nel velivolo o in un raggio di tre miglia dalla pista di atterraggio verso cui l'aereo fa rotta. Occorre che il segnale contraffatto presenti per il velivolo una potenza di segnale più forte rispetto alla reale comunicazione dell'aeroporto, di modo che l'aereo orienti il ricevitore sul segnale di attacco.

Problemi analoghi sono noti anche per altri ausili di navigazione basati sulle trasmissioni radio, come i GPS (cfr. anche cap. 5.2.2). Poiché i piloti sono addestrati anche per affrontare un guasto o un malfunzionamento dell'ILS, dovrebbero essere in grado di reagire adeguatamente a un simile attacco. Ma se questa tecnica sarà ulteriormente migliorata e impiegata in futuro questi attacchi potrebbero causare disagi per i voli e gli aeroporti. In questo caso si potrebbero prevedere degli attacchi con conseguenze simili a quelle dei fatti accaduti nel mese di dicembre 2018 quando droni non autorizzati hanno paralizzato l'aeroporto di Gatwick.[74]

Raccomandazione:

Invitiamo i lettori a segnalarci eventuali sistemi di controllo apertamente accessibili o inadeguatamente protetti individuati in Internet, in modo da poter informare i gestori.

Formulario d'annuncio MELANI

https://www.melani.admin.ch/melani/it/home/meldeformular/formular0.html

Lista di controllo delle misure di protezione dei sistemi di controllo industriali:

https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/misure-di-protezione-dei-sistemi-industriali-di-controllo--ics-.html

70 https://swisspower.ch/medien/medienmitteilungen/swisspower-lanciert-kooperation-für-cybersecurity-in-stadt-werken

71 https://www.usenix.org/

72 https://arstechnica.com/information-technology/2019/05/the-radio-navigation-planes-use-to-land-safely-is-insecure-and-can-be-hacked/

73 https://aanjhan.com/assets/ils_usenix2019.pdf

74 MELANI rapporto semestrale 2018/2, cap. 5.2.3.

4.3 Attacchi (DDoS, Defacements, Drive-By)

In Svizzera privati, organizzazioni e aziende sono tuttora vittime di varie tipologie di attacco.

4.3.1 Distributed Denial of Service – DDoS

Nel periodo oggetto del rapporto sono stati segnalati a MELANI svariati attacchi DDoS. Ciò dimostra che questo metodo è ancora utilizzato da vari attori per rendere inaccessibili i sistemi dei loro bersagli. Può trattarsi di tentativi di estorsione di matrice criminale così come di attivisti che desiderano danneggiare aziende o organizzazioni. Ci sono anche casi per cui non è stato possibile chiarire la motivazione. Si può supporre che gli aggressori talvolta testino la loro infrastruttura su vittime scelte casualmente.

Raccomandazione:

MELANI raccomanda svariate misure preventive e reattive per contrastare gli attacchi DDoS:

Lista di controllo delle misure contro gli attacchi DDoS:

https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/massnahmen-gegen-ddos-attacken.html

4.3.2 Hackeraggio di siti

Continuano gli attacchi contro i siti web, che vengono compromessi e utilizzati a scopo criminale. Per lo più gli hacker ottengono accesso ai siti web grazie a una versione obsoleta di un Content Management System (CMS) o tramite dati di accesso FTP rubati e collocano software dannosi o una pagina di phishing. Quando MELANI rileva casi di questo genere, informa i gestori dei siti e fornisce loro le indicazioni per risolvere il problema.[75]

Raccomandazione

Prevenire è meglio che reagire: se utilizzate un CMS come Typo3, Wordpress o Joomla, MELANI vi consiglia di dare uno sguardo alla lista di controllo «Misure per contribuire alla sicurezza dei sistemi di gestione dei contenuti (CMS)» in modo da proteggere adeguatamente i vostri siti web.

Lista di controllo delle misure per contribuire alla sicurezza dei sistemi di gestione dei contenuti (CMS):

https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/misure-per-contribuire-alla-sicurezza-dei-sistemi-di-gestione-de.html

75 https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/guida-alla-disinfestazione-dei-siti-web.html

4.3.3 Domain grabbing: quando una società di tiro si ritrova improvvisamente a vendere scarpe o una campagna politica pubblicizza accessori contraffatti

Più che un vero e proprio attacco, l'appropriazione dei nomi di dominio non rinnovati consiste nello sfruttamento del sistema. I cosiddetti domain grabber osservano quali nomi di dominio sono scaduti e li registrano a proprio nome una volta terminato il periodo di attesa. Spesso su questi domini vengono collocati web shop fraudolenti[76], tuttavia sono molti i modelli di business perseguiti con questi domini appena «scaduti». Essi beneficiano, per lo meno nel breve periodo, della buona reputazione costruita negli anni dal precedente titolare del dominio. Poiché in generale i link che da siti terzi conducono a questi domini sono ancora attivi. Essi talvolta continuano a figurare in testa agli elenchi dei risultati dei motori di ricerca.

Raccomandazione:

Le registrazioni dei nomi di dominio devono essere rinnovate con regolarità. Se avete un sito web, tenete d'occhio la scadenza del nome di dominio per evitare di perderlo. Anche la disattivazione di un sito web richiede una pianificazione. Lo spegnimento controllato di un dominio non è costoso e offre vari vantaggi: ad esempio può essere gestito ancora per un certo periodo per informare tutti i visitatori che il sito web verrà chiuso. Inoltre una valutazione dei referrer aiuta a informare gli altri gestori dei siti web che rimandano al vostro dominio. In fin dei conti si tratta di proteggere la reputazione dell'entità associata al sito web, sia essa un'azienda, un'associazione, un privato o una comunità d'interesse, così come i rispettivi clienti e simpatizzanti.

4.4 Ingegneria sociale e phishing

Per sferrare un attacco efficace occorre mettere in piedi una storia credibile che spinga la potenziale vittima a intraprendere un'azione. Gli attacchi di social engineering hanno più probabilità di riuscire se gli aggressori dispongono di molte informazioni sulle vittime potenziali. A tale scopo i criminali utilizzano sia le fonti liberamente disponibili sia le informazioni ottenute dai furti di dati. I dati sottratti sono esaminati, collegati ad altri dati rubati o pubblicamente accessibili, elaborati e poi rivenduti ad altri criminali. Questi dati possono essere utilizzati per lanciare attacchi individuali su misura o per inviare in modo automatizzato mailing di massa personalizzati (malspam).

4.4.1 Phishing

Nel primo semestre del 2019 si è registrato un aumento dei tentativi di phishing segnalati a MELANI. Sono stati notificati 2521 URL classificabili come phishing, trasmessi alle varie organizzazioni che combattono questo tipo di frode (produttori di browser, organizzazioni antiphishing, hosting provider coinvolti). Gli obiettivi degli aggressori restano sostanzialmente gli stessi: da un lato si tenta di rubare i dati delle carte di credito, dall'altro si cerca di ottenere il nome utente e la password per i servizi Internet come PayPal, Spotify o Apple. Sempre più

[76] In Svizzera questo fenomeno è osservato con una certa frequenza dal 2016. Da allora SWITCH, che gestisce la registrazione dei domini «.ch», attua misure di contrasto molto efficienti. Altri domini nazionali invece arrancano: https://www.nzz.ch/digital/kampf-gegen-fake-shops-im-netz-ld.1484852

frequentemente i tentativi di phishing prendono di mira gli account di posta elettronica, che possono essere utilizzati in seguito per ulteriori attacchi. Un metodo recentemente comparso sulla scena è il cosiddetto «Real time phishing» (phishing in tempo reale, cfr. cap. 4.4.2).

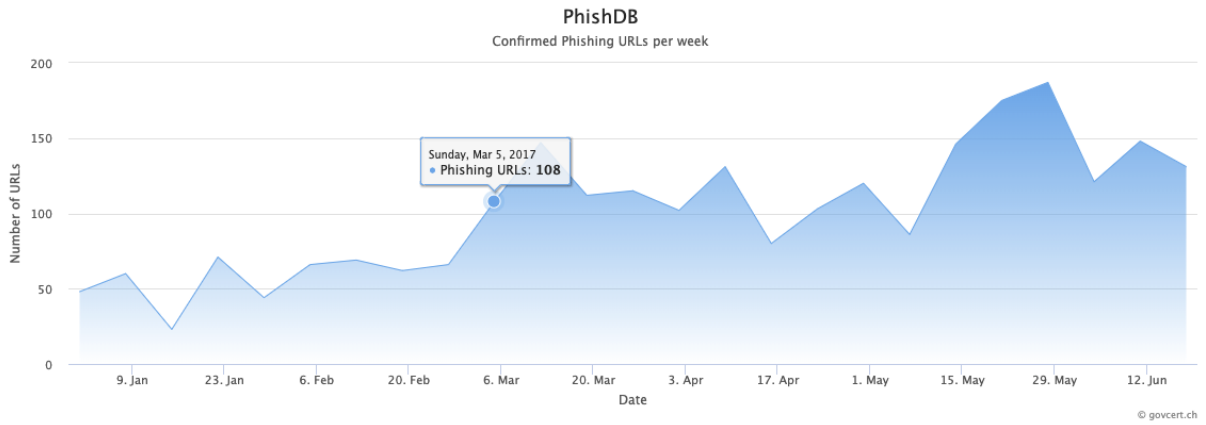

Figura 2: Pagine di phishing segnalate e confermate settimanalmente su antiphishing.ch nel primo semestre 2019

Questo incremento è riconducibile, in parte, alle grandi ondate di phishing mirate al furto dei dati delle carte di credito.

4.4.2 Real time phishing contro PostFinance e UBS

Il metodo di phishing più frequente consiste nel raccogliere in grande stile i dati di accesso per poi utilizzarli alcune ore dopo o qualche giorno dopo per accedere al conto della vittima. Spesso i dati di accesso rubati sono anche rivenduti. Questa procedura però non funziona se l'utente utilizza un secondo fattore per l'autenticazione (ad es. una password unica, in inglese «One Time Password», OTP). La risposta degli aggressori all'impiego sempre più frequente delle OTP è il real time phishing (phishing in tempo reale): l'aggressore entra immediatamente in azione non appena la vittima clicca sul link di phishing contenuto nell'e-mail che la indirizza al server web dell'aggressore.

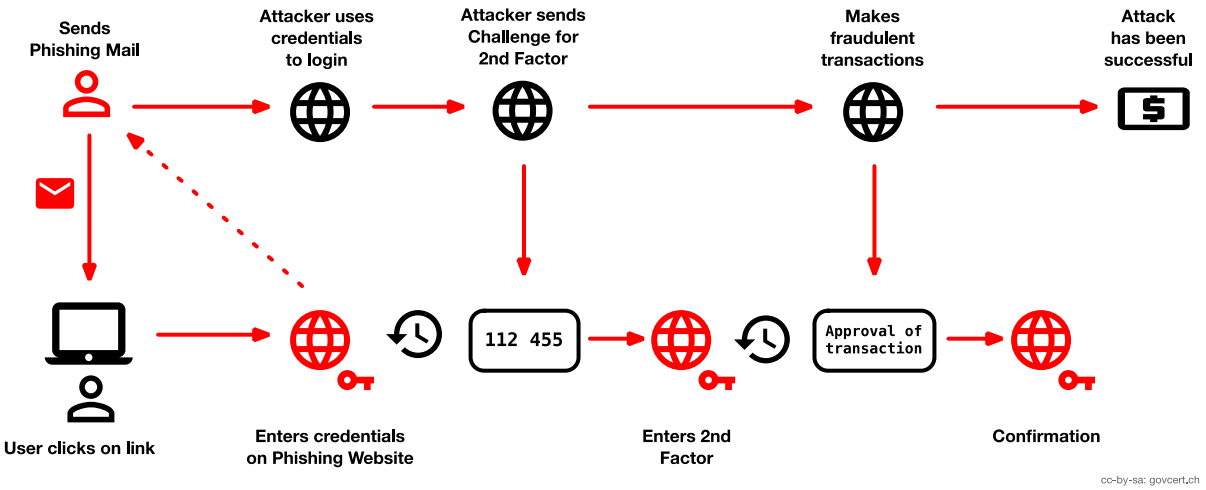

Figura 3: Schema di svolgimento di un attacco di real time phishing

L'aggressore presenta una pagina di login falsificata a regola d'arte in cui la vittima tenta di autenticarsi. Il criminale registra così i suoi dati e li utilizza per accedere alla vera piattaforma

di e-banking, che gli richiederà di autenticarsi con un secondo fattore. L'aggressore mostra allora la stessa richiesta alla vittima sul server web falsificato. Quando l'utente inserisce anche il secondo fattore, l'aggressore ottiene accesso al portale di e-banking e inganna l'utente con un messaggio di errore.

Nel periodo preso in esame da questo rapporto si sono osservate due campagne di questo tipo rivolte contro i clienti di istituti finanziari svizzeri.

4.4.3 Gli account dei social media sono preziosi

Oltre agli account di posta elettronica, il phishing prende di mira le informazioni delle carte di credito. Qualsiasi conto online è minacciato. Se con un account Twitter hackerato può essere avviata una campagna di disinformazione che pone in cattiva luce il legittimo utente, i profili Instagram[77] o gli account di Youtube hackerati possono implicare per i malcapitati anche conseguenze finanziarie. Abbonati e follower sono il capitale degli influencer che, se perdono il controllo della loro presenza online, devono ricominciare da capo e ricreare la loro community di sana pianta. Inoltre nel frattempo non possono pubblicare alcun contenuto online, perdendo così degli introiti. La perdita del controllo di un account online non ha conseguenze solo per le personalità più in vista, difatti la vita di un numero crescente di persone si svolge almeno in parte sulle piattaforme social. Perdere l'accesso per esempio al proprio account Facebook può significare non potere gestire i propri contatti per un certo tempo.

Raccomandazione

È importante proteggere gli account online nel miglior modo possibile, ad esempio con un'autenticazione a due fattori. Informatevi in anticipo sulle misure di sicurezza del fornitore dei servizi e sull'eventuale procedura che consente di recuperare il controllo di un account hackerato. È inoltre consigliabile utilizzare una password complessa e differente per ciascun servizio online.

4.4.4 Gli schermi piccoli aumentano il rischio di frodi

Gli smartphone sono piccoli computer. Molte persone effettuano la gran parte delle loro comunicazioni con questi dispositivi. Spesso anche gli appuntamenti sono gestiti tramite l'app del calendario dello smartphone. Una grande sfida per i programmatori di app sta nel riuscire a visualizzare in modo adeguato quante più informazioni importanti su uno schermo relativamente piccolo. Spesso questo fa sì che alcune informazioni basilari, come l'indirizzo completo di un link o l'indirizzo e-mail nascosto dietro il nome visualizzato (che può essere scelto liberamente dal mittente) siano difficilmente riconoscibili o accessibili. Sebbene la riduzione all'essenziale sia utile e appropriata per le normali condizioni di utilizzo dello smartphone, essa offre ai criminali molte possibilità per ingannare i destinatari delle e-mail e di altri messaggi. Oltre all'invio di e-mail, SMS e altri brevi messaggi fraudolenti, a seconda delle impostazioni dello smartphone e delle app è possibile inserire automaticamente richieste di appuntamento[78] così come visualizzare sullo schermo notifiche e altre comunicazioni.

---

77 https://blog.trendmicro.com/trendlabs-security-intelligence/how-a-hacking-group-is-stealing-popular-instagram-profiles/

78 Cfr. MELANI, Rapporto semestrale 2018/1, cap. 4.4.4.

Raccomandazione

Quando utilizzate lo smartphone, non lasciatevi ingannare da messaggi inaspettati, anche se provengono da un canale regolamentare e si presentano in un formato familiare. Chiedetevi sempre se il messaggio non sia stato inviato da qualcuno per indurvi a cliccare senza troppo riflettere. Eliminate senza indugio i messaggi sospetti. Assicuratevi che le impostazioni del vostro smartphone e delle app consentano di inserire nel calendario unicamente gli appuntamenti accettati e che la vostra sfera privata sia adeguatamente protetta.

4.4.5 Perdura la CEO-Fraud

MELANI ha messo in guardia dalla CEO-Fraud (truffa del CEO) già a partire dal 2013.[79] Questa truffa non è dunque nuova e viene tuttora utilizzata per attaccare sistematicamente svariate organizzazioni. Attualmente, oltre alle aziende private, fra i bersagli vi sono associazioni sportive e di vario genere così come le amministrazioni comunali. Sui loro siti web sono spesso presenti tutte le informazioni necessarie ai truffatori per compiere i loro attacchi. Gli organigrammi contengono i nomi e gli indirizzi e-mail delle persone che ricoprono le diverse funzioni, come i presidenti delle associazioni, i sindaci, i cassieri e i responsabili delle finanze. La procedura standard della CEO-Fraud consiste di un'e-mail in cui i truffatori si spacciano per il presidente e con varie motivazioni richiedono al responsabile delle finanze di eseguire un bonifico.

Da: «indirizzo falsificato del presidente dell'associazione»
Inviato: martedì, 19 marzo 2019 14.00
A: «Cassiera dell'associazione»
Oggetto: RICHIESTA

Ciao Corinna,
avrei bisogno che tu eseguissi un bonifico. Fammi sapere se puoi farlo subito, così ti mando le coordinate bancarie.
Attendo una tua risposta.

Saluti
«Nome del presidente»

Inviato dal mio iPhone

Mail 1: Il truffatore si spaccia per il presidente e richiede alla cassiera un bonifico urgente.

[79] MELANI rapporto semestrale 2013/1, cap. 3.4.

Ciao Corinna,

«Coordinate bancarie di un conto estero»

Informami quando è stato eseguito.

Saluti
«Nome del presidente»

Inviato dal mio iPhone

Mail 2: Dopo la risposta, il «presidente» invia il numero di conto per il bonifico all'estero.

Grazie alle informazioni facilmente reperibili online, i truffatori hanno automatizzato gli invii, trascurando evidentemente il controllo della qualità, con conseguenze talvolta curiose. Nelle piccole associazioni o nei piccoli comuni, il presidente o il sindaco può anche essere il responsabile delle finanze. Entrambe le funzioni hanno dunque lo stesso indirizzo e-mail. Ad esempio a MELANI è stato segnalato il caso di una cassiera di un comune, di cui al tempo stesso è anche la sindaca, che ha ricevuto al suo stesso indirizzo di posta elettronica un'e-mail dal presunto sindaco. Questo esempio mostra che i truffatori si procurano le informazioni necessarie al loro attacco da fonti liberamente accessibili (siti web aziendali, reti sociali).

Raccomandazione

MELANI raccomanda sempre di verificare quali informazioni sulle persone, le associazioni, le aziende ecc. sono accessibili online e se la loro pubblicazione è davvero necessaria. Altre misure protettive sono la sensibilizzazione del personale e la definizione di procedure precise, in particolare per i pagamenti.

INFO

Informazioni e raccomandazioni sulla truffa del CEO:

https://www.melani.admin.ch/melani/it/home/themen/CEO-Fraud.html

4.4.6 Malspam: intimidire e incuriosire per propagare il malware

I criminali informatici inventano sempre nuovi metodi per indurre i destinatari delle e-mail a cliccare su un link o ad aprire un file. La loro fantasia non ha limiti. Nei primi sei mesi del 2019 sono stati vari i tentativi di imbroglio a danno degli utenti, talvolta indotti a installare software nocivi da storie che fanno rizzare i capelli.

Abbonamento a pagamento: con un'e-mail molto concisa si ringraziano i destinatari per aver sottoscritto un abbonamento a un giornale o a una rivista, invitandoli a consultare i dettagli del pagamento e le condizioni di utilizzo in un documento allegato. Per ingannare i destinatari, i loro nomi e cognomi sono citati nell'oggetto dell'e-mail.

Azioni legali contro ex-clienti: la banca dati clienti di una piccola azienda è stata hackerata per inviare a tutti i contatti sottratti un'e-mail personale in cui i destinatari venivano accusati di aver violato le condizioni contrattuali e si comunicava l'avvio di un'azione per risarcimento dei danni. Per maggiori dettagli si rimandava a un documento allegato. Per ingannare i destinatari meno

attenti, come mittente compariva il nome dell'azienda, sebbene l'indirizzo effettivo da cui provenivano le e-mail non fosse stato falsificato.

Azioni legali contro attività di ristorazione: in un'e-mail si comunicava che un famigliare aveva contratto un'intossicazione alimentare dopo essere stato al ristorante, contro il quale si intentava un'azione legale. In questi casi l'e-mail fungeva unicamente per instaurare un contatto. Se il destinatario rispondeva, riceveva un'altra e-mail con un link dietro il quale si celava il malware. In tal modo i criminali diffondevano il programma nocivo in modo molto mirato, anziché ad ampio raggio, soltanto alle persone che reagivano al contatto iniziale. Questo ha due vantaggi: da un lato, il malware non si propaga su ampia scala e quindi occorre più tempo prima che giunga all'attenzione degli attori della sicurezza, come i produttori di antivirus. Dall'altro lato è più probabile che il destinatario clicchi sul link, perché ha già avuto un contatto con il mittente e attende la sua successiva e-mail.[80]

Aiuto per una ragazza fatta prigioniera: con un'e-mail, una ragazza sosteneva di essere stata incatenata in cantina dal suo aguzzino e pregava i destinatari di informare i suoi genitori perché potessero salvarla. Tutti i dati erano contenuti in un documento allegato.

Eutanasia ordinata e pagata: questo tentativo di frode informava impietosamente i destinatari che la procedura per la loro eutanasia era stata ordinata e pagata. Il personale sanitario sarebbe giunto a prelevarli a casa tra tre giorni. I documenti di accompagnamento necessari erano allegati all'e-mail. Anche in questo caso i destinatari hanno ricevuto una comunicazione personale, in cui era indicato il loro nome e l'indirizzo postale corretto.

Conclusione / Raccomandazione:

L'elemento comune a tutte queste frodi è cercare di indurre i destinatari, con motivazioni più o meno credibili, a cliccare senza perdere tempo su un link o ad aprire un file per ottenere «maggiori informazioni». Le e-mail erano quasi tutte personalizzate, cioè si rivolgevano ai destinatari per nome e talvolta indicavano anche l'indirizzo di domicilio o il numero di telefono, informazioni che, tipicamente, sono ricavate tramite le fughe di dati degli shop online o da rubriche hackerate in cui gli utenti presi di mira figuravano tra i contatti.

La presenza del proprio nome, dell'indirizzo di casa o del telefono non sono indicazioni su cui fare affidamento per determinare la legittimità del mittente di un messaggio. Siate scettici se ricevete delle e-mail che vi richiedono di compiere un'azione per evitare determinate conseguenze (perdita di denaro, denuncia penale o procedura giudiziaria, blocco del conto o della carta, perdita di un'opportunità, disgrazia), in particolare se fanno leva sull'urgenza. Non aprite mai gli allegati delle e-mail sospette e non cliccate mai sui link, neppure per curiosità. Rischiate di infettare il vostro dispositivo con software dannosi o di finire su siti web sospetti. In caso di dubbio richiedete al presunto mittente, tramite una modalità di contatto indicata sul suo sito web o altrimenti già a voi nota, di cosa si tratta esattamente e se ha effettivamente inviato l'e-mail.

[80] La stampa specializzata ha messo in guardia i ristoratori contro questa truffa: https://www.hotellerie-gastronomie.ch/de/artikel/achtung-ein-gastro-schreck-geistert-herum/ (del 19.3.19); https://www.baizer.ch/aktuell?artID=6788&lvl=2 (del 9.4.19); https://www.onlinewarnungen.de/warnungsticker/e-mail-lebensmittelvergiftung-trojaner-im-anhang-enthalten/ (del 21.5.19).

4.4.7 Nuovi tentativi di estorsione a nome del DFGP

Negli anni 2011 e 2012 le estorsioni online sono comparse per la prima volta in grande stile. Allora generalmente veniva bloccato il browser o l'intero computer e presunte autorità di perseguimento penale o società di gestione dei diritti d'autore sostenevano che l'utente avesse diffuso materiale pornografico illegale o condiviso illegittimamente contenuti musicali e cinematografici.[81] Questo tipo di attacco è stato in larga misura sostituito dai trojan di crittografia,[82] ma non ancora abbandonato del tutto, come dimostra il seguente esempio. I criminali hanno adattato il nuovo layout del sito web del dipartimento federale, ma il linguaggio utilizzato ricorda piuttosto dei messaggi phishing di prima generazione o dei tentativi di frode: gli errori di grammatica e l'uso di più lingue diverse sono chiari indizi che il sito visualizzato non può appartenere a un'autorità svizzera. In questo caso il computer non veniva infettato con malware, i criminali tentavano invece, con la sola intimidazione, di convincere le persone a eseguire il pagamento. La polizia non bloccherebbe mai un computer per riscuotere in tal modo una multa o una pena pecuniaria.

Figura 4: Sito web di blocco con logo federale

4.4.8 Fake sextortion: ancora molti cadono in questa trappola

Nel primo semestre del 2019 sono stati nuovamente riferiti casi di e-mail di fake sextortion con cui i mittenti sostenevano di aver piratato il computer del destinatario e di averlo filmato mentre si masturbava. Nel mese di febbraio 2019 MELANI ha pubblicato in merito una newsletter[83] e assieme ai corpi di polizia cantonali e ad altri partner ha lanciato un sito web[84] per sensibilizzare la popolazione su questo tema. Purtroppo sono ancora molte le persone che pagano il

81 Cfr. rapporto semestrale 2011/2, cap. 3.5 e 2015/2, cap. 4.5.2.

82 Si veda in merito il tema principale ransomware nel precedente capitolo 3.

83 https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/fake-sextortion.html

84 https://www.stop-sextortion.ch/it/

riscatto, senza sapere che quanto è sostenuto nelle e-mail è privo di fondamento. Sul sito web stop-sextortion.ch viene descritto in modo conciso come procedere anche qualora i ricattatori fossero davvero in possesso di materiale compromettente (se ad esempio la vittima ha partecipato precedentemente a una video chat o ha inviato delle foto in cui compare nuda).

Sono state osservate diverse ondate di e-mail di fake sextortion in inglese, tedesco, francese e anche alcune in italiano. La maggior parte di queste e-mail erano scritte in modo abbastanza corretto. Alcune apparivano invece tradotte rudimentalmente e contenevano affermazioni poco plausibili.

Complessivamente nell'arco di sei mesi a MELANI sono stati segnalati 4565 indirizzi bitcoin diversi. I pagamenti osservati si limitavano a pochi indirizzi; nella maggior parte dei casi non è stata effettuata alcuna transazione. Sono stati versati complessivamente 283 bitcoin (per un controvalore di circa 2,8 milioni di franchi alla fine di giugno 2019). Non si tratta solo di pagamenti dalla Svizzera, poiché è molto difficile dimostrare chi ha effettuato i pagamenti e da dove. Tuttavia queste cifre mostrano che viene tuttora versato del denaro anche se il fenomeno è già noto da molto tempo.

A livello internazionale, l'Internet Storm Center di SANS ha pubblicato le analisi degli indirizzi bitcoin utilizzati per i tentativi di fake sextortion che gli sono stati segnalati.[85] Il centro ha analizzato 434 indirizzi bitcoin. I versamenti sono stati effettuati solo su 56 indirizzi. Per un certo tempo il denaro non è stato toccato. Prima di ritirare il denaro, i criminali lo depositano su conti di consolidazione. SANS ha identificato due di questi indirizzi bitcoin di consolidazione, uno con 6190 bitcoin (per un controvalore di c. 62 mio. fr. a fine giugno 2019) e l'altro con 5312 bitcoin (per un controvalore di c. 53 mio. fr. a fine giugno 2019). L'autore dell'articolo di SANS suppone tuttavia che si tratti solo dell'inizio del cosiddetto cash-out e che l'importo effettivo superi di molto le cifre sopra indicate. Perché il cash-out vada a buon fine, i bitcoin sono suddivisi in importi più piccoli per poter mescolare il denaro in modo più efficace in un bitcoin mixer, rendendo impossibile la tracciabilità.

Raccomandazione

Se non conoscete personalmente il mittente dell'e-mail con cui tentano di ricattarvi e non avete partecipato precedentemente a una video chat, vi consigliamo di ignorare l'e-mail e di eliminarla. Non pagate in nessun caso il riscatto.

Se avete ricevuto un'e-mail di questo tipo potete contribuire alla prevenzione discutendo dell'argomento nella vostra sfera personale e professionale. In tal modo sensibilizzerete collaboratori, conoscenti e parenti e li aiuterete a non cedere all'estorsione.

Se invece avete avuto un precedente contatto con il ricattatore e questo è effettivamente in possesso di materiale compromettente, rivolgetevi al più vicino posto di polizia cantonale (https://polizei.ch/).

85 https://isc.sans.edu/forums/diary/Sextortion+Follow+the+Money+Part+3+The+cashout+begins/24592/; https://isc.sans.edu/forums/diary/Sextortion+Follow+the+Money+The+Final+Chapter/25204/

4.5 Fughe di dati

4.5.1 Traffico Swisscom dirottato su China Telecom

Il 6 giugno 2019 una parte consistente del traffico europeo di telefonia mobile è stato instradato per più di due ore sull'infrastruttura di China Telecom. Il caso si è verificato a seguito di un BGP route leak[86] nel centro di calcolo svizzero Safe Host che ha attribuito per errore all'Internet Service Provider (ISP) cinese oltre 70'000 connessioni della sua tabella di routing interna.

I route leak provocano il dirottamento del traffico dati su una connessione non voluta, causando il sovraccarico della rete o un «buco nero»[87]. A volte non è possibile trasmettere i dati, che vengono dunque cancellati senza essere recapitati a destinazione. Sono possibili anche delle analisi del traffico così come delle intercettazioni dello stesso. Nella maggior parte dei casi i route leak sono dovuti a errori di configurazione.

Anziché ignorare il BGP leak, China Telecom ha immediatamente assunto le connessioni dirottando il traffico di un numero elevato di reti mobili europee sulla propria rete. Ciò è avvenuto in contrasto con la prassi di filtraggio del Border Gateway Protocol (BGP) impiegato a livello di ISP per regolare l'istradamento del traffico dati ed evitare la diffusione dei BGP leak.

Tra le reti europee più colpite ci sono stati gestori di telefonia mobile in Svizzera (Swisscom), Francia (Bouygues Telecom, Numericable-SFR) e Olanda (KPN). La durata del dirottamento, oltre le due ore, è ritenuta relativamente lunga dagli esperti. Le ripercussioni sulla comunicazione globale sono state pesanti, con rallentamenti che hanno interessato le connessioni degli utenti delle reti mobili interessate. Durante questo periodo alcuni server non erano affatto raggiungibili. Non è stato chiarito se il dirottamento del traffico dati sia stato intenzionale o sia dovuto a un errore tecnico o umano.

In generale agli Internet Service Provider si consiglia di attenersi agli standard di sicurezza BGP per impedire che si verifichino queste deviazioni del traffico Internet.

4.5.2 Il fornitore di servizi TIC Citycomp ricattato dopo il furto dei dati

Nel mese di aprile 2019 i criminali informatici sono penetrati nella rete di Citycomp, fornitore di servizi per l'infrastruttura TIC.[88] Hanno copiato i dati interni per poi ricattare l'azienda, minacciandola di pubblicare i dati sottratti. L'azienda non ha ceduto al ricatto e così gli aggressori hanno pubblicato la banca dati di 516 GB su siti web appositamente creati. Tra i clienti colpiti figurano alcune filiali di aziende prestigiose come Oracle, Volkswagen o Airbus. Sono stati diffusi anche dati relativi alle aziende svizzere.

I pirati informatici hanno ricattato solo il fornitore di servizi e non i suoi clienti, poiché questi non erano ritenuti responsabili del «pessimo sistema di sicurezza» dell'azienda. Nel suo comunicato[89] Citycomp ha affermato di non aver ceduto a nessuna richiesta dei ricattatori e di aver avviato una collaborazione con specialisti esterni per risolvere il problema. Ha inoltre

86 https://www.thousandeyes.com/learning/glossary/bgp-route-leak

87 https://en.wikipedia.org/wiki/Black_hole_(networking)

88 https://www.vice.com/en_us/article/d3np4y/hackers-steal-ransom-citycomp-airbus-volkswagen-oracle-valuable-companies

89 https://www.citycomp.de/unternehmen/stellungnahme.html

comunicato di aver informato in modo trasparente i clienti e le pertinenti autorità per la protezione dei dati e che sono in corso indagini da parte della direzione della polizia criminale del Baden-Württemberg.

Raccomandazione

La perdita dei dati può verificarsi anche al di fuori dei vostri sistemi. I dati sensibili della vostra azienda possono essere archiviati anche presso i vostri fornitori e clienti. È bene assicurare a livello contrattuale che anche i vostri partner impieghino misure di sicurezza e procedure simili alle vostre per prevenire gli attacchi e porvi rimedio. Questo può implicare un ulteriore controllo, ma aiuta a evitare le brutte sorprese.

4.6 Crimeware

La parola crimeware è composta da crime (criminale) e software. Denota un gruppo di software nocivi impiegati a scopi criminali. I seguenti grafici non offrono una panoramica completa del malware in Svizzera, bensì mostrano la tendenza nel settore del crimeware: da un lato tramite le ondate di malspam, osservate da MELANI insieme ai team addetti alla sicurezza delle infrastrutture critiche, e dall'altro lato tramite i dati di DNS sinkhole.[90]

Nella prima metà del 2019 hanno destato molta preoccupazione gli ingenti danni provocati dagli attacchi di ransomware mirati (si veda il tema principale al cap. 3). In questi casi, i dati di accesso delle aziende, rubati tramite Emotet, sono stati rivenduti e utilizzati dagli aggressori per ottenere un primo accesso nella rete aziendale, da cui è partita una propagazione laterale.

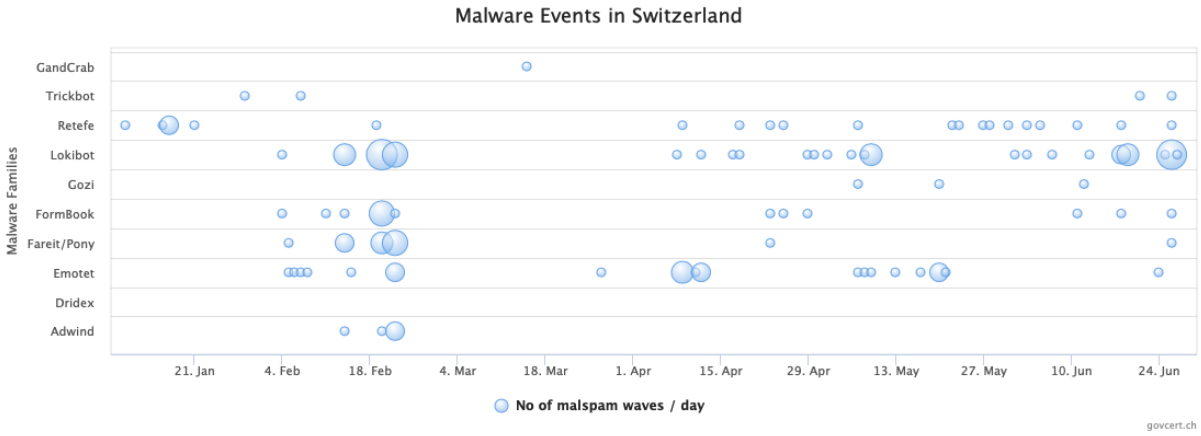

Figura 5: Ondate di malspam osservate

È nettamente visibile la grande quantità di ondate LokiBot così come la costante attività di Retefe. Emotet è leggermente sottorappresentato nel grafico, perché MELANI segue le diverse ondate nel loro complesso, anziché singolarmente.

Emotet ha rappresentato una grande minaccia nel periodo oggetto del rapporto perché gli aggressori hanno iniziato già lo scorso anno a rivendere bot infettati nelle aziende. Emotet rappresenta dunque un varco di accesso per attacchi mirati di ransomware (cfr. anche

[90] Con l'aiuto del DNS sinkholing è possibile dirottare sull'infrastruttura di organizzazioni di sicurezza il traffico verso i domini utilizzati a scopi criminali, cambiando la registrazione dei domini.

cap. 3.4.1). Pur non contenendo alcuna banca svizzera nei propri file di configurazione, Trickbot è spesso utilizzato in una seconda fase, successiva all'infezione iniziale con Emotet. La modularità di Trickbot è vantaggiosa per l'aggressore. Trickbot dispone di vari moduli, ad esempio per il furto dei dati di accesso o per la diffusione con l'aiuto della falla EternalBlue (vulnerabilità nel protocollo SMB).

Nel periodo in rassegna, oltre agli attacchi mirati di ransomware si sono verificati anche molti casi di attacchi non mirati, spesso eseguiti con GandCrab. In questi casi i file sul dispositivo sono stati codificati direttamente dopo l'esecuzione di un allegato.

Anche Retefe è stato abbastanza attivo ed è stato propagato dagli aggressori mediante ondate di malspam con svariati temi. A seconda della loro forma, le ondate erano rivolte talvolta contro le aziende, talvolta contro gli utenti finali.[91] Dal punto di vista tecnico Retefe è stato diffuso in larga misura tramite e-mail con un documento di Word allegato. Le e-mail utilizzavano spesso nomi di aziende o organizzazioni note per apparire credibili. Il codice attivo integrato nel documento di Word permetteva l'installazione di vari componenti sul dispositivo della vittima, come ad esempio un certificato root, per evitare la visualizzazione di avvisi sui certificati nel caso dell'attacco «man-in-the-middle», un SOCKS per l'uso dei servizi proxy e un tor client per deviare il traffico verso le piattaforme di e-banking. In aggiunta Retefe cambiava le impostazioni del browser (impostazioni proxy) per poter dirottare il traffico. Al primo tentativo di login sulla piattaforma di e-banking, Retefe tentava di indurre l'utente a installare sul proprio dispositivo mobile un'ulteriore app che serviva a carpire il secondo fattore di autenticazione.

MELANI raccoglie le informazioni sui dispositivi infettati in Svizzera e le diffonde agli Internet Service Provider e alle infrastrutture critiche. Il grafico seguente mostra il numero attuale di dispositivi infettati per ogni famiglia di malware, resi innocui tramite il DNS sinkholing:

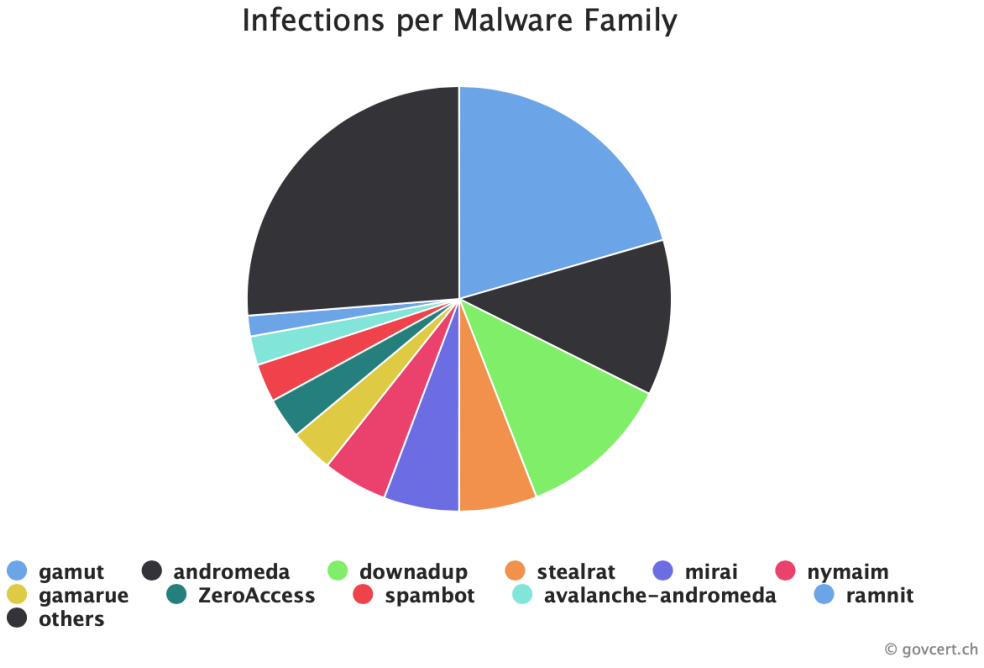

Figura 6: Diffusione di software nocivi noti a MELANI in Svizzera. La data di riferimento è il 30 giugno 2019. I dati attuali sono disponibili su: http://www.govcert.admin.ch/statistics/malware/

[91] Diffusione del malware tramite ingegneria sociale, cfr. cap 4.4.6.

È interessante il fatto che circa il 20 per cento delle infezioni riguardi lo spambot Gamut. Al secondo posto si trova Andromeda, un malware dropper che aiuta a installare altri software dannosi. Una parte notevole delle infezioni è tuttora dovuta a Downadup (noto anche come Conficker), un verme informatico attivo dal 2008.

5 La situazione a livello internazionale

5.1 Spionaggio

5.1.1 Sviluppi degni di nota

Nel semestre oggetto del rapporto sono stati scoperti numerosi attacchi di ciberspionaggio, in larga misura grazie ai rapporti e alle analisi delle aziende di sicurezza. Considerando le numerose segnalazioni, la diversità degli obiettivi, l'ingegnosità e le nuove tecniche degli attacchi, non è facile ottenere un quadro generale.

Per questo spesso si tenta di circoscrivere gli attacchi a determinati gruppi di aggressori o a certe regioni. Questa attribuzione[92] presenta delle difficoltà, perché spesso vi sono sovrapposizioni tra gruppi o campagne. Ad esempio le più recenti analisi di Kaspersky evidenziano che i gruppi noti per attacchi distinti Sofacy e Sandworm mostrano numerose similitudini e che in parte lavorano dalla stessa infrastruttura.[93] Per rendere le cose ancora più complicate, vengono usate le cosiddette «false flag» (false bandiere), con le quali gli aggressori vogliono coprire le loro tracce e indurre un'errata attribuzione. Ad esempio, nelle attività di Muddy Water sono state scoperte false flag, come parti di codice scritte in cinese. Tuttavia, la responsabilità sembra ricadere su un gruppo iraniano, molto attivo nel periodo in esame, che oltre ai tradizionali obiettivi nel Vicino Oriente ha preso di mira organizzazioni in Asia e Europa.[94]

In definitiva, in merito all'attribuzione si pone la questione delle peculiarità di un aggressore: quale elemento è così specifico dell'aggressore da permettere l'attribuzione? I mezzi tecnici utilizzati dall'aggressore soddisfano sempre meno questo criterio. Molti gruppi utilizzano oggi una varietà di strumenti apertamente disponibili per accedere a una rete o spostarsi al suo interno. Si pensa ad esempio a prodotti open source come lo strumento di penetration test Metasploit, l'ID collector Mimikatz o a degli strumenti rubati come l'exploit EternalBlue. La varietà di strumenti utilizzati in un attacco permette ai gruppi di rimanere agili e di impiegare le loro tecniche in base alle necessità in momenti specifici. Ne è un esempio l'arsenale impiegato dal gruppo Emissary Panda[95] nel 2019 in svariati attacchi contro i governi del Vicino Oriente. Strumenti propri sono stati impiegati con parsimonia e soltanto in precise situazioni. L'identificazione di un gruppo sulla base degli strumenti utilizzati è difficile se tutti i gruppi utilizzano le stesse tecniche.[96] A ciò si aggiunge che la cerchia dei potenziali aggressori si è notevolmente ampliata grazie alla maggiore disponibilità di strumenti reperibili in rete.

---

92 Qui è intesa l'attribuzione pubblica con indicazione ufficiale del nome dell'aggressore.

93 https://securelist.com/zebrocys-multilanguage-malware-salad/90680/

94 https://documents.trendmicro.com/assets/white_papers/wp_new_muddywater_findings_uncovered.pdf

95 https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/

96 Altri elementi tecnici come l'infrastruttura utilizzata (IP, domini) possono completare l'attribuzione.

Può sorprendere che l'attribuzione pubblica, in particolare dei governi, sia così diffusa,[97] sebbene l'assegnazione basata su elementi tecnici diventi sempre più incerta. Tuttavia ci sono altri elementi su cui basare l'attribuzione, come la risposta alla domanda «Cui bono: chi ne beneficia?». Gli obiettivi politici ed economici delle grandi potenze sono per lo più noti (a volte anche nell'ambito di strategie pubbliche) e gli interessi che stanno dietro un attacco sono spesso riconoscibili.

Per quanto affascinanti e complesse possano essere queste attribuzioni, sono di scarso aiuto per le aziende e gli utenti bersaglio degli attacchi: al massimo possono adattare la loro valutazione dei rischi alla luce degli interessi noti o sospetti degli Stati che conducono tali campagne di spionaggio. Ma per la vittima non è importante sapere chi è l'aggressore, quanto piuttosto riconoscere le proprie vulnerabilità e rendersi conto di come possono essere sfruttate. In questo senso, il numero e la varietà di strumenti disponibili non rappresenta una notizia positiva. Ogni aggressore ha infatti un enorme arsenale di strumenti a sua disposizione.

La protezione e la difesa degli obiettivi è resa più difficile dal fatto che gli attacchi sono effettuati anche attraverso elementi compromessi esterni ai bersagli. La catena di fornitura (supply chain) è da tempo al centro dell'attenzione.[98] Ne sono un esempio le attività del gruppo di spionaggio informatico APT10, attribuito alla Cina, che ha preso di mira i grandi Managed Service Provider (MSP).[99] Nel periodo in rassegna sono stati pubblicati vari articoli per la maggior parte inerenti temi già noti.[100] Anche un software utilizzato in ambito aziendale può essere vittima e veicolo di un'infezione, come nel caso del software tedesco di manutenzione remota TeamViewer. Nel maggio 2019 l'azienda ha ammesso un attacco risalente al 2016 le cui conseguenze sono di difficile valutazione.[101] Un altro esempio di attacco alla catena di fornitura è quello scoperto nel marzo 2019 a scapito degli utenti di dispositivi ASUS.[102] Pare che il codice dannoso sia stato diffuso tramite la funzione di aggiornamento automatico ASUS. L'attacco ha interessato un numero (sconosciuto) di dispositivi identificati tramite il loro indirizzo MAC. In questi casi gli utenti sono impotenti. Gli update del produttore del dispositivo sono urgentemente raccomandati proprio per motivi di sicurezza. Nel periodo oggetto del rapporto si sono verificati ulteriori attacchi tramite infrastrutture esterne che hanno compromesso il DNS. Essi saranno descritti dettagliatamente nel capitolo successivo.

5.1.2 DNS hijacking: guida all'agguato

Il Domain Name System (DNS) assicura che gli utenti Internet che contattano un dominio come www.melani.admin.ch siano collegati all'indirizzo IP del relativo server (ad es. 162.23.128.232). Nel mese di gennaio 2019 US-CERT[103] ha messo in guardia contro i tentativi

---

97 Negli ultimi anni gli USA o i suoi alleati hanno ufficialmente attribuito, ad esempio, NotyPetya alla Russia, Wannacry alla Corea del Nord e APT10 alla Cina. Cfr. anche cap. 4.1.4.

98 Trattato nell'ultimo rapporto semestrale 2018/2, capitoli 3 e nel presente rapporto al cap. 5.3.1.

99 MELANI rapporto semestrale 2017/1, capitoli 5.1.1 e 2018/2, capitoli 5.1.1.

100 https://uk.reuters.com/article/uk-china-cyber-cloudhopper-special-repor/special-report-inside-the-wests-failed-fight-against-chinas-cloud-hopper-hackers-idUKKCN1TR1DC

101 https://www.zdnet.com/article/chinese-cyberspies-breached-teamviewer-in-2016/

102 https://www.vice.com/en_us/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers

103 https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign

di penetrare nell'infrastruttura DNS e di modificarne i dati, in modo da deviare il traffico dei visitatori dei domini sui sistemi controllati dagli aggressori.

Talos, il reparto di sicurezza di Cisco, ha riferito di una variante denominata «DNSpionage»[104]. Da un lato è stato rilevato il malware omonimo contro gli utenti di computer Windows e dall'altro sono stati riscontrati reindirizzamenti a livello di rete contro obiettivi in Libano e negli Emirati Arabi Uniti. Controllando le registrazioni DNS, gli aggressori hanno potuto anche rilasciare certificati SSL validi per i loro server, per reindirizzare così anche il traffico crittografato.

Una panoramica più completa delle attività di dirottamento dei DNS è stata presentata dal fornitore di servizi di sicurezza FireEye[105] nel gennaio 2019. I ricercatori citano tre diverse varianti impiegate per manipolare le interrogazioni DNS di obiettivi in Medio Oriente, Nord Africa, Europa e Nord America. Gli aggressori hanno tentato soprattutto di estrarre dal flusso di dati reindirizzato ulteriori dati di accesso a sistemi come la posta elettronica e file server, per potervi poi accedere come utenti apparentemente legittimi.

Alla fine di gennaio 2019, l'azienda di sicurezza informatica Crowdstrike[106] ha confermato i metodi di attacco descritti e ha indicato i settori della pubblica amministrazione, dell'aviazione civile, dei fornitori di servizi Internet e dei fornitori di infrastrutture di rete tra gli obiettivi delle campagne di attacco che risalgono fino al 2017.

Nell'aprile 2019, Talos ha riferito di un altro gruppo, identificato con il nome di Sea Turtle[107], impegnato in attività simili contro l'infrastruttura DNS. Tra le vittime vi sono organizzazioni di sicurezza nazionale, ministeri degli esteri e note organizzazioni del settore dell'energia, nonché i loro fornitori di servizi DNS, come le società di registrazione o i fornitori di telecomunicazioni, che sono serviti da trampolino di lancio per gli attacchi contro i loro clienti. In una relazione successiva Talos[108] menziona tra le vittime anche l'organo di registrazione greco, che gestisce l'assegnazione dei domini «.gr». Gli attacchi si sono diffusi contro società dell'energia, think tank, organizzazioni non governative e contro almeno un aeroporto. Anche i fornitori di servizi e le organizzazioni in Svizzera devono fare i conti con gli attacchi di Sea Turtle, sia come mezzi attraverso i quali raggiungere il bersaglio finale sia come obiettivi diretti.

A seguito di questi attacchi, il massimo organo regolatore di Internet, ICANN, ha lanciato un appello per l'implementazione generale delle Domain Name System Security Extensions (DNSSEC).[109] Si tratta di un insieme di standard Internet che aggiungono meccanismi di sicurezza al DNS per garantire l'autenticità e l'integrità dei dati e respingere gli attacchi.

L'Amministrazione federale approva questi standard e ha introdotto le estensioni DNSSEC per tutti i suoi siti web.

---

104 https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html

105 https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

106 https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/

107 https://blog.talosintelligence.com/2019/04/seaturtle.html

108 https://blog.talosintelligence.com/2019/07/sea-turtle-keeps-on-swimming.html

109 https://www.icann.org/news/announcement-2019-02-22-en

5.2 Sistemi di controllo industriali

5.2.1 Sistemi di controllo dell'approvvigionamento energetico sempre nel mirino in caso di conflitto armato

Il 14 giugno 2019 Dragos, società di sicurezza specializzata in sistemi di controllo industriale, ha pubblicato un articolo sul proprio blog relativo alle attività di un gruppo chiamato Xenotime e al suo software nocivo Triton/Trisis, rivolto contro i sistemi di sicurezza industriale.[110] Secondo un rapporto di FireEye del 23 ottobre 2018, il malware sarebbe stato sviluppato da cibercriminali russi.[111]

Il rapporto di Dragos evidenzia che dalla metà del 2018 è stato osservato un incremento delle attività del gruppo nei Paesi europei e soprattutto negli Stati Uniti. Anche se si ritiene che nessun impianto sia stato compromesso, il gruppo ha continuato a svolgere attività di ricognizione. In particolare, Xenotime ha ampliato il target.[112] Il software maligno Triton/Trisis, ad esempio, è stato utilizzato sia nel settore dell'approvvigionamento e della produzione di energia elettrica sia in una raffineria di gas e petrolio.

Il 15 giugno 2019 il New York Times ha pubblicato un articolo su una possibile infezione malware causata dall'US Cyber Command (USCYBERCOM) ai danni della rete elettrica russa.[113] Queste operazioni sono state progettate negli ultimi anni non solo per dare agli Stati Uniti un vantaggio in caso di conflitto, ma soprattutto come deterrente alle operazioni informatiche russe contro gli Stati Uniti.

I rapporti indicati indicano che l'interesse statale per le infrastrutture critiche continua, soprattutto nel settore energetico[114] e gli operatori devono proteggere ulteriormente le loro reti e aumentare la propria capacità di reazione agli attacchi informatici.[115] Sul sito web dell'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) trovate lo standard minimo per garantire la sicurezza TIC nell'approvvigionamento elettrico.[116]

5.2.2 Lo spoofing GPS disturba i piloti nello spazio aereo israeliano

Da quando nella maggior parte degli smartphone è installato un sensore GPS, moltissime persone si affidano all'orientamento satellitare per spostarsi a piedi, in auto o in altro modo. Come accennato nel capitolo 4.2.2, anche per i piloti dei velivoli le coordinate GPS sono fondamentali per la rotta di volo. Nel mese di giugno 2019, molti piloti si sono lamentati dell'

---

110 https://dragos.com/blog/industry-news/threat-proliferation-in-ics-cybersecurity-xenotime-now-targeting-electric-sector-in-addition-to-oil-and-gas/, cfr. anche MELANI rapporto semestrale 2017/2, cap. 5.3.2.

111 https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

112 https://www.wired.com/story/triton-hackers-scan-us-power-grid

113 https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

114 Cfr. anche MELANI, rapporti semestrali 2015/2 cap. 5.3.1 e 2016/2 cap. 5.3.1.

115 Cfr. studio di Electrosuisse citato nel cap. 4.2.1.

116 https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards/minimalstandard_strom.html (disponibile solamente in tedesco)

inaffidabilità dei segnali GPS in avvicinamento all'aeroporto di Ben Gurion vicino a Tel Aviv.[117] L'Unione piloti israeliani ha ritenuto che la causa delle posizioni erroneamente visualizzate fosse un attacco di spoofing.

Le autorità di sicurezza israeliane hanno localizzato la fonte del segnale nella base aerea siriana di Khmeim e ritengono che i responsabili siano i sistemi russi di guerra elettronica. La base si trova a circa 350 km a nord di Ben Gurion ed è utilizzata intensamente dall'aviazione russa per sostenere il regime siriano. Se le accuse sono corrette, diventa chiara la potenza di cui devono disporre i sistemi di guerra elettronica russi per poter ottenere l'effetto descritto su tale distanza.

L'ambasciatore russo in Israele ha immediatamente smentito le accuse non ritenendole serie e liquidandole come fake news.[118]

5.2.3 Il telecomando controllato a distanza

Le enormi gru che trasportano carichi pesanti nei cantieri non sono sempre pilotate dalla cabina ma a volte vengono dirette da terra tramite una piccola barra di comando. Questi radiocomandi vengono utilizzati, oltre che nei cantieri, anche nel settore della logistica e negli impianti di produzione.

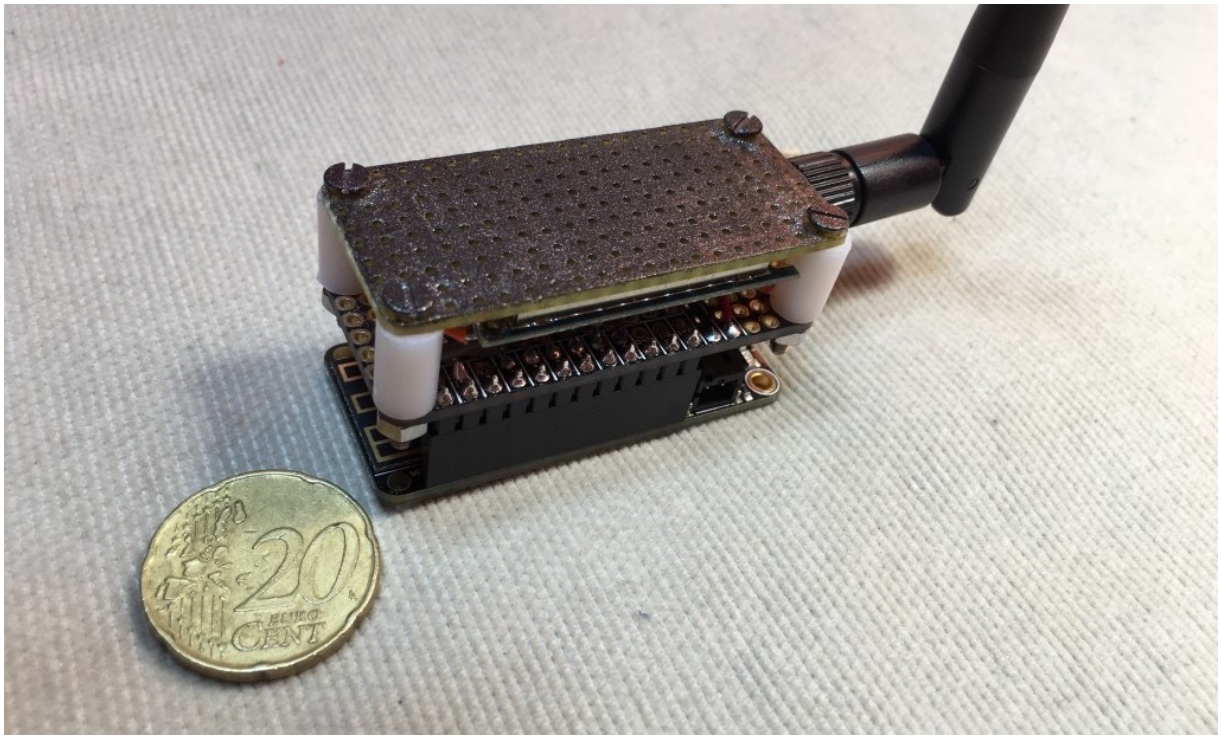

Figura 7: Confronto delle dimensioni del modulo radio RFQuack

[117] https://www.gpsworld.com/israel-accuses-russia-of-spoofing-in-its-airspace/

[118] https://www.bbc.com/news/technology-48786085

In un'analisi,[119] l'azienda di sicurezza giapponese TrendMicro è stata in grado di dimostrare che attraverso questa interfaccia radio è possibile sferrare attacchi, manipolando ad esempio i comandi. In questo caso il presupposto per un attacco riuscito è che l'aggressore sia fisicamente vicino al bersaglio, in modo che i segnali raggiungano il dispositivo attaccato. Per evitare di doversi trovare nelle vicinanze, gli aggressori possono collocare un piccolo trasmettitore nel raggio del sistema telecomandato e controllarlo a distanza via Wi-Fi o radio mobile. Per dimostrare la plausibilità della minaccia, i ricercatori hanno sviluppato RFQuack, un radiodispositivo tascabile alimentato a batteria (vedi figura sopra).

Raccomandazione

Per proteggersi al meglio da tali scenari di attacco, gli analisti raccomandano di studiare attentamente la documentazione del telecomando da acquistare. È necessario assicurarsi che i dispositivi offrano un meccanismo di collegamento configurabile, detto «pairing». Altre misure consistono nell'utilizzare il computer con cui viene programmato il telecomando non collegati alla rete e, se possibile, impiegare protocolli standard ben studiati come Bluetooth Low Energy.

Conclusione / Raccomandazione

La crescente informatizzazione e messa in rete di oggetti di uso quotidiano di qualsiasi tipo (Internet delle cose) offre molte nuove funzioni e comodità. Tra queste vi sono l'elettronica d'intrattenimento e l'accesso a Internet dall'auto o dall'aero. Tuttavia i rischi ad esse collegati non devono essere ignorati. Le nuove possibilità sono sempre accompagnate da nuovi pericoli di cui si deve tenere conto già in fase di sviluppo (security by design).

DOKU

Lista di controllo delle misure di protezione dei sistemi di controllo industriali:

https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/misure-di-protezione-dei-sistemi-industriali-di-controllo--ics-.html

5.3 Attacchi (DDoS, Defacements, Drive-By)

5.3.1 Piratato il fornitore di servizi informatici WIPRO

Nell'aprile 2019 il giornalista investigativo Brian Krebs ha riferito che il fornitore multinazionale di servizi informatici WIPRO è stato vittima di un ciberattacco.[120] Considerate le attività di gruppi come APT10 che attaccano i Managed Service Provider (MSP) per lo più per spiare i loro clienti, gli esperti temevano il peggio. Anche le analisi più recenti di RiskIQ[121] e

[119] https://blog.trendmicro.com/trendlabs-security-intelligence/demonstrating-command-injection-and-e-stop-abuse-against-industrial-radio-remote-controllers/

[120] https://krebsonsecurity.com/2019/04/experts-breach-at-it-outsourcing-giant-wipro/

[121] https://cdn.riskiq.com/wp-content/uploads/2019/06/Gift-Cardsharks-Intelligence-Report-2019-RiskIQ.pdf

Proofpoint[122] presuppongono un attacco ai clienti dell'azienda, ma per una motivazione diversa. L'aggressore sembra mirare più al guadagno economico che allo spionaggio. Si ritiene che il gruppo sia attivo dal 2015 o 2016 e che per finanziare le proprie attività abbia puntato soprattutto sui buoni regalo (gift cards) delle aziende.

Nella maggior parte dei casi gli aggressori hanno infiltrato le reti delle loro vittime tramite phishing. Secondo RiskIQ hanno utilizzato dei template di Lucy Security, una società con sede in Svizzera operante sul fronte della sensibilizzazione. Ciò non significa necessariamente che l'azienda stessa sia stata compromessa. Gli aggressori hanno anche utilizzato strumenti di attacco liberamente accessibili o, dopo una compromissione iniziale, hanno sfruttato i software dual use esistenti sulla rete della vittima.

Questo attacco dimostra ancora una volta quanto sia reale il rischio di attacchi lungo la catena di fornitura (supply chain). Non è solo durante gli attacchi di spionaggio che gli aggressori tentano di entrare nel sistema target compromettendo i fornitori. Anche altri gruppi di criminali sembrano adottare questo approccio.

5.3.2 Botnet cerca di craccare il server RDP con attacchi brute force

Da anni gli aggressori navigano in Internet alla ricerca di porte aperte o scarsamente protette, da utilizzare come varchi di accesso alle reti. Queste porte sono solitamente assegnate a un servizio o a un protocollo Internet e a volte sono predefinite. Ora per trovare queste «porte aperte» ci sono addirittura dei motori di ricerca che non richiedono particolari conoscenze tecniche. Alcuni di questi varchi sono più popolari di altri. Nel semestre scorso MELANI ha nuovamente accertato numerosi tentativi di scansione dei protocolli RDP.[123] L'impostazione predefinita prevede la porta RDP 3389.

Quando è stato pubblicato l'articolo di SANS[124], la botnet GoldBrute, controllata mediante un unico server *Command & Control*, aveva scansionato 1,5 milioni di server RDP esposti in Internet. La botnet cresce costantemente. Il sistema infetto scarica il botcode e quindi inizia a scansionare in modo casuale altri indirizzi IP sulle porte RDP. Quando il bot ha trovato 80 indirizzi IP per i quali vi è una porta RDP accessibile, li comunica al server di comando, che inoltra a ogni bot un set di indirizzi IP da craccare con un attacco di brute force. Tuttavia, aspetto insolito, il tentativo è effettuato solo con un nome utente assegnato e un'unica password associata, per sfuggire ai radar e non venire riconosciuti dai comuni programmi di sicurezza. I sistemi compromessi dalla porta RDP diventeranno a loro parte dei bot. In teoria, gli aggressori potrebbero anche installare un altro malware, come un ransomware o un software di data mining, con gravi conseguenze per i proprietari del sistema violato.

5.3.3 Novità da Anonymous

Negli ultimi tempi le azioni rivendicate da Anonymous sono diventate poco frequenti. Uno dei motivi potrebbe essere l'arresto di alcuni membri del collettivo a seguito delle azioni precedenti. Nonostante ciò, alcuni eventi, in particolare inerenti la libertà di informazione, hanno mobilitato di nuovo gli attivisti. Come è avvenuto ad esempio per l'arresto di Julian Assange a Londra,

---

122 https://www.flashpoint-intel.com/blog/wipro-threat-actors-active-since-2015/

123 Remote Desktop Protocol: protocollo di rete di Microsoft per l'accesso a distanza ai computer Windows.

124 https://isc.sans.edu/forums/diary/GoldBrute+Botnet+Brute+Forcing+15+Million+RDP+Servers/25002/

che ha scatenato azioni contro gli interessi inglesi ed ecuadoriani. Il fondatore di Wikileaks aveva ottenuto l'asilo presso l'ambasciata dell'Ecuador a Londra nel 2012. In risposta alla revoca dell'asilo e all'arresto nell'aprile 2019, un gruppo, presentatosi come Anonymous, ha pubblicato dati rubati a diversi servizi di polizia inglesi. Pare che tra questi non vi fossero dati personali. Un altro gruppo ha rivendicato a nome di Anonymous attacchi DDoS sui siti web delle autorità britanniche. Anche le autorità ecuadoriane hanno segnalato attacchi DDoS, in particolare sul sito web della banca centrale e del primo ministro.

5.3.4 Attacchi DDoS per bitcoin

È noto da tempo che il successo delle valute virtuali stuzzica i criminali e i furti virtuali tendono ad aumentare. MELANI ha già segnalato più volte attacchi a utenti o piattaforme di tali valute.[125] Più una valuta o un servizio è popolare, maggiore è il rischio di un attacco. Quest'anno è stato colpito il servizio di portafoglio bitcoin Electrum. I suoi utenti sono stati indotti a scaricare una versione manipolata dell'applicazione. A tal fine, gli aggressori hanno posizionato una serie di nodi dannosi nella rete peer-to-peer utilizzata per autorizzare le transazioni. Quando l'utente raggiungeva uno di questi nodi (che funge da server nella rete peer-to-peer), riceveva un messaggio di errore con un link per scaricare un presunto aggiornamento dell'app. In realtà si trattava di un programma maligno con il quale il portafoglio veniva poi svuotato.

Non è tutto. Come reazione alle contromisure dei gestori di Electrum, sono stati effettuati attacchi DDoS sui nodi di rete non compromessi. In caso di irraggiungibilità dei nodi «reali», gli utenti venivano più facilmente reindirizzati ai nodi «fittizi» con l'aggiornamento maligno. In aprile, l'azienda di sicurezza Malwarebytes ha stimato che sono stati rubati in questo modo 771 bitcoin (pari a c. 4 mio. $ US ad aprile).[126]

5.4 Fughe di dati

5.4.1 Hackeraggio di Citrix

Il 6 marzo 2019 l'FBI ha informato la società di software Citrix dell'infiltrazione da parte di criminali informatici internazionali della sua rete interna.[127] A sua volta Citrix ha informato i suoi clienti della furto di dati subito. I dati cui hanno avuto accesso i pirati informatici sono tuttora oggetto di indagini. Secondo Citrix, tuttavia, non ci sono prove che gli hacker abbiano manomesso il software ufficiale Citrix o altri prodotti.

L'accaduto è probabilmente parte di una sofisticata campagna mirata contro governi, imprese militari-industriali, società energetiche, istituzioni finanziarie e operatori di infrastrutture critiche.[128]

---

125 Cfr. in particolare MELANI rapporto semestrale 2017/2, cap. 5.4.3.

126 https://blog.malwarebytes.com/cybercrime/2019/04/electrum-bitcoin-wallets-under-siege/

127 https://www.citrix.com/blogs/2019/03/08/citrix-investigating-unauthorized-access-to-internal-network/

128 https://www.forbes.com/sites/kateoflahertyuk/2019/03/15/who-is-resecurity-the-mysterious-firm-that-blamed-iran-for-the-citrix-hack/; https://www.theregister.co.uk/2019/03/08/citrix_hacked_data_stolen/

5.4.2 Magento: la sicurezza degli shop online

I moduli di espansione vulnerabili (di fornitori terzi) sono attualmente la principale fonte di attacchi al software di e-commerce Magento. Ad esempio una vulnerabilità nel protocollo del database MySQL, documentata da anni, ha permesso ai criminali di integrare del codice dannoso in alcuni shop online. Ciò dimostra quanto sia difficile per chi commercia su Internet mantenere i siti web al riparo da codici dannosi, in quanto anche i moduli di terze parti utilizzati devono essere aggiornati. Questo genera un conflitto di interessi tra la stabilità dell'e-shop e una politica di aggiornamento continuo, anche perché Magento non offre un modo standardizzato di notifica sui rilasci critici da parte di terzi.

5.4.3 Data leak a Panama

I ricercatori in materia di sicurezza hanno scoperto un server Elasticsearch non protetto su cui erano memorizzate informazioni personali di quasi il 90 per cento dei panamensi. I dati esposti includevano nomi completi, date di nascita, numeri di passaporto, numeri di assicurazione sanitaria e altre informazioni personali. Il database conteneva anche 3,4 milioni di record di cittadini panamensi che venivano chiamati «pazienti». CERT-Panama ha protetto la banca dati subito dopo aver ricevuto la segnalazione. Tuttavia, non è più possibile determinare se qualcuno abbia avuto accesso ai dati durante il periodo in cui non erano protetti.

5.4.4 Milioni di dati di Facebook trovati sul cloud server di Amazon

I ricercatori in materia di sicurezza hanno trovato ancora una volta innumerevoli dati degli utenti di Facebook pubblicamente visibili sui server di cloud computing di Amazon.[129] La scoperta più recente dimostra che, anche un anno dopo lo scandalo Cambridge Analytica, i dati degli utenti di Facebook sono ancora poco sicuri e ampiamente disponibili online. Il fatto è che per anni Facebook ha contrattualmente reso i dati relativamente disponibili a chiunque integrasse il social network nel proprio servizio. Questa pratica è stata interrotta solo di recente. Le scoperte dimostrano, tuttavia, che le aziende che accedono ai dati di Facebook attraverso i contratti sono troppo poco attive nel campo della protezione dei dati. Dopo diversi scandali, è legittimo avanzare dei dubbi sulla sicurezza dei dati degli utenti su Facebook così come sulla trasparenza nella gestione degli stessi in rapporto al singolo utente. Tuttavia, questo non è un problema specifico solo di Facebook. In tempi di BigData e di automazione, questo argomento è più attuale che mai, perché l'analisi dei record permette di trarre conclusioni considerevoli. Gli utenti sono invitati a riflettere sulla loro presenza nel mondo digitale e sulla pubblicazione dei dati personali. L'esempio più recente mostra in modo impressionante come i problemi di sicurezza e il controllo dei dati siano stati aggravati da un'altra tendenza: il passaggio della gestione e della conservazione dei dati prevalentemente dai data center propri ai servizi di cloud computing dei giganti della tecnologia.

[129] https://www.upguard.com/breaches/facebook-user-data-leak

5.5 Vulnerabilità

5.5.1 BlueKeep – La lacuna di sicurezza nel protocollo RDP adatta alla propagazione di un verme

Nel maggio 2019 è stata resa nota una vulnerabilità nel Remote Desktop Protocol (RDP) di Microsoft (BlueKeep nota anche come CVE-2019-0708). Poco dopo che Microsoft ha annunciato la lacuna e ha rilasciato la patch di sicurezza, gli aggressori hanno lanciato attività di scansione automatica per trovare porte RDP aperte.[130] Successivamente hanno tentato un attacco brute force (provando con password semplici, deboli o già note) per accedere ai sistemi e sfruttarne la vulnerabilità.

La lacuna di sicurezza consente di eseguire il codice tramite accesso remoto. Dato che la vulnerabilità è presente in tutte le versioni da Windows 2000 a Windows 7, compresa la Windows Server 2008 R2, è stata classificata come molto critica. Le versioni più recenti (Windows 8 e 10) non ne sono interessate. Microsoft ha rilasciato una patch il 14 maggio 2019 che funziona con tutte le versioni, anche quelle che non sono più supportate da Microsoft perché hanno raggiunto la fine del loro ciclo di vita.

La prerogativa di questa vulnerabilità è il suo comportamento da verme informatico. In altre parole un software dannoso può propagarsi «automaticamente» senza l'interazione umana sui sistemi privi di patch. Ciò potrebbe avere conseguenze devastanti, in quanto molti sistemi sono vulnerabili e non sempre possono essere protetti con patch in modo tempestivo.

Esistono attualmente alcune prove della possibilità di sfruttare questa vulnerabilità. I ricercatori non hanno però diffuso pubblicamente una guida pratica e la lacuna non è ancora attivamente sfruttata dai criminali. Tuttavia, da tempo si è osservato un aumento delle attività di scansione delle porte RDP. Tale scansione delle porte può essere utilizzata per creare un elenco di sistemi vulnerabili, in modo da conoscere già i potenziali obiettivi quando sarà reso disponibile un exploit funzionante. È solo questione di tempo prima che qualcuno realizzi un exploit che non tarderà a diffondersi.[131]

Raccomandazione

Per proteggersi da BlueKeep è assolutamente necessario installare la patch di sicurezza appropriata. Inoltre, MELANI consiglia di disattivare i remote desktop service e le relative porte se non sono strettamente necessari.

L'aumento delle scansioni delle porte RDP è inquietante soprattutto perché esistono molte porte più o meno liberamente accessibili da Internet. Secondo alcuni studi, nei casi di ransomware verificatisi nel primo trimestre del 2019 il varco di accesso più frequente era costituito da porte RDP aperte o mal configurate.[132] Questo accade spesso anche perché né gli utenti né gli amministratori sanno che il servizio è attivato nella loro rete. Ciò significa che gli utenti

130 https://www.zdnet.com/article/intense-scanning-activity-detected-for-bluekeep-rdp-flaw/

131 Questa previsione sembra peraltro realizzata già al termine della redazione di questo rapporto, in quanto Bluekeep è ormai integrato nello penetration tool «open source» Metasploit.

132 https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rdp-security-explained/ssss

sono attaccati attraverso un vettore di cui ignorano l'esistenza e quindi non adottano misure di protezione a tale riguardo. A questo proposito, è essenziale che gli utenti e gli amministratori conoscano le loro reti e sappiano quali servizi e dispositivi sono disponibili per garantire una protezione efficace.

Come descritto sopra, nel capitolo 3, gli effetti del ransomware sono gravi e possono paralizzare completamente un'azienda per diversi giorni. Inoltre gli aggressori possono utilizzare il varco RDP per spostarsi lateralmente nella rete aziendale e quindi avanzare verso obiettivi più interessanti. Pertanto possono rubare, eliminare o crittografare dati importanti e renderli inutilizzabili. In assenza di una soluzione di backup valida e testata, tali dati vengono di solito persi, finché qualcuno non crea un cosiddetto strumento di decrittazione che permette di ripristinare almeno una parte dei dati.

Per evitare un attacco del genere, McAfee dà i seguenti suggerimenti:[133]

Raccomandazioni

- Non consentire connessioni RDP sulla rete Internet aperta; la porta RDP non dovrebbe MAI essere aperta a Internet in quanto vi sono attività di scansione continue e gli utenti sono vulnerabili agli attacchi di denial of service o ai furti degli account;
- usare password complesse perché vi sono molti tentativi di attacchi brute-force sulle porte RDP;
- utilizzare l'autenticazione multifattoriale (ad es. token di sicurezza, invio del codice tramite notifica o verifica biometrica);
- utilizzare RDP gateway per avere più controllo (ad es. per abilitare il login);
- bloccare i nomi utente o gli indirizzi IP che presentano troppi tentativi di login non riusciti;
- utilizzare un firewall per limitare l'accesso;
- usare la crittografia;
- attivare la network level authentication (NLA). Questa misura protegge in larga misura dalla vulnerabilità BlueKeep, in quanto un aggressore dovrebbe effettuare il login con un account valido prima di poterne sfruttare la vulnerabilità;
- limitare i diritti di accesso degli utenti che possono eseguire il login tramite RDP (di solito non tutti gli amministratori hanno bisogno di accesso).

Adottando queste misure correttamente ridurrete significativamente il rischio di attacchi ransomware o di altri attacchi che prendono di mira il protocollo RDP.

5.5.2 Vulnerabilità EXIM in milioni di server di posta elettronica

Exim è un cosiddetto MTA (Mail Transfer Agent), ossia un componente del server di posta elettronica. Si tratta di un software che riceve e invia e-mail. La maggior parte dei sistemi basati

[133] https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rdp-security-explained/ssss

su Unix usano componenti Exim; nei sistemi Debian essi sono installati come software standard.[134,135]

La vulnerabilità ha due componenti: da un lato, gli aggressori locali (insider) possono eseguire comandi di sistema con accesso root, dall'altro, anche gli aggressori che hanno solo accesso remoto possono compiere operazioni simili in presenza di alcune configurazioni non standard.

Questa vulnerabilità è stata attivamente sfruttata dagli aggressori una settimana dopo la sua pubblicazione. I rapporti in merito non concordano sul numero di sistemi vulnerabili esistenti in tutto il mondo al momento della diffusione della lacuna di sicurezza: secondo skyboxSecurity sarebbero interessati più di 3,5 milioni di server. SecureZoo[136] stima che siano più di 4 milioni i dispositivi (c. il 90 % di tutte le installazioni al mondo) che utilizzano la versione vulnerabile di Exim.[137] L'ultima versione di Exim non presenta più questa vulnerabilità. Tutti i sistemi devono essere aggiornati con urgenza alla versione Exim 4.92. Il software Exim è presente nel 57 per cento di tutti i server di posta elettronica. I ricercatori stimano quindi che il potenziale di danno sia immenso.[138]

Valutazione:

Ogni giorno sono pubblicate molte vulnerabilità. Per alcune di queste esiste già una patch di sicurezza al momento del rilascio, per altre non è così. Poiché in un'azienda vengono solitamente utilizzati sistemi e software diversi, può risultare difficile tracciare manualmente tutti i punti deboli relativi all'hardware e al software utilizzati. Gli aggiornamenti dovrebbero quindi essere installati automaticamente, se possibile. Non tutte le vulnerabilità pubblicate sono effettivamente sfruttate dagli aggressori. Tuttavia, esistono vulnerabilità che possono essere sfruttate con relativa facilità: dopo poco tempo sono già integrate negli exploit kit e quindi presentano un potenziale di danno rilevante.

5.5.3 Trasformazione di uno smartphone in una cimice

Nel primo semestre del 2019 sono state rilasciate due vulnerabilità che hanno permesso agli aggressori di trasformare uno smartphone in una microspia. Una è stata scoperta nell'applicazione Facetime e l'altra in WhatsApp.

Per quanto riguarda WhatsApp si è trattato di una cosiddetta vulnerabilità buffer overflow nel modulo VoIP (Voice-over-IP), utilizzato per telefonare con quest'app. La vulnerabilità è stata utilizzata per inviare allo smartphone colpito pacchetti SRTCP[139] appositamente realizzati. Più precisamente era sufficiente effettuare una chiamata WhatsApp manipolata verso lo smartphone di destinazione. Non era neppure necessario che la persona chiamata rispondesse e non veniva neanche visualizzata una chiamata senza risposta. Di conseguenza era

134 https://meterpreter.org/cve-2019-10149-exim-remote-code-execution/
135 https://blog.skyboxsecurity.com/exim-vulnerability/ssss
136 https://www.securezoo.com/2019/06/critical-exim-vulnerability-discovered-and-patched/
137 https://www.cisecurity.org/advisory/a-vulnerability-in-exim-could-allow-for-remote-command-execution_2019-061/
138 https://www.securezoo.com/2019/06/critical-exim-vulnerability-discovered-and-patched/
139 Secure Real Time Control Transport Protocol: https://tools.ietf.org/html/rfc3711

difficile scoprire che lo smartphone era stato compromesso. Pare che la vulnerabilità sia stata scoperta quando un avvocato in Gran Bretagna è rimasto vittima di un simile attacco.[140]

La vulnerabilità in FaceTime è stata individuata casualmente da un giovane. Si tratta di un errore del software nell'app FaceTime per iPhone.[141] La vulnerabilità permetteva, con poche operazioni, di ascoltare le registrazioni della persona chiamata e di vedere le immagini della videocamera anteriore ancora prima che la persona rispondesse alla chiamata. Per la riuscita dell'attacco occorreva che il chiamante si aggiungesse alla chiamata come un'altra persona. Apple ha rilasciato poco dopo una patch di sicurezza per questo bug che ha risolto il problema.[142]

5.5.4 Vulnerabilità Zero-Day di Internet Explorer: irresponsible disclosure

Accade spesso che i ricercatori in materia di sicurezza pubblichino exploit per le vulnerabilità precedentemente segnalate ai produttori di software, per costringerli a rilasciare immediatamente le patch.

È accaduto anche per l'expoit Zero Day di Internet Explorer.[143] Un ricercatore ha informato Microsoft a riguardo, ma quando la società ha comunicato di non avere in programma il rilascio di una patch, il ricercatore ha pubblicato l'exploit insieme a una cosiddetta «proof of concept», nella quale dimostrava la possibilità di rubare file locali e quindi di esplorare a distanza le versioni del programma quando un utente apriva un file MHT[144] preparato (che sui sistemi Windows viene aperto in modo predefinito con Internet Explorer).

I gruppi di criminalità informatica utilizzano spesso i file MHT per lo spear-phishing o la diffusione di malware. È iniziata la sfida tra i criminali che implementano questo metodo e Microsoft, impegnata nel rilascio di una patch adeguata.

Nel caso di queste «irresponsible disclosure» non è possibile affermare in generale se i ricercatori sono semplicemente impazienti o se sussiste effettivamente un problema da parte del produttore. In ogni caso, i produttori di software dovrebbero esaminare seriamente tutte le segnalazioni di vulnerabilità e fornire ai ricercatori in materia di sicurezza un feedback adeguato, indicando anche un orizzonte temporale per l'eliminazione della vulnerabilità.

5.6 Misure preventive e perseguimento penale

5.6.1 Infranta la rete criminale responsabile di GozNym

Il trojan e-banking GozNym era gestito da una rete criminale con una chiara divisione del lavoro e membri distribuiti in differenti Stati (tra cui Georgia, Bulgaria, Ucraina, Moldavia, Kazakistan e Russia). Una complessa operazione di polizia, cui hanno partecipato diversi Paesi e organizzazioni internazionali, ha permesso l'arresto di diversi membri della banda. Tra questi

---

140 https://securityaffairs.co/wordpress/85477/breaking-news/whatsapp-zero-day.html

141 https://www.buzzfeednews.com/article/nicolenguyen/facetime-bug-iphone

142 https://9to5mac.com/2019/01/28/facetime-bug-hear-audio/

143 https://www.zdnet.com/article/internet-explorer-zero-day-lets-hackers-steal-files-from-windows-pcs/

144 Nei file MHT sono salvate le pagine web, compresa la grafica e gli altri elementi integrati.

vi erano sviluppatori di malware, uno specialista per la distribuzione di massa di e-mail, alcuni hacker incaricati delle vere e proprie rapine online delle banche, agenti di riciclaggio del denaro sporco e altre persone con funzioni di supporto. Nel maggio del 2019, dieci membri del gruppo sono stati incriminati a Pittsburgh e sono in corso ulteriori processi in Georgia, Moldavia e Ucraina. Un perseguimento penale è attualmente in corso in Ucraina anche contro il provider di Bulletproof Hosting Service, per aver prestato i propri servizi per più di 20 campagne di malware oltre a GozNym.[145]

5.6.2 Un altro successo contro il finto supporto Microsoft

MELANI ha già riferito nel precedente rapporto semestrale in merito a un'azione di polizia contro la truffa delle finte chiamate di supporto informatico. Allora la polizia indiana era intervenuta in 26 call center da dove erano partite le chiamate in lingua inglese.[146] Nel frattempo è andata a buon fine anche un'operazione della polizia francese,[147] che ha arrestato tre francesi sospettati di essere le menti della truffa. Attraverso la visualizzazione sul computer di messaggi difficili da rimuovere, le vittime erano indotte a credere che il loro dispositivo fosse infetto e a chiamare il presunto supporto Microsoft al numero visualizzato. In un primo momento le tracce hanno portato nel Maghreb in cui si trovavano i falsi operatori del supporto. Ma grazie alle indagini sui flussi di denaro è infine stato possibile identificare i mandanti francesi.

La truffa del falso supporto Microsoft esiste ormai da quasi dieci anni. MELANI non cessa di mettere in guardia i lettori da questo fenomeno.[148] Tuttavia continua a ricevere segnalazioni di questo tipo di truffa, che evidentemente è tuttora attuata con successo e dunque non scomparirà tanto rapidamente. Allo stesso tempo, ci si può attendere che le autorità di perseguimento penale riescano ad arrestare sempre più truffatori.

6 Tendenze e prospettive

6.1 I costi della cibercriminalità

Gli esperti concordano sul fatto che la cibercriminalità sia in costante aumento. Le cause sono ampiamente note: la crescente digitalizzazione di tutte le nostre attività offre un ampio ventaglio di possibilità per la criminalità. Ciò è indiscusso. È invece difficile quantificare questo sviluppo e ancor più difficile stimare i danni per i singoli Paesi o a livello mondiale. La difficoltà maggiore nell'ottenere cifre affidabili risiede nel gran numero di dati sommersi relativi alla criminalità informatica. Sia perché i reati non sempre vengono denunciati o segnalati, sia perché le vittime non riconoscono affatto i reati. Le statistiche sui costi della criminalità informatica

---

145 https://www.europol.europa.eu/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation

146 MELANI rapporto semestrale 2018/2, cap. 5.5.1.

147 http://www.leparisien.fr/faits-divers/cybercriminalite-trois-chefs-d-entreprise-soupconnes-d-avoir-pirate-8-000-francais-31-01-2019-8001474.php

148 https://www.melani.admin.ch/melani/it/home/meldeformular/formular0/meldeformularhaeufigefragen/mich-hat-eine-firma-angerufen-und-gesagt--dass-mein-computer-mit.html; https://www.melani.admin.ch/melani/it/home/themen/fake_support.html

devono quindi essere sempre interpretate con cautela, in quanto spesso si tratta di stime o proiezioni.

Nonostante queste difficoltà, i dati quantitativi sono importanti per gli attori della lotta contro la cibercriminalità e per le autorità politiche competenti, in particolare per la pianificazione di misure adeguate. Questo capitolo riassume alcuni studi sulla criminalità informatica pubblicati nella prima metà del 2019. Le cifre possono fornire informazioni sulla portata dei fenomeni osservati. Confrontando i risultati ottenuti con lo stesso metodo in periodi di tempo diversi, è anche possibile identificare gli sviluppi.

Nello studio «Measuring the Changing Cost of Cybercrime»,[149] presentato a Boston in giugno 2019 in occasione del Workshop on the Economics of Information Security, gli autori confrontano i dati e le stime attuali con quelli del primo studio condotto nel 2012. Sono state effettuate valutazioni sistematiche dei costi dovuti alla criminalità informatica, con particolare attenzione alle frodi. Nei sette anni intercorsi tra gli studi si osserva un cambiamento di paradigma nell'uso delle TIC: i dati sono sempre più memorizzati nel cloud, il laptop è stato sostituito dallo smartphone, Android ha sostituito Windows e le persone vivono sempre più (anche) online e sui social media. Di conseguenza, la metà di tutti i reati patrimoniali (per quantità e somme) sono ora commessi online. Gli autori hanno anche osservato un brusco aumento dei casi di compromissione delle e-mail aziendali (Business E-Mail Compromise, BEC) e dei reati che coinvolgono le criptovalute. È stato inoltre constatato che l'azione penale contro la criminalità informatica non è efficace quanto quella contro i reati patrimoniali tradizionali, pertanto i ricercatori esortano a investire più denaro nel perseguimento penale che nella prevenzione e nell'anticipazione. Difatti, anche se la prevenzione e l'anticipazione sono molto importanti, dal punto di vista finanziario l'ammontare dei danni è ancora troppo elevato.[150]

Per quanto riguarda i ransomware, lo studio afferma che i criminali hanno realizzato profitti per circa 16 milioni di dollari in due anni (2015–2017). Tuttavia, il danno effettivo (compresa la perdita di dati, la perdita di produzione, i tempi di recupero ecc.) è stimato di gran lunga superiore.

Secondo l'OTA (Online Trust Alliance) della Internet Society[151] i cibercriminali hanno adattato le loro attività per migliorare i loro guadagni. I soli attacchi di ransomware hanno causato danni per 8 miliardi di dollari lo scorso anno, ma l'OTA teme che il costo degli attacchi di ransomware salirà a 20 miliardi di dollari entro il 2021 e stima che gli attacchi informatici siano costati in totale più di 45 miliardi di dollari nel 2018.[152,153]

149 https://www.repository.cam.ac.uk/handle/1810/294492

150 https://www.inside-it.ch/articles/54646

151 https://www.internetsociety.org/news/press-releases/2019/internet-societys-online-trust-alliance-reports-cyber-incidents-cost-45b-in-2018/

152 https://www.hackread.com/cloud-hosting-provider-insynq-hit-by-megacortex-ransomware/

153 https://www.finanzen.ch/nachrichten/aktien/internet-societys-online-trust-alliance-reports-cyber-incidents-cost-$45b-in-2018-1028337623

Secondo uno studio di Crowdstrike, il ransomware Ryuk ha fruttato ai criminali più di 3 milioni di euro in quattro mesi, sebbene Ryuk non sia un ransomware inviato in massa, bensì impiegato in modo mirato.[154]

Un altro fenomeno che ha generato grandi guadagni per gli aggressori è il cosiddetto Business E-Mail Compromise (BEC), ovvero compromissione delle e-mail aziendali. Si tratta di ciberattacchi contro le aziende che prevedono l'invio per e-mail di fatture o istruzioni di pagamento. Di solito vengono utilizzati indirizzi e-mail falsificati dei mittenti o account e-mail compromessi dell'ufficio finanze di fornitori e partner commerciali. Negli Stati Uniti, in tre quarti dei casi sono stati compiuti tentativi per trasferire denaro su conti statunitensi. In Svizzera, nella maggior parte dei casi osservati i versamenti dovevano essere effettuati su conti esteri. Queste truffe, tentate e riuscite, segnalate all'FBI nel 2018 si aggirano attorno a una media di 301 milioni di dollari al mese. Se anche solo una minima parte dei destinatari paga le false fatture o esegue gli ordini di bonifico fittizi, gli aggressori fanno comunque buoni affari. Lo studio rileva che la classica frode del CEO (il presunto CEO trasmette all'ufficio finanze un ordine di pagamento urgente)[155] è in calo e gli ordini di pagamento contraffatti sono sempre più spesso effettuati a nome di persone esterne (clienti, fornitori ecc.). A volte vengono hackerati gli account di posta elettronica di persone esterne, ma a volte il loro indirizzo è semplicemente oggetto di spoofing, cioè falsificato e non compromesso. Le BEC rappresentano un'attività lucrativa perché i profitti sono piuttosto elevati, a fronte di rischi e costi relativamente bassi.[156]

Un altro studio proviene dall'azienda di sicurezza informatica Positive Technology[157] e tenta di descrivere i costi che gli aggressori devono sostenere per realizzare un attacco APT. Le APT sono campagne condotte da attori sponsorizzati da uno Stato. Essi possono anche operare al servizio di Stati finanziariamente deboli. Sulla base degli strumenti di attacco utilizzati, i ricercatori cercano di stimare i costi per l'acquisto o la produzione degli stessi. Gli esperti concludono che un programma per l'invio di spear-phishing (phishing mirato) costa circa 2000 dollari. Va inoltre aggiunto un software di penetration testing che ha un costo compreso tra 8000 e 40 000 dollari. Gli strumenti per un attacco contro una banca costano dunque almeno 55 000 dollari. Una campagna di spionaggio informatico costa invece almeno 500 000 dollari. Queste cifre vanno tuttavia trattate con cautela, poiché i prezzi degli strumenti di attacco variano notevolmente. Lo sviluppo in proprio degli strumenti risulta invece più costoso, poiché in aggiunta occorre pagare per le conoscenze specialistiche degli hacker e degli sviluppatori di software. D'altra parte, ci sono strumenti di attacco che sono legalmente disponibili in commercio che sono utilizzati anche dai penetration tester professionisti. Questi sono di solito più economici e rendono anche più difficile l'attribuzione degli attacchi a specifici APT, poiché gli stessi strumenti sono utilizzati da gruppi o nazioni diverse.

A seguito dei casi degli ultimi anni e della maggiore consapevolezza, sempre più aziende aumentano i loro budget per la sicurezza informatica. Uno studio di ESI ThoughtLab[158] afferma che l'entità media dei danni causati dagli attacchi informatici nell'ultimo anno fiscale è pari a

---

154 https://www.lemonde.fr/pixels/article/2019/01/14/le-rancongiciel-ryuk-a-rapporte-plus-de-3-millions-d-euros-a-ses-auteurs_5408807_4408996.html

155 Cfr. cap. 4.4.5.

156 https://www.fincen.gov/sites/default/files/shared/FinCEN_Financial_Trend_Analysis_FINAL_508.pdf

157 https://www.ptsecurity.com/ww-en/analytics/advanced-persistent-threat-apt-attack-cost-report/

158 https://www.helpnetsecurity.com/2019/07/15/boost-cybersecurity-investments/

4,7 milioni di dollari per vittima, precisando che più di un'azienda su dieci ha perso oltre 10 milioni di dollari. Gli autori dello studio hanno condotto un'indagine presso diverse aziende per scoprire se sono state attaccate e se intendono investire di più nella sicurezza informatica in futuro. A quanto pare, le imprese della maggior parte dei settori aumenteranno notevolmente i loro investimenti nella sicurezza informatica.

Valutazione:

La criminalità informatica è in piena espansione perché spesso permette di arricchirsi con dei metodi relativamente semplici. I cibercriminali non necessitano di un capitale di partenza considerevole né di approfondite nozioni specialistiche, in quanto esistono sempre più metodi d'attacco commercializzati come servizi (*as a service*, *aaS). Così dei gruppi di hacker offrono delle prestazioni secondo il modello RaaS (*ransomware as a service*), che dei delinquenti possono acquistare ed utilizzare pur con limitate capacità specialistiche per realizzare ingenti guadagni o per recare seri danni alle loro vittime.

Uno degli obiettivi della lotta contro la cibercriminalità è di mettere fine a questo modello d'affari. Concreatamene si tratta di aumentare la difficoltà di riuscita di un attacco rendendo i guadagni più incerti e diminuire i profitti. I cibercriminali opportunisti tentano di penetrare in una rete con i mezzi a loro disposizione. Se l'organizzazione presa di mira è sufficientemente protetta e se gli strumenti standard utilizzati non riscuotono in breve tempo il successo sperato, essi andranno rapidamente altrove. Questa constatazione non vale evidentemente per gli hacker sponsorizzati da uno Stato, poiché di solito il loro obiettivo è penetrare in una determinata rete e quindi possono investire anche molto tempo e denaro in un attacco contro un bersaglio specifico.

6.2 Protezione dei dati personali e misure di protezione sociale: qual è il giusto equilibrio?

Sia nella nostra vita privata che in quella professionale utilizziamo quotidianamente tecnologie di crittografia, cosa che fino a qualche anno fa sarebbe stata inimmaginabile. Ad esempio, molti comunicano con WhatsApp, che nella versione attuale utilizza il protocollo di segnale per la crittografia end-to-end delle chat. Ciò significa che i messaggi scritti sono disponibili come testo in chiaro solo sui dispositivi del mittente e del ricevente. Per la trasmissione via Internet, i testi sono crittografati. Come accade per la comunicazione interpersonale, anche i siti web sono sempre più spesso contattati in forma criptata. Le valutazioni dei dati di telemetria dei browser Chrome[159] e Firefox[160] mostrano che in quattro casi su cinque le connessioni stabilite tramite questi browser sono ormai protette da certificati TLS. A questa evoluzione ha contribuito certamente la possibilità per i gestori dei siti web di ottenere gratuitamente i certificati nell'ambito dell'iniziativa Let's Encrypt[161] dell'organizzazione no-profit Internet Security Research Group (ISRG).

159 https://transparencyreport.google.com/https/overview?hl=it

160 https://letsencrypt.org/stats/

161 https://letsencrypt.org/about/

La tendenza verso connessioni criptate più numerose e migliori continuerà ad accentuarsi. L'anno scorso, ad esempio, l'Internet Engineering Task Force (IETF) ha rilasciato la versione 1.3 (TLS 1.3) del protocollo Transport Layer Security.[162] Anche le interrogazioni DNS sono sempre più spesso trasmesse in forma criptata. Mozilla prevede di attivare in via predefinita il protocollo DNS-over-https (DoH) per il suo browser Mozilla Firefox.[163] Nell'attuale versione 9 di Android il protocollo DNS-over-TLS (DoT), se disponibile, è forzato dal sistema[164] e la nuova generazione di telefonia mobile 5G offre una migliore protezione contro le false antenne di telefonia mobile.[165]

Tutti questi ulteriori sviluppi migliorano la riservatezza delle connessioni per gli utenti dei dispositivi, ma limitano taluni meccanismi di protezione consolidati contro contenuti criminali o le possibilità di monitoraggio per il perseguimento penale. Ad esempio, le interrogazioni DNS criptate impediscono agli aggressori di modificarle lungo il percorso di rete, ma a seconda del server contattato, rendono impossibili gli avvisi degli ISP in merito ai siti di phishing o alle pagine che tentano di diffondere un malware. MELANI supporta i gestori di black list, affinché gli utenti di Internet non finiscano su siti di phishing[166] e rivelino involontariamente i loro dati di accesso, ad esempio per l'e-banking. Un problema simile si presenta con la terminazione SSL, dove le connessioni crittografate vengono interrotte su un proxy per filtrare i contenuti dannosi come il malware. I metodi consolidati utilizzati da molte aziende sono resi notevolmente più difficili o addirittura impossibili da TLS1.3.

Soprattutto nel campo del perseguimento penale, l'evoluzione verso una maggiore cifratura è stata spesso oggetto di un acceso dibattito,[167] in quanto i meccanismi di protezione contro i contenuti criminali e di monitoraggio dei criminali facevano affidamento su determinate vulnerabilità dell'infrastruttura. Il problema è che anziché cercare modi per attuare, nell'uso personale della tecnologia, la protezione e la sorveglianza legale senza penalizzare la sicurezza, alcuni attori statali hanno agito vietando nuove tecnologie o prescrivendo l'integrazione di backdoor. Spesso si è sostenuto sommariamente che queste misure non penalizzano la sicurezza degli utenti. Solo di recente al ministero di giustizia americano si è ammesso che le misure proposte per la protezione statale della società non sono possibili senza pregiudicare la sicurezza degli utenti finali.[168]

È dunque possibile discutere in modo trasparente, in un'azienda così come in uno Stato nel suo complesso, quali restrizioni personali possono essere tollerate per ridurre i rischi di natura prioritaria. Un esempio di come la terminazione SSL può essere implementata nel rispetto della protezione dei dati personali è fornito nella checklist per la decrittazione delle connessioni web elaborata dall'organo incaricato per la sicurezza dei dati del Cantone di Zurigo.[169]

---

162 https://www.ietf.org/blog/tls13/

163 https://blog.mozilla.org/futurereleases/2019/04/02/dns-over-https-doh-update-recent-testing-results-and-next-steps/

164 https://android-developers.googleblog.com/2018/04/dns-over-tls-support-in-android-p.html

165 https://www.zdnet.com/article/stingray-spying-5g-will-protect-you-against-surveillance-attacks-say-standards-setters/

166 https://www.antiphishing.ch/it/informazioni/

167 https://www.theregister.co.uk/2019/06/25/andrew_sullivan_internet_society_interview/

168 https://www.schneier.com/blog/archives/2019/07/attorney_genera_1.html

169 https://dsb.zh.ch/internet/datenschutzbeauftragter/de/publikationen/anleitungen/_jcr_content/contentPar/form/formitems/kein_titel_gesetzt__0/download.spooler.download.1562593220478.pdf/Checkliste-Entschluesselung-Webverbindungen.pdf

Tutte le organizzazioni dovrebbero approfittare nel loro ambiente informatico delle nuove tecnologie volte a aumentare la sicurezza dell'infrastruttura dei collaboratori e introdurre solo in modo ponderato restrizioni in questo senso per la protezione contro i contenuti criminali. Insistere su posizioni estreme induce i partecipanti che non concordano con esse ad adottare misure di elusione. Solo con il giusto equilibrio è possibile raggiungere la sicurezza ottimale per tutti nell'Internet del futuro.

6.3 Rischio deglobalizzazione delle catene di fornitura?

Immaginate il seguente scenario: il software di un componente della centralina elettronica del veicolo presenta un errore che in rari casi genera il malfunzionamento dei freni. Per quanto spiacevole, richiamando rapidamente i modelli di varie case automobilistiche che utilizzano questo componente, il problema può essere risolto in soli 15 minuti presso il garage di fiducia con un semplice aggiornamento del software. Resta esclusa dall'update solo una nuova auto ipoteticamente europea, che era stata acquistata, dopo accurate riflessioni, proprio in ragione della sicurezza offerta. Questo perché, a causa di presunti interessi di sicurezza nazionale, il fornitore del veicolo è stato sottoposto nel proprio Paese a un regime di controllo delle esportazioni e purtroppo non è più autorizzato a operare trasferimenti tecnologici con aziende la cui società madre ha sede in Cina.

Sebbene tutto questo possa sembrare artificioso, qualcosa di simile è effettivamente accaduto nella prima metà del 2019 nell'industria delle comunicazioni. Il 16 maggio 2019, il Bureau of Industry and Security (BIS) del Dipartimento del commercio degli Stati Uniti ha emanato una cosiddetta Final Rule, che ha inserito il produttore cinese di TIC Huawei e le sue affiliate in un elenco di organizzazioni, sottoponendo il trasferimento di beni e know-how a queste unità commerciali a un regime di controllo delle esportazioni. Pertanto alle aziende statunitensi è vietato fare affari con queste organizzazioni senza un permesso speciale. Di conseguenza, alcuni giorni dopo Google ha annunciato che non avrebbe più fornito aggiornamenti Android a Huawei nel prossimo futuro e che prima o poi i telefoni cellulari dell'azienda cinese sarebbero stati banditi dall'ecosistema di Google. Poco dopo i produttori di chip Intel, Qualcomm e Broadcomm hanno rilasciato dichiarazioni simili.

La risposta di Huawei alle dichiarazioni dei produttori di chip mirava principalmente a rassicurare i clienti. Il produttore ha infatti spiegato di avere scorte sufficienti di hardware e che per i suddetti disagi disponeva sin d'ora di alternative indipendenti dai produttori USA, così da poter soddisfare le consegne programmate, come quelle per Sunrise in vista della realizzazione dell'infrastruttura di rete 5G. Dato il rischio di esclusione dalla famiglia Android, il produttore cinese di telefoni cellulari ha annunciato ad esempio la possibilità di creare un proprio sistema operativo e quindi un proprio ecosistema.

Con il loro intervento, nel frattempo spostato temporalmente e leggermente smussato, nell'industria nazionale delle TIC,[170] le autorità statunitensi hanno esacerbato fino a livello globale una controversia commerciale fondamentalmente bilaterale, mettendo così in luce anche la vulnerabilità delle catene di fornitura altamente globalizzate, in particolare per quanto riguarda l'industria delle comunicazioni. Se prima la principale minaccia per le aziende e per i clienti al di fuori di USA e Cina poteva essere rappresentata da costi più elevati a causa delle sanzioni reciproche tra i due Paesi, ora anche gli utenti svizzeri dei prodotti e dei componenti Huawei

[170] Cfr. anche MELANI rapporto semestrale 2018/2, cap. 3.

si trovano ad affrontare la questione della garanzia, della durata di funzionamento, della manutenzione e dell'interoperabilità future di questi prodotti. In generale sorge la questione se lo Stato, esercitando un potere di mercato de facto predominante, non abbia creato un precedente per azioni simili in contesti diversi. Le implicazioni di politica economica risultanti dalla sottomissione di Huawei al regime sanzionatorio statunitense sono evidenti. Di conseguenza si pone almeno ipoteticamente la domanda se qualcosa di simile non possa accadere anche contro un produttore indesiderato non cinese, per non parlare delle incertezze per la pianificazione e dei costi che la situazione attuale già comporta.

Le catene di fornitura sono oggi un fenomeno globale, non solo nel settore TIC, ma praticamente in tutta la produzione industriale. Del resto i fornitori non limitano le loro attività a una manciata di Paesi. Ad esempio U-Blox, lo spin-off del Politecnico federale di Zurigo con sede a Thalwil, è un fornitore leader internazionale di componenti di localizzazione ad alta precisione per lo sviluppo e la produzione di veicoli a guida autonoma. Queste catene di fornitura globalizzate ruotano attorno alla possibilità di scambiare, installare e impiegare la tecnologia e il know-how secondo i principi dell'economia di mercato, per realizzare un'ampia gamma di prodotti finali il cui successo o fallimento è determinato dal mercato.

Le perturbazioni di questo sistema colpiscono in prima linea le piccole economie nazionali aperte come la Svizzera, che in mancanza di alternative nazionali dipendono da fornitori stranieri e il cui indotto è costituito da clienti stranieri, in un mercato di domanda e offerta il più possibile aperto e interoperabile a livello globale. Questo per quanto riguarda la pianificazione e la sicurezza degli investimenti così come la possibilità di optare, nell'ambito della gestione del rischio, per una combinazione di componenti (infrastrutturali) provenienti da diverse sfere di influenza statale.

Lo slancio avviato a maggio nasconde il pericolo di una regionalizzazione a medio e lungo termine delle catene di approvvigionamento e può portare in extremis al fatto che la sicurezza di base di alcuni prodotti non è più garantita temporaneamente. O per analogia all'esempio introduttivo: prima che il produttore fornisca una soluzione, c'è comunque soltanto una possibilità su 100'000 che i freni dell'auto nuova non funzioneranno perché un'interferenza nella catena di produzione non permette una soluzione rapida.

7 Politica, ricerca, policy

7.1 Svizzera: interventi parlamentari

Intervento	Numero	Titolo	Depositato da	Depositato il	CN/CS	Dip.	Stato delle deliberazioni e link
Mo.	19.3009	Programma d'incentivazione per la diffusione di progetti di digitalizzazione innovativi nel settore della formazione	CSEC-N	21.2.2019	CN	CSEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193009
Mo.	19.3010	Lancio di un programma per incentivare la digitalizzazione nelle università federali e cantonali, nelle scuole universitarie professionali e nel settore della formazione professionale e della formazione continua	Commissione della scienza, dell'educazione e della cultura (CSEC-N)	21.2.2019	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193010

Intervento	Numero	Titolo	Depositato da	Depositato il	CN/CS	Dip.	Stato delle deliberazioni e link
Ip.	19.3051	Huawei e le sfide del 5G. Rischi e opportunità per la Svizzera	Regazzi Fabio	6.3.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193051
Mo.	19.3121	Trattamento delle fughe di dati a livello nazionale	Buffat Michaël	14.3.2019	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193121
Po.	19.3135	Abbiamo sotto controllo la cibersicurezza nel settore degli acquisti dell'esercito?	Dobler Marcel	18.3.2019	CN	DDPS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193135
Po.	19.3136	Infrastrutture critiche. Abbiamo il controllo sui componenti hardware e software?	Dobler Marcel	18.3.2019	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193136
Ip.	19.3139	Minimizzare i ciber-rischi con addetti alla cibersicurezza	Müller Damian	18.3.2019	CS	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193139
Ip.	19.3185	Acquisti della Confederazione. Nessuna backdoor digitale	Vogler Karl	20.3.2019	CN	DDPS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193185
Po.	19.3199	Aumentare la sicurezza dei dispositivi connessi	Reynard Mathias	21.3.2019	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193199
Ip.	19.3205	Meno dinamismo nella digitalizzazione. Cosa intraprende il Consiglio federale?	Burkart Thierry	21.3.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193205
Ip.	19.3255	Difendere la democrazia liberale dai rigurgiti di antisemitismo e dai venti di estrema destra	Wermuth Cédric	21.3.2019	CN	DFI	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193255
Ip.	19.3267	La prassi del Servizio SCPT in materia di obblighi dei fornitori di servizi di comunicazione derivati è conforme alla legge?	Flach Beat	21.3.2019	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193267
Ip.	19.3321	L'introduzione della tecnologia 5G per la telefonia mobile in Svizzera implica una buona informazione della popolazione da parte della Confederazione	Amman Thomas	22.3.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193321
Ip.	19.3330	I dati dei pazienti saranno venduti al miglior offerente?	Reynard Mathias	22.3.2019	CN	DFI	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193330
Po.	19.3342	Introdurre un sistema di autorizzazioni per gli open government data	Badran Jacqueline	22.3.2019	CN	DFI	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193342

Intervento	Numero	Titolo	Depositato da	Depositato il	CN/CS	Dip.	Stato delle deliberazioni e link
Ip.	19.3377	Differenze cantonali nell'ambito dei procedimenti penali per pornografia infantile. Ancora nessuna necessità di intervento?	Guhl Bernhard	22.3.2019	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193377
Mo.	19.3428	Necessità di ampliare il comitato consultivo «Trasformazione digitale»	Kälin Irène	7.5.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193428
Ip.	19.3431	Vantaggi economici della tecnologia 5G e conseguenze per la salute?	Fiala Doris	7.5.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193431
Mo.	19.3448	Rigetto provvisorio dell'opposizione. Adeguamento alla mutata prassi commerciale (digitalizzazione)	Dobler Marcel	8.5.2019	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193448
Ip.	19.3461	Cibersicurezza. Meglio agire autonomamente o in modo collettivo?	Béglé Claude	8.5.2019	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193461
Ip.	19.3505	Attribuzione delle concessioni per la telefonia mobile 5G senza documentazione di base per le autorità aggiudicatrici	Töngi Michael	9.5.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193505
Ip.	19.3534	5G. Un gruppo di lavoro analizza l'impatto delle onde elettromagnetiche in Svizzera. L'indipendenza dei membri è importante almeno tanto quanto le loro competenze	Borloz Frédéric	3.6.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193534
Ip.	19.3535	Lancio del 5G in Svizzera. Onere supplementare per i Cantoni. Quale compensazione da parte della Confederazione?	Gschwind Jean-Paul	3.6.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193535
Po.	19.3574	Offensiva per un servizio pubblico digitale	Marti Min Li	11.6.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193574
Po.	19.3593	Digitalizzazione delle collezioni naturalistiche per favorire la ricerca svizzera	Germann Hannes	12.6.2019	CS	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193593
Mo.	19.3649	Basi legali per un fondo teso a promuovere la digitalizzazione	Savary Géraldine	18.6.2019	CS	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193649
Ip.	19.3659	Swisscom lancia la piovra di dati Beem. Come è compatibile con la strategia del proprietario della Confederazione?	Marti Samira	19.6.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193659
Mo.	19.3663	Un consiglio digitale, in nome del popolo!	Pardini Corrado	19.6.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193663

Intervento	Numero	Titolo	Depositato da	Depositato il	CN/CS	Dip.	Stato delle deliberazioni e link
Ip.	19.3686	Dichiarazione di Tallinn sull'e-government. Dove si situa la Svizzera e cosa deve fare?	Gruppo liberale radicale	19.6.2019	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193686
Ip.	19.3693	Trasformazione digitale, una grande sfida	Fiala Doris	19.6.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193693
Po.	19.3759	Legge sul credito al consumo. Requisiti formali al passo con l'era digitale	Dobler Marcel	20.6.2019	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193759
Po.	19.3785	L'analfabetismo digitale porta all'esclusione sociale	Reynard Mathias	20.6.2019	CN	DFI	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193785
Ip.	19.3787	Come interviene la Confederazione contro i discorsi d'odio in Internet?	Seiler Graf Priska	20.6.2019	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193787
Po.	19.3850	Come garantire un contributo efficace del settore privato a progetti di sviluppo e promuovere le nuove tecnologie?	Béglé Claude	21.6.2019	CN	DFAE	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193850
Ip.	19.3865	Ginevra internazionale. Come può la Svizzera sostenere lo sviluppo digitale delle organizzazioni internazionali e delle ONG e allo stesso tempo proteggere i dati delle vittime di conflitti?	Derder Fathi	21.6.2019	CN	DFAE	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193865
Ip.	19.3866	Un comando «Cyber» per l'esercito svizzero	Candinas Martin	21.6.2019	CN	DDPS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193866
Po.	19.3878	Il 5G non deve minacciare la neutralità della rete	Béglé Claude	21.6.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193878
Mo.	19.3884	Una strategia per la sovranità digitale svizzera	Derder Fathi	21.6.2019	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193884
Ip.	19.3919	Intelligenza artificiale e trasformazione digitale. Ci vuole una strategia olistica	Ricklin Kathy	21.6.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193919
Iv.pa.	19.417	Riscossione di una tassa sulle piattaforme digitali destinata alla promozione dei media	Töngi Michael	21.3.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20190417
Iv.pa.	19.418	Per un modello di promozione a favore dei media elettronici	Töngi Michael	22.3.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20190418

Intervento	Numero	Titolo	Depositato da	Depositato il	CN/CS	Dip.	Stato delle deliberazioni e link
Dom.	19.5274	Tecnologia 5G: informare e spiegare per superare alcuni pregiudizi presenti nella popolazione	Regazzi Fabio	5.6.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195274
Dom.	19.5286	Antenne 5G. Quali sono i valori limite applicabili?	Schneider Schüttel Ursula	5.6.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195286
Dom.	19.5296	Tecnologia 5G. Quali alternative esistono?	Schneider Schüttel Ursula	5.6.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195296
Dom.	19.5315	Il 5G è già in funzione?	Hardegger Thomas	11.6.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195315
Dom.	19.5349	5G. E ora?	Bigler Hans-Ulrich	12.6.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195349
Dom.	19.5355	5G. Ritardi e costi per l'economia?	Brunner Hansjörg	12.6.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195355
Dom.	19.5370	Beem	Masshardt Nadine	12.6.2019	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195370

7.2 Studio del CSS mette a confronto le strategie nazionali di sicurezza informatica. Le sfide per la Svizzera

Nel marzo 2019 il Center for Security Studies (CSS) del Politecnico federale di Zurigo ha pubblicato uno studio comparativo sulle strategie nazionali in materia di cibersicurezza in Germania, Finlandia, Francia, Paesi Bassi, Israele, Italia e Svizzera, giungendo alle conclusioni illustrate qui di seguito.[171] In generale le strategie di sicurezza informatica hanno molte similitudini a livello concettuale. Sono degni di nota alcuni aspetti chiave quali l'approccio olistico, che comprende sia la sicurezza nazionale sia le questioni socioeconomiche, l'elevata importanza attribuita alla cooperazione internazionale, l'accento posto sulla necessaria cooperazione con il settore privato e la necessità di sensibilizzazione, formazione e informazione ad ampio spettro. Le differenze più importanti riguardano l'inserimento della cibersicurezza all'interno delle strutture statali e l'assegnazione delle competenze. Ciò riguarda in particolare il grado di centralizzazione e il rapporto tra forze civili e militari. Le differenze sono in gran parte dovute alla cultura politica e all'organizzazione dei sistemi politici.

Il CSS ha individuato una serie di sfide nell'ambito dello sviluppo e dell'attuazione delle strategie nazionali. Ad esempio l'integrazione verticale della sicurezza informatica nazionale nel

[171] https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/MELANI%20Studie_final_AW_18März2019.pdf

quadro della sicurezza nazionale e il coordinamento orizzontale dei vari organismi responsabili della cibersicurezza. Inoltre, in futuro i Paesi dovranno occuparsi in misura maggiore della promozione della cooperazione internazionale e dell'elaborazione di standard internazionali di condotta nel ciberspazio. Completano il quadro delle esigenze future la necessità di un'adeguata conoscenza della situazione e la gestione efficiente delle crisi.

7.3 Attuazione della strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)

Negli ultimi due anni il Consiglio federale ha preso decisioni fondamentali per proteggere la Svizzera contro i rischi informatici. Nell'aprile 2018 ha adottato la Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)[172] per gli anni 2018–2022. L'obiettivo principale della SNPC è quello di consentire alla Svizzera di cogliere le opportunità della digitalizzazione rendendola adeguatamente protetta e resiliente contro i ciber-rischi. Da questa visione, la SNPC identifica sette obiettivi strategici, che devono essere raggiunti attraverso 29 misure in un totale di dieci campi d'azione.

A differenza della prima SNPC 2012–2017, il settore della ciberdifesa, che fa riferimento al ruolo dell'esercito e del servizio di intelligence nell'attribuzione e nella prevenzione degli attacchi informatici così come nel garantire la prontezza d'intervento militare, è parte integrante della nuova strategia. Ulteriori innovazioni riguardano l'estensione del gruppo target al complesso economico e sociale (la prima strategia si concentrava sulla protezione delle infrastrutture critiche) e una maggiore attenzione alla standardizzazione e alla regolamentazione, in cui rientra anche la verifica dell'obbligo di notifica. Con questi adeguamenti, la SNPC adempie la propria funzione di strategia globale, tenendo conto della crescente importanza dei ciber-rischi per tutte le aziende e ponendo le basi per l'elaborazione di standard e misure di regolamentazione.

7.3.1 Piano di attuazione e organizzazione della Confederazione nell'ambito dei ciber-rischi

È chiaro che l'ambizioso portafoglio della SNPC può essere attuato con successo solo se il lavoro dei diversi attori coinvolti è coordinato in modo ottimale e se vengono sfruttate tutte le competenze esistenti. Tutti i soggetti coinvolti in seno alla Confederazione, ai Cantoni, all'economia e alle università hanno pertanto elaborato congiuntamente il piano di attuazione[173] della SNPC, che è stato approvato dal Consiglio federale il 15 maggio 2019.[174] Per ogni misura, il piano di attuazione determina quale organizzazione debba attuare specifici progetti ed entro quale termine e costituisce dunque la base per il controllo strategico con cui sarà monitorato lo stato di avanzamento della SNPC.

Contemporaneamente all'elaborazione del piano di attuazione, la Confederazione ha riesaminato e adeguato la propria organizzazione.[175] I principali elementi di questa organizzazione relativamente all'attuazione della SNPC sono illustrati nella figura seguente.

---

172 https://www.isb.admin.ch/isb/it/home/themen/cyber_risiken_ncs/ncs_strategie.html

173 https://www.isb.admin.ch/isb/it/home/themen/cyber_risiken_ncs/umsetzungsplan.html

174 https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-75046.html

175 https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-73839.html

Figura 8: Organizzazione della Confederazione nell'ambito dei ciber-rischi

Elementi importanti della nuova organizzazione sono il rafforzamento del coordinamento interdipartimentale e la collaborazione con l'economia, i Cantoni e le università. Per questi compiti sono stati istituiti i seguenti nuovi organi:

- il **Comitato del Consiglio federale per la cibersicurezza:** vi siedono il capo del Dipartimento federale delle finanze (DFF), del Dipartimento federale di giustizia e polizia (DFGP) e del Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) e ha il compito di vigilare sull'attuazione della SNPC;
- il **Comitato ristretto per la cibersicurezza:** rafforza il coordinamento fra i tre ambiti della sicurezza, della difesa e del perseguimento penale, assicura una valutazione congiunta delle minacce in atto e vigila sulla gestione, da parte dei servizi della Confederazione, degli incidenti gravi avvenuti a livello interdipartimentale;
- il **Comitato direttivo della SNPC (CD SNPC)** assicura l'attuazione coordinata e mirata delle misure definite nella SNPC ed elabora proposte per il suo ulteriore sviluppo.

7.3.2 Il Delegato alla cibersicurezza e il Centro di competenza per la cibersicurezza

Oltre agli organi di coordinamento, con il Delegato federale alla cibersicurezza e il Centro di competenza per la cibersicurezza sono state create due strutture centrali. Il Delegato federale alla cibersicurezza assume la direzione strategica della cibersicurezza all'interno della Confederazione, guida il Centro di competenza così come gli organi interdipartimentali istituiti dalla Confederazione (ad eccezione del Comitato per la cibersicurezza) e rappresenta la Confederazione in altri organi. Questa posizione centrale è stata affidata a Florian Schütz,[176] che ha assunto le sue funzioni nell'agosto del 2019 ed è direttamente subordinato al capo del Dipartimento delle finanze.

[176] https://www.efd.admin.ch/efd/it/home/dokumentation/nsb-news_list.msg-id-75421.html

Il Centro di competenza della Confederazione per la cibersicurezza, aggregato al DFF, è il punto di contatto nazionale per tutte le questioni riguardanti la cibersicurezza. Si basa sull'organizzazione esistente di MELANI e la amplia per offrire servizi a tutta l'economia e fornire al pubblico avvisi e informazioni sui rischi informatici. All'interno della Confederazione supporta gli uffici con cibercompetenze in materia di prevenzione, standardizzazione e regolamentazione. Nella gestione di incidenti legati alla sicurezza assumerà la competenza di impartire istruzioni agli uffici federali.

Con l'adozione del piano di attuazione della SNPC, il Consiglio federale ha parlato anche di risorse per il Centro di competenza per la cibersicurezza, affinché possa adeguatamente ampliare le attività operative esistenti di MELANI a partire dal 1°gennaio 2020.

Una descrizione più dettagliata del Centro di competenza della Confederazione per cibersicurezza e dei suoi compiti sarà pubblicata nel prossimo rapporto semestrale di MELANI.

8 Prodotti MELANI pubblicati

8.1 Blog GovCERT.ch

8.1.1 Gravi attacchi di ransomware contro PMI svizzere

9.5.2019 – Considerato il crescente numero di casi di ransomware che mostrano un modus operandi piuttosto sofisticato, pubblichiamo un avviso tramite la Newsletter MELANI unitamente a questo post nel blog, che documenta i dettagli tecnici dei recenti attacchi di ransomware contro le piccole e medie imprese (PMI) svizzere. L'obiettivo di questo post nel blog è quello di farvi comprendere meglio le varie modalità operative delle più comuni famiglie di ransomware che hanno colpito obiettivi svizzeri negli ultimi mesi.

➔ https://www.govcert.admin.ch/blog/36/severe-ransomware-attacks-against-swiss-smes

8.2 Newsletter MELANI

8.2.1 Sextortion: presi di mira numerosi svizzeri – le autorità lanciano il sito web stop-sextortion.ch

24.4.2019 – In un'e-mail, i dei truffatori affermano di avere accesso a computer e webcam e minacciano di pubblicare foto e video a contenuto sessuale se non viene pagato il riscatto richiesto. Questo genere di truffa è chiamata «fake sextortion» e di solito i criminali esigono il pagamento di un riscatto in bitcoin. Con questa truffa, negli ultimi sei mesi alcuni delinquenti sono riusciti a incassare illecitamente bitcoin del valore di circa 360 000 franchi, nonostante le somme richieste fossero piuttosto esigue. Fino a quando i destinatari di queste e-mail pagheranno il riscatto, tale modo di procedere sarà incoraggiato e continuerà ad essere utilizzato. Aiutateci a fermare questo genere di truffa non pagando più nessun riscatto. Il sito Internet stop-sextortion.ch, lanciato oggi dalle autorità, fornisce informazioni utili e permette di segnalare le e-mail di fake sextortion.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/fake-sextortion.html

8.2.2 Crypto-ransomware: attacchi sempre più mirati alle reti aziendali

9.5.2019 – Dall'inizio del 2019 sono sempre più numerose le PMI e le grandi imprese in Svizzera e all'estero a comunicare che i propri dati sono stati cifrati e resi quindi illeggibili dai cosiddetti «crypto-ransomware». In alcuni casi sono stati cifrati anche i backup, impedendo così il ripristino delle attività delle imprese colpite.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/verschluesselungstrojaner-greifen-vermehrt-gezielt-unternehmensn.html

9 Glossario

Termine	Descrizione
Agente finanziario	È un agente finanziario chiunque svolga legalmente l'attività di intermediario finanziario e quindi anche operazioni di trasferimento di denaro. In tempi recenti questo concetto è utilizzato nel contesto delle transazioni finanziarie illegali.
APT Advanced Persistent Threat	Questa minaccia provoca un danno molto ingente, che si ripercuote sulla singola organizzazione o su un Paese. L'aggressore è disposto a investire molto tempo, denaro e conoscenze nell'attacco e dispone generalmente di notevoli risorse.
Attacchi Supply Chain	Attacco con cui si cerca di infettare l'obiettivo finale infettando precedentemente un'azienda nella catena di fornitura.
Attacchi Watering Hole	Infezione mirata per mezzo di software maligno tramite siti che di preferenza vengono visitati solamente da un gruppo specifico di utenti.
Attacco DDoS	Attacco di Distributed-Denial-of-Service. Un attacco DoS in cui la vittima è attaccata simultaneamente da numerosi sistemi diversi.
Autenticazione a due fattori	L'autenticazione a due fattori è impiegata per accrescere la sicurezza. A tal fine sono necessari almeno due dei tre fattori di autenticazione: 1. una cosa che si conosce (ad es. password, PIN ecc.); 2. una cosa che si ha (ad es. certificato, token, elenco da cancellare ecc.); 3. una cosa che si è (ad es. impronte digitali, scanner della retina, riconoscimento vocale ecc.).
Backdoor	Backdoor (in italiano: porta posteriore) designa una parte del software che consente agli utenti di accedere al computer eludendo le normali protezioni di accesso oppure

Termine	Descrizione
	un'altra funzione altrimenti protetta di un programma per computer.
BGP Border Gateway Protocol	Protocollo di istradamento o «routing» utilizzato in Internet che determina il percorso dei pacchetti dati tra le reti.
Bitcoin	Sistema di pagamento decentrato che può essere utilizzato in tutto il mondo e nome di un'unità di moneta digitale.
Bot	Trae origine dalla parola slava per lavoro (robota). Designa un programma che esegue autonomamente una determinata azione alla ricezione di un comando. I cosiddetti malicious bot possono pilotare a distanza i computer compromessi e indurli a eseguire qualsiasi azione.
Botnet	Una rete costituita da più bot, pilotata tramite un'infrastruttura del tipo «command and control».
Brute Force	Metodo di risoluzione di problemi nei settori dell'informatica, della crittografia e della teoria dei giochi, fondato sulla sperimentazione di tutti i casi possibili.
C2 Command & Control	Infrastruttura di comando e controllo delle botnet. La maggior parte dei bot può essere sorvegliata attraverso un canale di comunicazione e ricevere comandi.
CaaS Cybercrime-as-a-Service	La cibercriminalità come servizio acquistabile consente a criminali tecnicamente poco esperti di svolgere attività illegali in Internet per mezzo di strumenti di facile utilizzo.
CEO-Fraud	Si parla di «CEO Fraud» (truffa del CEO) nel caso di usurpazione dell'identità di un dirigente d'azienda e quando a suo nome si richiede al servizio competente (servizio finanziario, contabilità) di effettuare un versamento su un conto generalmente all'estero.
CPU / Processore	«Central Processing Unit» / processore: unità centrale di un computer, contiene i circuiti logici necessari al funzionamento di un programma per computer.
Cryptomining	Con il mining vengono creati nuovi blocchi che si aggiungono alla blockchain. Il procedimento richiede calcoli molto complessi, pertanto viene retribuito.
Defacement	Deturpamento di pagine web.

Termine	Descrizione
DNS Domain Name System	Con l'ausilio del DNS, Internet e i suoi servizi sono di agevole utilizzazione, in quanto gli utenti al posto dell'indirizzo IP, possono utilizzare un vocabolo (ad es. www.melani.admin.ch).
Dropper / Downloader	Programma che scarica e installa una o più istanze di malware.
Exploit-Kit	Kit che consente a criminali di generare programmi, script o righe di codice mediante i quali è possibile sfruttare le vulnerabilità dei sistemi di computer.
File ZIP	Zip è un algoritmo e un formato di file per la compressione dei file, destinato a ridurre lo spazio di memorizzazione dei file per l'archiviazione e la trasmissione.
GPS Global Positioning System	Il Global Positioning System (GPS), ufficialmente NAVSTAR GPS, è un sistema globale di navigazione satellitare per la determinazione della posizione e la misura del tempo.
Infezione da «drive-by»	Infezione del computer mediante malware unicamente attraverso la consultazione di una pagina web. L'infezione avviene perlopiù per il tramite dell'utilizzo di exploit che sfruttano le lacune nel sistema di sicurezza lasciate scoperte dal visitatore.
Infezione da pagina web	Infezione di un computer con malware unicamente attraverso la consultazione di un sito web. Spesso le pagine web colpite contengono offerte serie e sono state precedentemente compromesse allo scopo di propagare il malware. L'infezione avviene perlopiù per il tramite dell'utilizzo di exploit che sfruttano le lacune nel sistema di sicurezza lasciate scoperte dal visitatore.
Internet delle cose	L'espressione «Internet delle cose» indica che nel mondo digitale il computer è integrato in misura crescente da «oggetti intelligenti», ossia dall'applicazione dell'intelligenza digitale agli oggetti reali.
ISP Internet Service Provider	Gli offerenti di prestazioni Internet forniscono servizi, contenuti o prestazioni tecniche indispensabili per l'utilizzazione o la gestione dei contenuti e dei servizi Internet.
Javascript	Un linguaggio di script orientato sugli oggetti per lo sviluppo di applicazioni. Gli Javascript sono elementi di programma integrati nel codice HTML, che consentono determinate funzioni nel browser di Internet. Ne può essere

Termine	Descrizione
	un esempio il controllo dei dati immessi dall'utente in un modulo web. È così possibile verificare se tutti i caratteri immessi alla richiesta di un numero telefonico corrispondono effettivamente a delle cifre. Come gli ActiveX Control, gli JavaScript sono eseguiti sul computer del visitatore di pagine Internet. Oltre a funzioni utili, è però anche possibile programmare funzioni nocive. Diversamente dagli ActiveX Control, gli JavaScript sono supportati da tutti i browser.
Lacuna di sicurezza	Vulnerabilità dell'hardware o del software, tramite la quale gli aggressori possono accedere a un sistema.
Malspam	Invio di e-mail di massa con cui viene diffuso il malware.
Malware / Software maligno	Termine generico per software che esegue funzioni nocive su un computer. Rientrano tra l'altro in questo gruppo i virus, i vermi informatici e i cavalli di Troia.
Metadati	I metadati o metainformazioni sono dati che contengono informazioni su altri dati.
MITM	Attacco Man-in-the-Middle. Attacco nel corso del quale l'aggressore si insinua inosservato su un canale di comunicazione tra due partner, in modo da essere in grado di seguire o di modificare lo scambio di dati.
MSP Managed Services Provider	Un fornitore di modelli operativi o di soluzioni operative è un fornitore di servizi IT che fornisce e gestisce un insieme definito di servizi per i propri clienti.
NAS Network Attached Storage	Archiviazione collegata alla rete: disco rigido o server di dati collegato direttamente a una rete.
P2P	Peer to Peer. Un'architettura di rete nel cui ambito i sistemi partecipanti possono assumere le medesime funzioni (diversamente dalle architetture cliente-server). Il P2P è sovente utilizzato per lo scambio di dati.
Patch	Un software che sostituisce le componenti di un programma affette da errori, sopprimendo così per esempio una lacuna di sicurezza.
Phishing	Nel caso del phishing i truffatori tentano di accedere ai dati confidenziali di ignari utenti di Internet. Si può trattare per esempio di informazioni sui conti di offerenti di aste online (ad es. eBay) o di dati di accesso a servizi bancari

Termine	Descrizione
	via Internet. I truffatori sfruttano la buona fede e la disponibilità delle loro vittime inviando loro e-mail nei quali l'indirizzo del mittente è falsificato.
Protocollo SMB	Server Message Block (SMB): protocollo per la condivisione in rete di file, stampanti e server in reti di computer.
Proxy	Interfaccia di comunicazione in una rete che funge da intermediario che riceve le richieste da un lato per poi effettuare il collegamento dall'altro lato con il proprio indirizzo.
RaaS Ransomware-as-a-Service	Il ransomware come servizio acquistabile consente a criminali tecnicamente poco esperti di effettuare attacchi per mezzo di strumenti di facile utilizzo.
Ransomware	Malware che nel caso tipico codifica i dati delle vittime per convincerle a pagare un riscatto.
RDP Remote Desktop Protocol	Un protocollo di rete di Microsoft per l'accesso a distanza ai computer Windows.
Remote Administration Tool	Il software di manutenzione a distanza (in inglese: Remote Administration Tool) costituisce un'applicazione nell'ambito del concetto di manutenzione a distanza di qualsiasi computer o sistema di computer.
Router	Apparecchiature del settore delle reti di computer, della telecomunicazione o anche di Internet che collegano o separano più reti di computer. I router sono ad esempio utilizzati nelle reti domestiche per effettuare il collegamento tra la rete interna e Internet.
Script PowerShell	PowerShell è un framework multipiattaforma di Microsoft che consente di automatizzare, configurare e gestire sistemi ed è composto da un interprete a riga di comando (shell) e da un linguaggio di scripting.
Sistemi industriali di controllo (ICS)	I sistemi di controllo e di comando constano di una o più apparecchiature che guidano, regolano e/o sorvegliano il comportamento di altre apparecchiature o sistemi. Nella produzione industriale il concetto di «sistemi industriali di controllo» (inglese: Industrial Control Systems, ICS) è corrente.

Termine	Descrizione
Smartphone	Lo smartphone è un telefono mobile che mette a disposizione una maggiore funzionalità di computer di quella di un telefono mobile progredito usuale.
SMS	Short Message Service. Servizio per l'invio di messaggi brevi (160 caratteri al massimo) agli utenti di telefonia mobile.
Social Engineering	Gli attacchi di social engineering sfruttano la disponibilità, la buona fede e l'insicurezza delle persone per accedere per esempio a dati confidenziali o per indurre le vittime a effettuare determinate operazioni. Una nota forma di social engineering è il phishing.
Software maligno / Malware	Termine generico per software che esegue funzioni nocive su un computer. Rientrano tra l'altro in questo gruppo i virus, i vermi informatici e i cavalli di Troia.
Spam	Il termine spam designa l'invio non sollecitato e automatizzato di pubblicità di massa, definizione nella quale rientrano anche le e-mail di spam. Si designa come spammer l'autore di queste comunicazioni mentre l'invio come tale è denominato spamming.
Spearphishing mail	Attacco mirato di phishing. Si fa ad esempio credere alla vittima di comunicare tramite e-mail con una persona di fiducia.
Spoofing	Falsificazione degli elementi di indirizzo o dei segnali allo scopo di ingannare il destinatario o il dispositivo ricevente.
Take down	Take down (rimozione) è un'espressione utilizzata quando un provider ritira un sito dalla rete a causa della presenza di contenuti fraudolenti.
TCP/IP	Transmission Control Protocol / Internet Protocol (TCP/IP). Famiglia di protocolli di rete anche designata come famiglia di protocolli Internet a causa della sua grande importanza per Internet.

Termine	Descrizione
TLD Top-Level-Domain	Ogni nome di dominio in Internet consta di una successione di serie di caratteri separati da un punto. La designazione Top-Level-Domain si riferisce all'ultimo nome di questa successione e costituisce il livello più elevato della risoluzione del nome. Se ad esempio il nome completo di dominio di un computer, rispettivamente di un sito web, è de.example.com, l'elemento a destra (com) rappresenta il Top-Level-Domain di questo nome.
UDP	«User Datagram Protocol»: protocollo di rete molto semplice, senza connessione, che trasporta datagrammi della famiglia di protocolli Internet.
USB	Universal Serial Bus. Bus seriale che (per il tramite di corrispondenti interfacce) consente il raccordo di periferiche come tastiera, mouse, supporti esterni di dati, stampante ecc. Al momento del raccordo o della disgiunzione di un dispositivo USB il computer non deve essere riavviato. I nuovi dispositivi sono per lo più riconosciuti e configurati automaticamente (a dipendenza però del sistema operativo).
Verme informatico	Diversamente dai virus, i vermi informatici non necessitano di un programma ospite per diffondersi. Essi sfruttano piuttosto le lacune di sicurezza o gli errori di configurazione del sistema operativo o delle applicazioni per diffondersi autonomamente da un computer all'altro.
WLAN	L'abbreviazione WLAN (o Wireless Local Area Network) significa rete locale senza fili.
Zero-Day	Exploit che appare il giorno stesso in cui la lacuna di sicurezza è resa nota al pubblico.