Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Centro nazionale per la cibersicurezza NCSC
Servzio 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 2020/I (gennaio – giugno)

29 OTTOBRE 2020

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

1 Panoramica / Contenuto

2 Editoriale

La ciberdiplomazia svizzera all'insegna della geopolitica digitale

Inviato speciale per la politica estera e di sicurezza in ambito cyber, Jon Fanzun

Jon Fanzun, Inviato speciale per la politica estera e di sicurezza in ambito cyber

Fino a pochi anni fa la cibersicurezza era un tema di nicchia che a livello internazionale veniva discusso quasi esclusivamente da esperti del settore. Oggi la cibersicurezza è parte integrante della politica internazionale ed è oggetto di accese discussioni. Il tema è inoltre di grande attualità poiché le tecnologie digitali svolgono un ruolo centrale nella nostra società dell'informazione altamente sviluppata. Per questo motivo le tecnologie chiave si trovano al centro di conflitti globali.

L'attuale disputa tra Stati Uniti e Cina per le reti 5G è un esempio calzante di come le questioni di politica di sicurezza, economiche e sociali si combinino in una nuova forma di geopolitica. A tale proposito, si può parlare di una «geopolitica digitale», incentrata su una concorrenza non solo tecnologica, ma anche ideologica fra un modello liberale e uno statalista.

In questo contesto, la Svizzera è chiamata a difendere attivamente i propri interessi anche nel ciberspazio. L'ufficio dell'Inviato speciale per la politica estera e di sicurezza in ambito cyber del DFAE assolve questo compito in collaborazione con diversi partner dell'Amministrazione federale, in particolare anche con il Centro nazionale per la cibersicurezza (NCSC). Il corrispondente quadro strategico è definito dall'attuale Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC 2.0), così come dalla strategia di politica estera 2020–2023.

La Svizzera si impegna a favore di un ciberspazio libero, sicuro e aperto, utilizzato per scopi pacifici e basato su regole chiare e fiducia reciproca, sostenendo il principio secondo cui il diritto internazionale debba essere applicato e attuato anche nel ciberspazio. A livello internazionale, inoltre, ci impegniamo per coinvolgere attori rilevanti della società civile e dell'economia. Diamo voce ai nostri interessi e valori presso fori internazionali come l'ONU, l'OSCE e anche l'OCSE. Altrettanto importanti sono i «ciberdialoghi» bilaterali, che, conformemente alla SNPC 2.0, intendiamo ampliare e intensificare con determinati Paesi nei prossimi anni.

Considerando la progressiva formazione di blocchi, il drammatico calo della fiducia fra gli Stati e la conseguente frammentazione del ciberspazio, sarà però difficile ottenere dei progressi nella diplomazia internazionale in questo ambito. Di per sé sarà già complicato consolidare il consenso finora ottenuto, documentato per esempio dal rapporto dello «United Nations Group of Governmental Experts» (GGE) del 2015.

Quando la fiducia scema e i dibattiti si inaspriscono, cresce anche la necessità di mediazione. Sotto questo profilo la Svizzera può far valere i suoi punti di forza a livello diplomatico e la sua credibilità trasferendo la propria esperienza dal mondo offline a quello online. In questo ambito la Ginevra internazionale svolge un ruolo importante. La Svizzera può offrire una cornice dove discutere di cibersicurezza e nuove tecnologie all'insegna della fiducia. Il «Geneva Dialogue

on responsible Behaviour in Cyberspace» è un buon esempio di come la Svizzera possa contribuire concretamente al miglioramento della cibersicurezza coinvolgendo nelle discussioni su questo tema imprese globali come Microsoft, Kaspersky o Huawei.

La ciberdiplomazia è uno sport di squadra. Il coinvolgimento degli attori rilevanti e delle loro competenze è essenziale per dare voce agli interessi della Svizzera sulla scena internazionale. L'unione e il coordinamento delle forze nell'ambito del NCSC generano un valore aggiunto anche per la cibersicurezza internazionale della Svizzera. Desidero quindi ringraziare tutti gli attori coinvolti dei diversi dipartimenti per il loro impegno a favore di un ciberspazio libero, sicuro e aperto.

Jon Fanzun

Una nota sulla nostra attività:

Il rapporto semestrale MELANI esce per l'ultima volta in questa veste; le edizioni successive verranno pubblicate dal Centro nazionale per la cibersicurezza (NCSC). Il 1° luglio 2020, con l'entrata in vigore dell'ordinanza sulla protezione contro i ciber-rischi nell'Amministrazione federale, MELANI è infatti stata integrata nel NCSC.

Per poter migliorare costantemente i nostri prodotti e rispondere alle esigenze dei lettori, vi invitiamo a comunicarci **la vostra opinione su questo rapporto**:

https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/evaluation-halbjahresbericht1.html

3 Tema principale: COVID-19

3.1 Opportunità per l'ingegneria sociale

I ciberattori adeguano regolarmente gli attacchi d'ingegneria sociale («*social engineering*») ai grandi eventi d'attualità come catastrofi naturali e manifestazioni sportive. È stato così anche nel caso della pandemia in corso. Un nuovo virus poco conosciuto e che potenzialmente può colpire tutti si presta perfettamente a questo tipo di attacchi, che sfruttano sentimenti come insicurezza, paura e curiosità. I criminali hanno quindi tentato di installare di nascosto sui computer della popolazione software nocivi o di convincere singole persone a divulgare dati personali in cambio di informazioni sul virus (scoperte recenti sui vettori di infezione, casi di contagio, dati aggiornati sulla diffusione, ecc.). In altri casi si pubblicizzavano misure di protezione e metodi di trattamento. La disponibilità inizialmente limitata di dispositivi di protezione individuale come mascherine e disinfettanti ha inoltre offerto ai malintenzionati l'occasione di attirare l'attenzione con offerte corrispondenti.[1] Dopo che i governi hanno stabilito misure a sostegno della popolazione e delle imprese, sono state diffuse anche e-mail fraudolente su questo argomento.[2] In particolare nei casi in cui erano state ideate procedure straordinarie e pertanto inconsuete. Anche il tracciamento dei contatti (il cosiddetto «contact tracing») è un'opportunità per l'ingegneria sociale. Quando, dopo la riapertura, i parchi divertimenti e i luoghi di svago hanno cominciato a promuovere offerte speciali, i criminali hanno colto l'occasione per diffondere false offerte.[3] Probabilmente anche lo sviluppo e il lancio di vaccini verranno sfruttati dai criminali per mimetizzare attacchi di questo tipo.

Uno scenario che ha ottenuto nuovo slancio in seguito alla chiusura dei negozi e al conseguente incremento degli ordini online è stata la consegna di pacchi che apparentemente non potevano essere recapitati o presentavano qualche problema. Spesso questi messaggi erano collegati alla richiesta di compiere una determinata azione.[4] I destinatari venivano invitati per e-mail o SMS a pagare le spese di spedizione mancanti o una commissione per lo sdoganamento. Tali messaggi a nome di servizi di spedizione come DHL, FedEx e UPS, ma anche della Posta o della dogana vengono solitamente usati per diffondere software nocivi, commettere truffe, svolgere attività di phishing o promuovere abbonamenti trappola (cfr. n. 3.1.3 e anche la panoramica sulle segnalazioni ricevute al n. 4).

---

1 https://securityintelligence.com/posts/german-task-force-for-covid-19-medical-equipment-targeted-in-ongoing-phishing-campaign/

2 https://www.cisa.gov/sites/default/files/publications/Avoid_Scams_Related_to_Economic_Payments_COVID-19.pdf; https://www.proofpoint.com/us/blog/threat-insight/ready-made-covid-19-themed-phishing-templates-copy-government-websites-worldwide

3 https://www.cybercrimepolice.ch/de/fall/wieder-betrug-mit-themenpark-tickets-zoo-zuerich-nein-abofalle/; https://www.srf.ch/news/schweiz/abzocke-mit-abofalle-betrug-im-namen-des-zueri-zoo

4 https://www.cybercrimepolice.ch/de/fall/sms-angeblich-im-namen-der-post-betrueger-verteilen-spionage-app/; https://www.cybercrimepolice.ch/de/fall/angebliche-paketlieferung-mit-code-per-sms-freischalten/; https://www.kaspersky.com/blog/covid-fake-delivery-service-spam-phishing/35125/

3.1.1 Diffusione di malware

Anche se alcune prima di altre, praticamente tutte le principali famiglie di software nocivo sono state diffuse con l'alibi del coronavirus o del COVID-19. Il fattore di diffusione più frequente sono state le e-mail con allegati infetti o link a siti compromessi. Inoltre, sugli app store non ufficiali sono state proposte app che offrivano presunte mappe di diffusione del virus e un servizio di notifiche in caso presenza di persone infette nelle vicinanze.[5] Allo stesso modo, sono state scoperte delle copie di app di tracciamento ufficiali «arricchite» di software nocivi.[6] È stato sfruttato anche l'aumentato interesse verso le soluzioni per videoconferenze: linkando siti web contraffatti con la tecnica del *typosquatting* (ossia scegliendo un dominio che può essere facilmente confuso con un altro), sono stati offerti file di installazione di programmi per le videoconferenze contenenti malware.[7]

Il 13 marzo un'ondata di e-mail con software nocivi ha preso di mira la Svizzera.[8] In questa occasione, a figurare come apparente mittente era l'Ufficio federale della sanità pubblica (UFSP), indicato anche in inglese (Federal Office of Public Health, FOPH). I messaggi sono stati inviati tramite l'ambasciata del Kenya a Parigi, la cui infrastruttura IT era stata violata. Nel file Excel allegato era nascosto Agent Tesla, un trojan in grado di intercettare e registrare tutto ciò che viene digitato sulla tastiera e di effettuare screenshot.

Fig. 1: e-mail a nome dell'UFSP con allegato dannoso

---

5 https://www.cybercrimepolice.ch/de/fall/vorsicht-vor-falscher-corona-virus-mapping-app/; https://symantec-blogs.broadcom.com/blogs/threat-intelligence/android-apps-coronavirus-covid19-malicious; https://research.checkpoint.com/2020/covid-19-goes-mobile-coronavirus-malicious-applications-discovered/

6 https://www.anomali.com/blog/anomali-threat-research-identifies-fake-covid-19-contact-tracing-apps-used-to-monitor-devices-steal-personal-data; https://www.bleepingcomputer.com/news/security/new-f-unicorn-ransomware-hits-italy-via-fake-covid-19-infection-map/; https://cert-agid.gov.it/news/campagna-ransomware-fuckunicorn-sfrutta-emergenza-covid-19/

7 https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/; https://blog.trendmicro.com/trendlabs-security-intelligence/zoomed-in-a-look-into-a-coinminer-bundled-with-zoom-installer/

8 https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/gefaelschte-emails-im-namen-des-bag.html

Con queste esche legate a coronavirus e COVID-19, nella maggior parte dei casi sono stati diffusi software nocivi in grado di rubare informazioni (*infostealer* o *spyware*).[9] Spesso gli *spyware* contengono anche moduli che consentono di installare altri malware a scelta. In alcuni casi sono stati diffusi dei ransomware direttamente tramite questo tipo di e-mail.

Raccomandazione

Se avete cliccato su un link o aperto allegati ricevuti in e-mail sospette, il vostro dispositivo potrebbe essere stato infettato da un software nocivo. Controllate ed eventualmente pulite (o meglio ancora formattate) il dispositivo. Se non sapete come fare, rivolgetevi a un tecnico. I programmi antivirus non offrono alcuna garanzia di riconoscere e rimuovere completamente le infezioni. Dopo la formattazione cambiate tutte le password utilizzate con il dispositivo in questione.

3.1.2 Phishing

Gli eventi di attualità e le situazioni inusuali vengono spesso sfruttate come pretesto dai cibercriminali per convincere le persone a effettuare una determinata azione facendo leva – tramite tecniche di ingegneria sociale – sulla loro curiosità, paura o scarsa conoscenza della materia. Per conferire credibilità allo scenario, spesso si fa riferimento all'evento vero e proprio. Per esempio, poco prima dell'imposizione del lockdown sono state inviate e-mail a nome di Netflix in cui si promettevano accessi gratuiti durante la crisi del coronavirus.[10] Per usufruire dell'offerta era necessario indicare i dati della carta di credito. Il phishing tramite finte piattaforme per videoconferenze rappresenta un ulteriore esempio di come la situazione straordinaria è stata sfruttata dai truffatori. Numerosi utenti si sono trovati a utilizzare tali software di comunicazione e collaborazione per la prima volta. Di conseguenza, per molti di loro non era facile riconoscere se un messaggio proveniva dalla piattaforma o se si trattava di un falso.[11] Queste incertezze sono state sfruttate dai criminali per indirizzare gli utenti verso maschere di accesso manipolate dove veniva loro richiesto di inserire le password.

Raccomandazione

Quando ricevete messaggi di un nuovo tipo o inusuali è sempre opportuna una buona dose di scetticismo. Anziché cliccare sui link inviati, dovreste se possibile accedere al vostro account nel modo consueto. Prima di inserire dati personali, password o informazioni sulle carte di credito accertatevi di essere effettivamente sul sito desiderato.

---

9 https://blog.checkpoint.com/2020/05/11/april-2020s-most-wanted-malware-agent-tesla-remote-access-trojan-spreading-widely-in-covid-19-related-spam-campaigns/; https://www.lastline.com/labsblog/infostealers-weaponizing-covid-19/; https://www.bleepingcomputer.com/news/security/microsoft-warns-of-covid-19-phishing-spreading-info-stealing-malware/.

10 https://www.cybercrimepolice.ch/de/fall/corona-phishing-mail-im-namen-von-netflix/

11 https://www.darkreading.com/cloud/fake-microsoft-teams-emails-phish-for-credentials/d/d-id/1337717; https://abnormalsecurity.com/blog/abnormal-attack-stories-microsoft-teams-impersonation/; https://abnormalsecurity.com/blog/abnormal-attack-stores-zoom-phishing-campaign/;

3.1.3 Abbonamenti trappola

Durante il lockdown del mese di marzo, in Svizzera sono stati diffusi messaggi tramite WhatsApp che mettevano in palio buoni per l'acquisto di alimentari. Come mittente figuravano aziende del commercio al dettaglio intenzionate a «sostenere la nazione durante la pandemia di coronavirus». A questo fine i truffatori hanno sfruttato marchi noti come Migros, Coop e Denner.[12] Sul sito web a cui rimandava il link venivano chiesti i dati della carta di credito con la scusa di verificare l'identità e garantire che ogni persona ricevesse un solo buono. Nelle clausole scritte in piccolo sulla pagina era tuttavia nascosto un costoso abbonamento che veniva poi addebitato mensilmente sulla carta di credito.

Raccomandazione

Gli estratti conto delle carte di credito andrebbero sempre controllati con attenzione per poter eventualmente bloccarle in accordo con l'istituto emittente in caso di irregolarità o addebiti ingiustificati. I truffatori possono utilizzare i dati sottratti per effettuare addebiti, ma anche rivenderli a terzi.

3.2 Attacchi a siti e servizi web

In diversi Paesi i siti web di ospedali e autorità che fornivano informazioni sulla pandemia oppure offrivano servizi sono stati per breve tempo irraggiungibili.[13] Alcuni responsabili dei siti hanno affermato che le interruzioni sono state provocate da attacchi DDoS. Sebbene questa sia una spiegazione plausibile e generalmente corretta, in alcuni casi ad aver sovraccaricato i server potrebbe essere stato l'elevato interesse della popolazione per contenuti e servizi.

12 https://www.cybercrimepolice.ch/de/fall/whatsapp-fake-kettenbrief-im-umlauf-migros-verlost-kostenlose-lebensmittel-im-wert-von-250-euro-um-die-nation-waehrend-der-corona-pandemie-zu-unterstuetzen/; https://www.cybercrimepolice.ch/de/fall/weiterer-whatsapp-fake-kettenbrief-angeblich-von-denner-im-umlauf/; https://www.cybercrimepolice.ch/de/fall/wieder-whatsapp-fake-kettenbrief-diesmal-im-namen-von-coop/; https://www.cybercrimepolice.ch/de/fall/neuer-whatsapp-kettenbrief-migros-verlost-gutscheine-in-hoehe-von-chf-180-/

13 https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response; https://hungarytoday.hu/coronavirus-govt-website-attack-shutdown/; https://www.lesechos.fr/tech-medias/hightech/laphp-victimes-dune-cyberattaque-1188022; https://news.trust.org/item/20200401133925-o6wx4/

Raccomandazione

Nelle imprese fortemente dipendenti dalla disponibilità di servizi IT è necessario dare la massima priorità alla salvaguardia dei canali corrispondenti. Individuate i servizi tanto importanti da produrre conseguenze rilevanti sulla vostra organizzazione in caso di interruzione. Pensate anche ai sistemi di base senza i quali le vostre applicazioni commerciali critiche non funzionerebbero. Sviluppate una strategia contro gli attacchi *DDoS*. Devono essere noti gli uffici interni ed esterni competenti, così come le persone che possono intervenire in caso di attacco. Idealmente, un'impresa si occupa del problema delle minacce *DDoS* a livello di direzione prima di un attacco nel quadro della gestione generale del rischio, stabilendo a livello aziendale un certo stato di allerta rispetto al tema *DDoS*. Un attacco *DDoS* può colpire qualsiasi organizzazione. Parlate con il vostro fornitore di servizi Internet delle vostre esigenze e definite misure adeguate.

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

3.3 Attacchi contro ospedali

Gli ospedali erano fra gli obiettivi preferiti dei cibercriminali già prima della pandemia, in particolare come bersaglio di ransomware.[14] Visto il temuto sovraccarico delle istituzioni del sistema sanitario a causa del coronavirus, è stata prestata particolare attenzione a ogni contrattempo in questo settore. Quando il 16 marzo è stato reso noto che un ospedale in Repubblica Ceca che ospita un importante centro di test per il coronavirus era stato limitato nelle sue funzioni in seguito a un caso di ransomware, il clamore internazionale è stato notevole. Diversi governi hanno condannato con veemenza questi attacchi al sistema sanitario, invocando la collaborazione internazionale per porre un freno a queste pratiche. Alcuni programmatori di ransomware hanno promesso di non attaccare gli ospedali. Tuttavia, anche in seguito diverse strutture hanno denunciato casi di ransomware.[15] Vari fornitori di servizi di sicurezza si sono offerti di aiutare gratuitamente le istituzioni sanitarie interessate.[16]

3.4 Ciberspionaggio

In condizioni normali le spie acquisiscono informazioni che possono essere molto diverse a seconda del continente e del Paese (in base alle priorità definite dai relativi governi). Durante la pandemia da coronavirus, i governi erano invece interessati alle stesse informazioni sul virus e sulla malattia causata da quest'ultimo. Nonostante si tratti di un problema che riguarda tutto il genere umano, non tutti gli attori coinvolti collaborano in maniera incondizionata. Diversi Paesi non si fidano gli uni degli altri, così come non si fidano dell'Organizzazione mondiale

14 Cfr. rapporti semestrali MELANI 2016/1, n. 5.4.3; 2017/1, n. 3; 2019/1, n. 3, e 2019/2, n. 4.6.1.

15 https://www.bleepingcomputer.com/news/security/ryuk-ransomware-keeps-targeting-hospitals-during-the-pandemic/; https://securityaffairs.co/wordpress/100548/malware/ryuk-ransomware-hospitals-covid19.html;

16 https://www.coveware.com/blog/free-ransomware-assistance-to-healthcare-coronavirus; https://cybersecurity.att.com/blogs/labs-research/a-surge-in-threat-activity-related-to-covid-19; https://coronahelp.isss.ch/

della sanità (OMS). Convinti che vengano loro nascoste delle informazioni, incaricano i propri agenti di ottenerle. Mentre l'accertamento di eventuali ritocchi al ribasso nel numero dei contagi in un Paese può essere sfruttato per migliore valutazione del rischio o a fini di propaganda politica, le informazioni sull'adeguatezza delle misure di protezione, dei metodi di trattamento e dei farmaci presentano un'utilità diretta per i propri provvedimenti. Per quanto riguarda i potenziali vaccini, la questione si complica un po': nonostante numerose istituzioni accademiche e altre organizzazioni portino avanti la ricerca e si confrontino regolarmente, in questo ambito sono tuttavia attive anche diverse imprese private che sperano di conseguire grandi utili attraverso prodotti sviluppati in proprio e brevetti. La sfida di trovare un farmaco efficace e di fornirlo alla popolazione del proprio Paese, se non addirittura al mondo intero, è una questione scientifica e logistica, ma anche economica e politica. Sullo spionaggio ai tempi della COVID-19 si veda anche il numero 4.6.1.

Conclusione

Tutti gli attori coinvolti nell'attività di ricerca e sviluppo nell'ambito della pandemia da coronavirus devono fare i conti con attacchi di spionaggio di diversa natura. Tanto le organizzazioni statali quanto quelle private sono interessate a dati, risultati delle ricerche e segreti commerciali in questo campo.

3.5 Lavoro da casa, ma sicuro!

La digitalizzazione del lavoro quotidiano ha ricevuto una grande spinta dalla pandemia. In molte imprese è stato introdotto o esteso il telelavoro a domicilio. Le riunioni si sono svolte sempre più spesso al telefono o in videoconferenza. Tuttavia, le organizzazioni hanno in parte trasformato in breve tempo la propria infrastruttura informatica nell'ottica del lavoro in home-office senza un'adeguata implementazione di misure di sicurezza, esponendo in questo modo le proprie reti.[17] I malintenzionati hanno intensificato le proprie attività di scansione per identificare le soluzioni di accesso remoto vulnerabili e individuare i punti deboli presenti o le implementazioni non abbastanza protette di soluzioni «*Remote Desktop Protocol*» (*RDP*) e server *VPN* («*Virtual Private Network*») al fine di sfruttarli per penetrare nelle reti aziendali. Anche gli attacchi phishing sono stati mirati sulla base della mutata situazione lavorativa. Molti utenti utilizzavano per la prima volta software di videoconferenza e collaborazione e non avevano dimestichezza con i messaggi inviati da tali piattaforme, motivo per cui i corrispondenti falsi[18] erano difficili da riconoscere. Sul lavoro a domicilio si veda anche il numero 6.1.

17 https://blog.shodan.io/trends-in-internet-exposure/

18 https://www.darkreading.com/cloud/fake-microsoft-teams-emails-phish-for-credentials/d/d-id/1337717; https://abnormalsecurity.com/blog/abnormal-attack-stories-microsoft-teams-impersonation/; https://abnormalsecurity.com/blog/abnormal-attack-stores-zoom-phishing-campaign/

Raccomandazione

L'uso dell'infrastruttura informatica privata (in particolare di computer) per il lavoro a domicilio, amplia la superficie a rischio di ciberattacchi, visto che reti private e dispositivi personali sono spesso protetti in modo meno efficace rispetto alle infrastrutture aziendali gestite da professionisti. Anche per quanto riguarda il riconoscimento degli attacchi di *ingegneria sociale*, i collaboratori in telelavoro sono spesso abbandonati a sé stessi non potendo discutere immediatamente con colleghe e colleghi di fatti sospetti. Le campagne di sensibilizzazione, così come l'allestimento e la pubblicizzazione di canali di segnalazione ai responsabili aziendali della sicurezza informatica possono risultare utili sotto questo punto di vista.

Liste di controllo MELANI per il telelavoro:

Per le imprese: https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/fernzugriff.html

Per gli utenti: https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/fernzugriff-enduser.html

3.6 App per il tracciamento di prossimità

Al fine di tracciare la diffusione del coronavirus e adottare misure protettive mirate e adeguate, in molti Paesi sono state introdotte applicazioni per il tracciamento dei contatti o di prossimità. Questa nuova tecnologia viene impiegata per ricostruire le potenziali catene di contagio e informare sui rischi le persone interessate. Questi strumenti tecnici possono fornire un importante contributo nel contrastare la diffusione del virus indicando quando una persona è stata esposta al contagio. In questo modo le persone possono essere informate ma anche invitate a sottoporsi ai test e ad adottare misure temporanee volte a prevenire l'ulteriore diffusione del virus.

Anche se tutti auspicano la fine della pandemia, non tutti sono disposti a condividere dati, accettare limitazioni o adeguarsi all'imposizione di nuovi obblighi. In diversi Paesi il lancio delle app di tracciamento ha dato luogo a critiche sia a causa delle carenze nella protezione dei dati che delle eventuali lacune di sicurezza. Ponderare i diversi interessi e trovare una soluzione accettabile per la popolazione è una vera sfida. Si tratta di una nuova tecnologia per la quale è necessario innanzitutto raccogliere esperienze e che è destinata a maturare con il tempo.

Nota

Nel quadro del progetto svizzero COVID-19 Proximity Tracing, il NCSC ha istituito una task force sul tema «Security & Privacy» chiamata a valutare questioni di cibersicurezza e protezione della sfera privata. Attraverso un test pubblico di sicurezza avviato il 28 maggio 2020, ulteriori professionisti e interessati stanno esaminando a fondo la sicurezza dell'intero sistema.

https://www.melani.admin.ch/melani/it/home/public-security-test/infos.html

4 Eventi / situazione

Panoramica delle segnalazioni ricevute

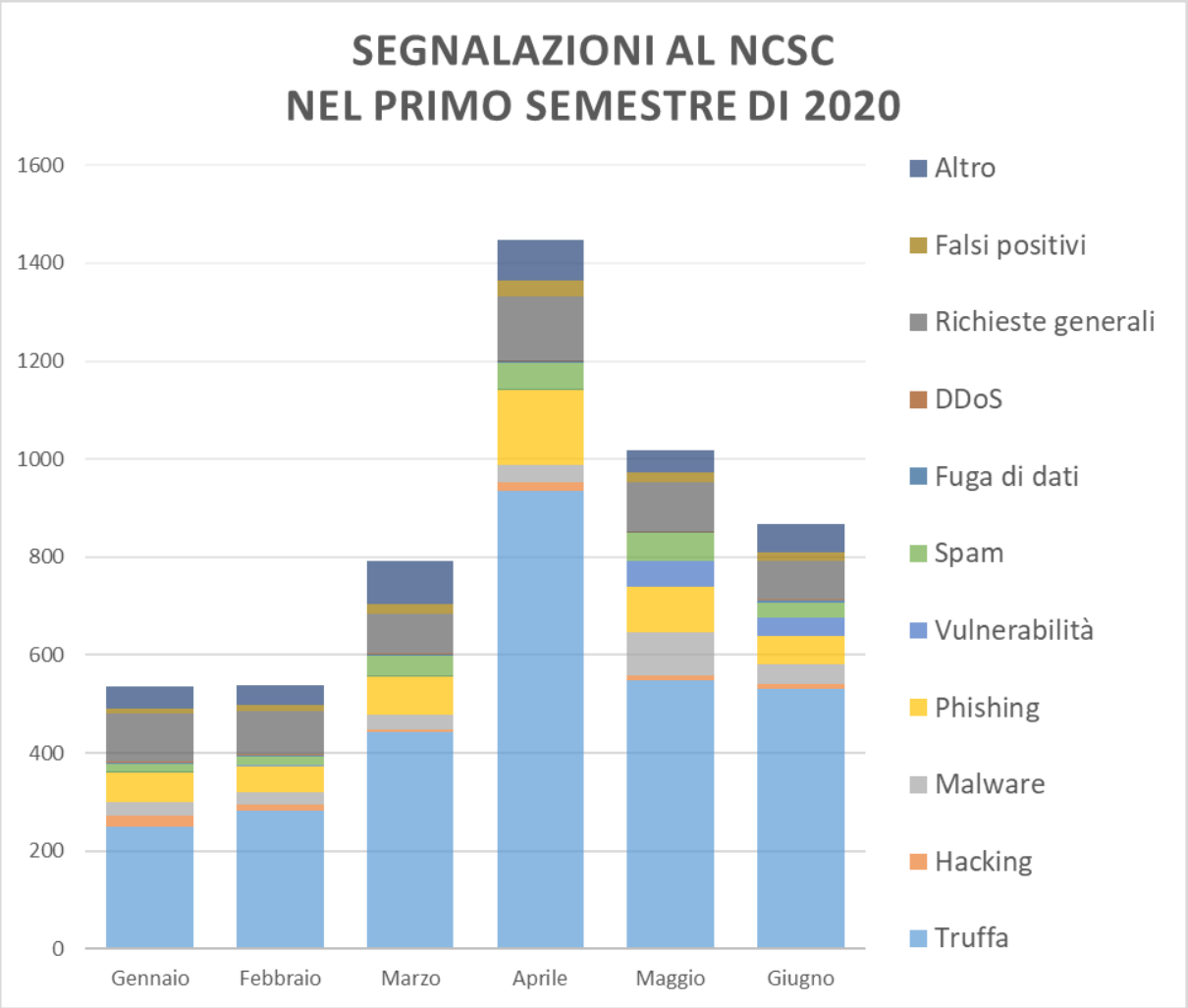

Fig. 2: Segnalazioni pervenute all'NCSC nel primo semestre del 2020

Nel primo semestre del 2020 il servizio di contatto nazionale per la cibersicurezza del NCSC ha registrato complessivamente 5152 segnalazioni. Oltre la metà degli annunci (precisamente 2938) riguardava tentativi di frode, con 825 casi di e-mail con «truffa dell'anticipo».

Frequenti sono stati anche i cosiddetti «abbonamenti trappola» legati alla consegna di un pacco. Si tratta di una variante di un tipo di truffa noto già da tempo, con la quale si promuovono offerte apparentemente gratuite, che dopo alcuni giorni si trasformano in abbonamenti a pagamento. Questa clausola, tuttavia, è intenzionalmente scritta molto in piccolo. Nelle varianti in circolazione durante l'estate era richiesta una piccola commissione per il presunto recapito di un pacco. Anche in questo caso, tuttavia, veniva stipulato un abbonamento all'insaputa della vittima. Erano richiesti i dati della carta di credito o l'invio di un codice a un numero breve. Durante la crisi legata al coronavirus, i truffatori si sono specializzati in questa nuova variante perché molte persone effettuavano acquisti online e dunque attendevano pacchi (cfr. n. 3.1).

Sono state numerose anche le e-mail ricattatorie. Con 578 segnalazioni, la quota più ampia riguarda i messaggi di *fake sextortion*.[19] In questo tipo di truffa si fa credere alla vittima che il computer è stato hackerato e che sono state registrate immagini compromettenti dalla web-cam. Di norma è una menzogna e si tratta quindi di un bluff. Nel primo semestre del 2020 sono stati osservati anche tentativi di estorsione contro gli amministratori di siti web. In questo caso, nelle e-mail si diceva che i siti erano stati hackerati e i corrispondenti database rubati. Infine si minacciava di rendere pubblici i dati sottratti. Anche in questo caso la minaccia era priva di fondamento (cfr. n. 4.7.5). I truffatori non esitano nemmeno a ricorrere a storie più violente, come dimostrato dagli allarmi bomba inviati via e-mail a due aziende (anche in questo caso si è rivelato tutto una finzione).

Nei primi sei mesi del 2020 ha fatto ritorno anche una vecchia truffa: la cosiddetta «truffa del dominio» è stata infatti segnalata 63 volte. In questo caso, una supposta azienda di gestione domini contatta il proprietario di un sito «.ch» affermando che un'altra ditta è interessata al corrispondente dominio «.com». Il proprietario del sito può tuttavia correre ai ripari acquistandolo. I domini vengono offerti a un prezzo fortemente rincarato, e non è nemmeno sicuro che vengano effettivamente registrati.

Dalle aziende sono stati notificati anche 94 casi della cosiddetta «truffa del CEO». I criminali si informano in questo caso in anticipo, generalmente tramite il sito dell'azienda, su indirizzi e-mail e funzioni dei collaboratori. Sulla base di queste informazioni viene poi inventata una storia su misura per la società presa di mira. A nome del responsabile della stessa, i truffatori ordinano alla contabilità o al servizio finanziario di effettuare un pagamento urgente.

I casi di software nocivi (malware) segnalati sono stati 232. Degne di nota sono le 42 segnalazioni di ransomware (troiani che cifrano file a scopo di estorsione). Rispetto ai tentativi di truffa questo numero è piuttosto ridotto, ma il potenziale danno è molto maggiore (cfr. n. 4.1.1).

4.1 Malware: la situazione attuale

La statistica riportata di seguito mostra i malware che hanno colpito maggiormente gli utenti di Internet in Svizzera. Le statistiche provengono da diverse fonti e vengono aggregate e filtrate per l'intero spazio IP svizzero noto al NCSC. Le informazioni tecniche di dettaglio vengono messe a disposizione dei provider svizzeri affinché possano informare i clienti sulle infezioni e raccomandare apposite misure. A volte le varie famiglie di malware sono difficili da distinguere, visto che non esiste uno schema di nomenclatura internazionale. È importante tenere presente che questi numeri rappresentano solo la punta dell'iceberg, poiché la banca dati contiene solo i dati di singoli server *«command and control»*.

[19] https://www.melani.admin.ch/melani/it/home/meldeformular/formular0/meldeformularhaeufigefragen/Fake-Sextortion.html

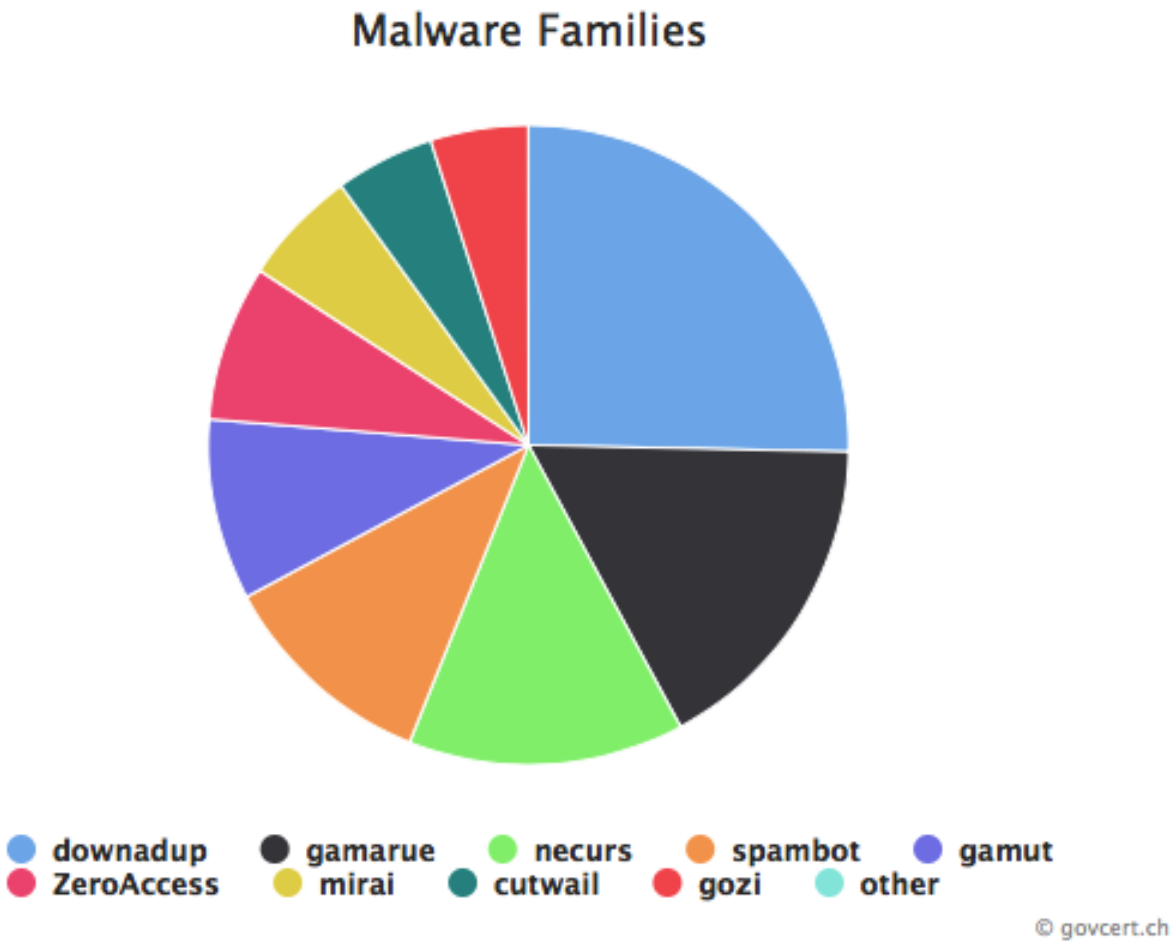

Figura 3: Ripartizione dei malware in Svizzera noti all'NCSC (stato: 30 giugno 2020).
I dati aggiornati sono pubblicati all'indirizzo: https://www.govcert.admin.ch/statistics/malware/.

4.1.1 Ransomware: ultimi sviluppi

MELANI sta seguendo da diversi anni il fenomeno del ransomware.[20] Secondo le statistiche della società Trustwave,[21] questa minaccia in continua espansione è quadruplicata nel 2019 e occupa attualmente la prima posizione nella classifica degli eventi più frequenti nel campo della cibersicurezza. Ad aumentare non è solo il numero delle infezioni da ransomware, ma anche la quantità di vettori di attacco e di servizi che forniscono strumenti per l'esecuzione di un attacco e la trattativa per il pagamento del riscatto («*ransomware-as-a-service*», *RaaS*). Secondo un rapporto della società Coveware,[22] che si occupa di contrastare gli attacchi ransomware, nel primo trimestre dell'anno in corso le richieste di riscatto sono aumentate del 33 per cento rispetto agli ultimi mesi del 2019.

---

20 Cfr. Rapporti semestrali MELANI 2011/2, n. 3.5; 2013/2, n. 3.1; 2014/2, n. 3.6 e 5.3; 2015/1, n. 4.6.1.5; 2015/2, n. 4.5.1; 2016/1, n. 4.6.3, 4.6.4 e 5.4.3; 2016/2, n. 4.6.3 e 6.1; 2017/1, n. 3; 2017/2, n. 5.4.2; 2018/2, n. 4.5.4 e 5.3.5; 2019/2, n. 4.6.1.

21 https://www.zdnet.com/article/Ransomware-is-now-the-biggest-online-menace-you-need-to-worry-about/

22 https://www.coveware.com/blog/q1-2020-Ransomware-marketplace-report

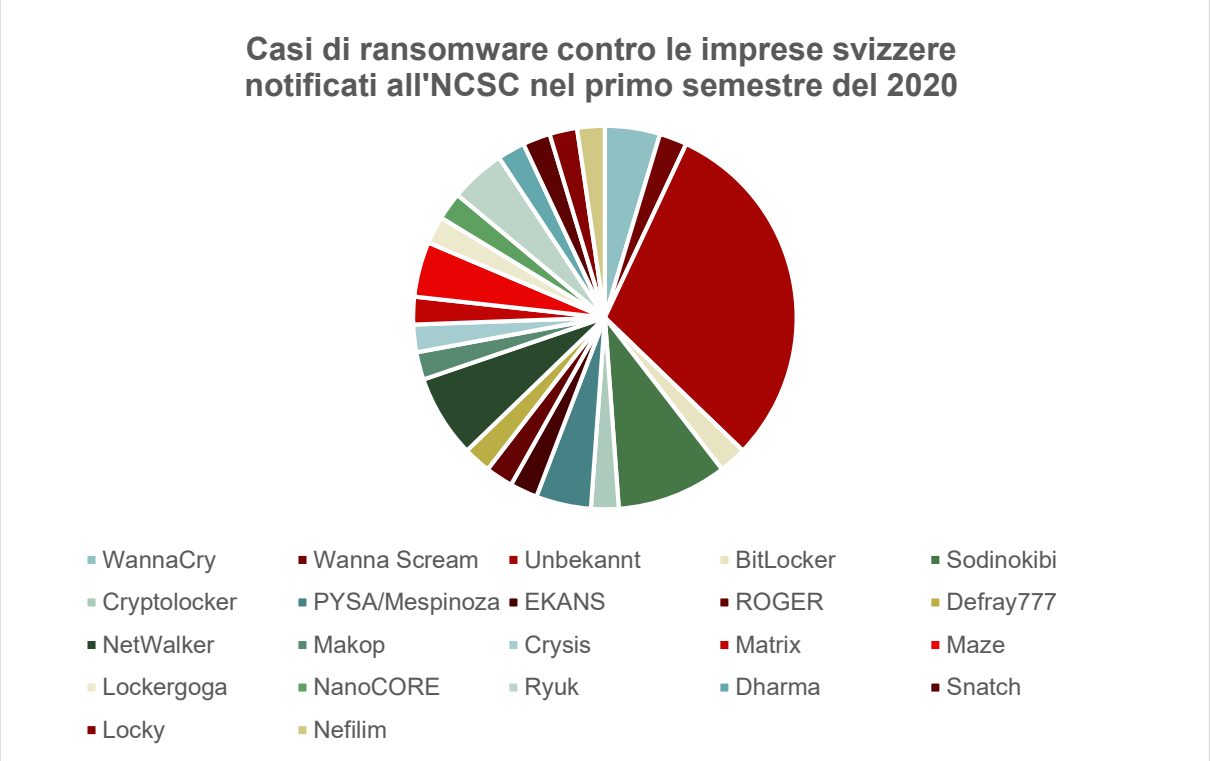

Fig. 4: Casi di ransomware contro le imprese svizzere notificati all'NCSC nel primo semestre del 2020

Anche nel periodo oggetto del presente rapporto, le imprese svizzere sono finite nel mirino di attacchi ransomware. Complessivamente, al NCSC sono stati notificati 42 casi di attacchi ransomware contro aziende. Purtroppo non tutte le segnalazioni includevano informazioni sul malware impiegato per l'attacco. Come emerge dalla figura 4, nel primo semestre del 2020 sono stati segnalati svariati tipi di attacchi ransomware. Nonostante la maggioranza delle notifiche al NCSC riguardi PMI, sono state coinvolte anche società di dimensioni maggiori. Grande interesse mediatico ha destato l'attacco di gennaio contro il gruppo francese Bouygues Construction, che dopo un attacco con il malware Maze per risolvere la situazione ha dovuto sospendere temporaneamente la produzione in tutte le filiali (compresa quella svizzera).[23] All'inizio di maggio, a cadere vittima di un ransomware è stato il produttore di veicoli ferroviari Stadler Rail. La società è stata ricattata con la minaccia di pubblicare i dati rubati qualora non avesse pagato un riscatto pari a 5,8 milioni di franchi.[24] Per aumentare la probabilità che il riscatto venga effettivamente pagato, i criminali adeguano gli importi richiesti a quelle che secondo loro sono le possibilità finanziarie delle vittime. I privati devono quindi pagare somme molto inferiori, spesso meno di mille franchi. Gli importi richiesti differiscono fortemente da campagna a campagna. Ryuk, noto fra l'altro per le pretese proibitive, ha ad esempio preteso circa 300 000 franchi di riscatto da una PMI, mentre WannaCry ha reclamato solo 1500 franchi da un'impresa simile, anche se dopo il pagamento solo una parte dei dati è stata effettivamente decriptata.

23 https://www.itnews.com.au/news/bouygues-construction-it-taken-out-by-Ransomware-537516

24 https://www.srf.ch/news/cyberAngriff-auf-stadler-rail-solange-es-etwas-zu-holen-gibt-wird-schindluder-getrieben; https://www.swissinfo.ch/eng/cyberattack-_hackers-demand-millions-in-ransom-for-stolen-stadler-rail-documents/45794036

Evoluzione del modus operandi

Già a novembre 2019 un gruppo che utilizza il ransomware Maze aveva modificato il proprio modello commerciale: prima dell'attacco vero e proprio ha cominciato a scaricare i dati della vittima per poi estorcerle denaro minacciandola di pubblicarli su un blog appositamente creato nel caso in cui il ricatto con la criptazione non fosse andato a buon fine. Questa procedura ha buone probabilità di riuscita perché oltre a danneggiare la reputazione e la pubblicazione di segreti d'affari può comportare anche conseguenze legali collegate alle norme sull'elaborazione dei dati personali. I dati pubblicati, inoltre, possono essere utilizzati per ulteriori attacchi. Nel primo semestre del 2020 il numero dei gruppi che hanno applicato questa strategia è aumentato fortemente. Oltre a Maze, l'azienda di cibersicurezza Coveware conta sei ulteriori famiglie di ransomware per le quali è stata riscontrata questa modalità di attacco collegata alla pubblicazione dei dati: Sodinokibi/REvil, DoppelPaymer (il successore di BitPaymer), Mespinoza/PYSA, NetWalker, CLoP e Nephilim[25] (così come la sua nuova versione, Nemty).[26, 27] Questi malware circolano anche in Svizzera, sebbene non tutte le infezioni segnalate a MELANI siano collegate a una fuga di dati. Ogni attacco ransomware nel quadro di una delle campagne citate può essere collegato a un furto di dati. Gli attori di Maze affermano di aver criptato e rubato i dati non solo a Stadler Rail, ma anche all'assicurazione Chubb, che tuttavia non ha confermato.[28]

Nell'ultimo rapporto semestrale,[29] MELANI aveva previsto che i cibercriminali avrebbero trovato altri strumenti e altre vie per trarre profitto dai dati sottratti (a seconda del loro valore), ad esempio non limitandosi a utilizzarli per esercitare pressione. Questo caso si è puntualmente verificato: recentemente, i cibercriminali responsabili della diffusione del ransomware Sodinokibi/REvil hanno messo all'asta i dati rubati dopo che le vittime si erano rifiutate di pagare il riscatto.[30] Altri gruppi richiedono addirittura un doppio riscatto, uno per recuperare i documenti criptati e il secondo per garantire l'eliminazione definitiva dei dati rubati.[31] Le richieste di denaro variano a seconda della vittima e della campagna, ma in alcuni casi sono esorbitanti. A titolo di esempio: a luglio Sodinokibi/REvil ha richiesto allo studio legale per celebrità Grubman Shire Meiselas & Sacks il pagamento di un riscatto pari a 42 milioni di dollari americani per evitare la pubblicazione dei dati rubati e ottenere il codice di decriptazione. Di fronte al rifiuto di pagare, i ricattatori hanno iniziato a vendere all'asta un gran numero di documenti su personalità del mondo dello spettacolo, con prezzi di partenza compresi fra 600 000 dollari e 1 000 000 di

---

25 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/investigation-into-a-nefilim-attack-shows-signs-of-lateral-movement-possible-data-exfiltration/

26 Questo schema sta ottenendo sempre più il favore dei cibercriminali, per esempio tramite la fondazione da parte di un altro attore *ransomware* di una piattaforma su cui pubblicare i dati sottratti, anche se al momento non sono state ancora diffuse fughe di dati. Questo schema è conosciuto come «Sekhmet», cfr. https://www.bleepingcomputer.com/news/security/three-more-Ransomware-families-create-sites-to-leak-stolen-data/

27 A questi si aggiunge il *ransomware* «RagnarLocker» (noto anche come «Ragnarok»), che finora non ha ancora fatto la sua comparsa in Svizzera: https://www.securityweek.com/ragnar-locker-Ransomware-uses-virtual-machines-evasion

28 https://www.bankinfosecurity.com/insurer-chubb-investigating-security-incident-a-14023

29 Cfr. Rapporto semestrale MELANI 2019/2, n. 4.6.1.

30 https://www.bleepingcomputer.com/news/security/revil-Ransomware-creates-ebay-like-auction-site-for-stolen-data/

31 https://krebsonsecurity.com/2020/06/revil-Ransomware-gang-starts-auctioning-victim-data/

dollari.[32] La vendita di dati rubati tramite forum criminali non è una novità, ma la pubblicazione e l'uso come strumenti di pressione rappresenta una nuova variante che potrebbe convincere sempre più vittime a cedere e pagare il riscatto. Si veda anche il numero 4.5 sulle fughe di dati.

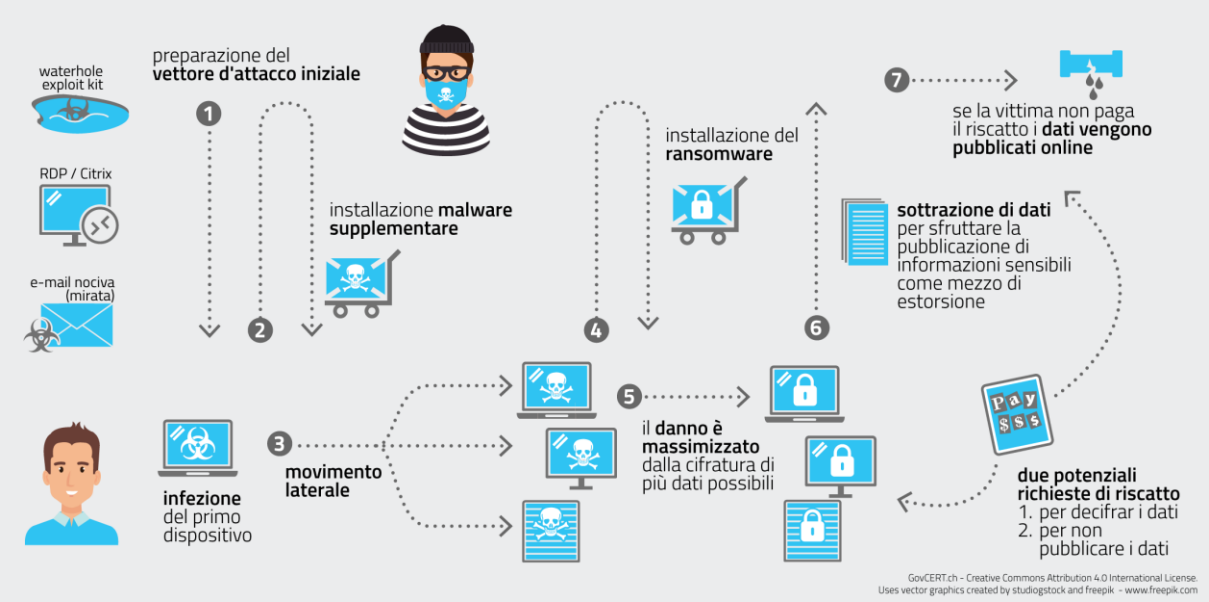

Fig. 5: Attuale modus operandi degli attacchi con ransomware

La possibilità di ottenere guadagni ragguardevoli e la complessità degli attacchi a più livelli hanno portato alla proliferazione di modelli di collaborazione fra diversi gruppi criminali, così come fra membri di tali gruppi e freelance. Secondo FireEye, ad esempio, il ransomware Maze non è utilizzato da un singolo gruppo, bensì da diversi attori organizzati in una rete di partner (rete di affiliazione). In altre parole, gli sviluppatori di ransomware collaborano con altri soggetti che si occupano ad esempio della diffusione di malware, stabiliscono l'accesso alla rete oppure sono responsabili dell'esplorazione delle reti infettate o di altri aspetti specifici. Possono agire come «dipendenti» oppure ricevere una commissione dopo il pagamento del riscatto.[33]

Inizialmente Maze veniva diffuso soprattutto con l'aiuto di e-mail infette, ma nel primo semestre del 2020 ci sono state sempre più spesso infezioni con questo ransomware nel quadro di attacchi più strutturati, che sfruttano un'infezione preesistente con un altro malware e prima della criptazione consentono un'infiltrazione più capillare nella rete. Il fornitore di servizi di sicurezza FireEye ha riscontrato notevoli differenze nelle modalità degli attacchi osservati, ad esempio per quanto riguarda il tempo che intercorre fra l'infezione iniziale e l'uso del ransomware, oppure il vettore di intrusione utilizzato (ad es. una porta *RDP* aperta o altri servizi accessibili tramite Internet e mal configurati, con password deboli o sfruttando dati di accesso sottratti e successivamente venduti sul dark web). Vi sono anche notevoli differenze in merito

32 https://www.scmagazine.com/home/security-news/cybercrime/lebron-james-among-the-1st-stars-to-have-their-stolen-law-firm-files-put-up-for-auction/

33 https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-Ransomware-incidents.html

alle strategie per una maggiore persistenza («*persistence*») sulla rete o la possibilità di interazione con i sistemi della vittima nelle singole fasi dell'esplorazione e della diffusione nella rete («*lateral movement*»). Questa varietà è considerata un ulteriore indizio del coinvolgimento di diversi attori. I criminali dietro a Maze hanno inoltre pubblicato sul loro sito dati rubati a uno studio di architetti dai responsabili del ransomware LockBit. Un membro del gruppo Maze aveva dichiarato la loro disponibilità ad avviare prossimamente una collaborazione con un terzo gruppo.[34]

Maze non è l'unico ransomware i cui responsabili puntano sulla strategia «l'unione fa la forza». Anche i criminali dietro a NetWalker stanno creando da marzo 2020 reti di affiliazione che pubblicizzano i propri ransomware nel quadro di un «blog underground». Per reclutare i partner vengono promessi profitti colossali pari al 70 per cento del riscatto, ossia prospettando un guadagno compreso tra 487 000 e 1 000 000 di dollari. Inoltre, anche per NetWalker è stata creata una piattaforma destinata alla pubblicazione dei dati sottratti. In questo modo i partner possono pubblicare autonomamente informazioni sulle vittime delle infezioni allo scopo di ottimizzare i proventi dai diversi attacchi.[35]

Evoluzione tecnica

Nell'ultimo rapporto semestrale[36] si era già parlato del fatto che in molti casi un'infezione tramite ransomware non richiede alcuna interazione da parte degli utenti. Assieme ad altre particolarità, come la possibilità di utilizzare lo stesso malware per un gran numero di vittime, ciò spiega il successo di questo fenomeno. Tra i vettori più sfruttati nelle campagne ransomware tra gennaio e giugno 2020 per introdursi nelle reti aziendali vi sono le porte *RDP* con una protezione insufficiente,[37] i cui diritti di accesso possono essere acquistati sul mercato nero a prezzi molto bassi. Come porte di accesso all'infrastruttura informatica è possibile sfruttare anche server con lacune di sicurezza. Nel primo semestre del 2020, il malware Sodinokibi/REvil – già penetrato tramite una falla di sicurezza nei prodotti *VPN* di Pulse Secure – è stato il primo ransomware ad aver bucato una rete aziendale sfruttando la vulnerabilità di Citrix CVE-2019-19781 (cfr. n. 4.4). Nel periodo oggetto del rapporto, oltre a Sodinokibi/REvil sono stati osservati altri due ransomware che sfruttano questo punto debole come vettore di penetrazione: Maze e RagnarLocker.[38] Anche in Svizzera non si esclude che si siano verificate infezioni tramite server *VPN* Pulse Secure e Citrix vulnerabili.

Negli ultimi mesi il NCSC ha riscontrato un forte aumento degli attacchi contro le porte *RDP* come vettori iniziali per attacchi ransomware mirati. C'è una moltitudine di scansioni contro le porte *RDP* con le quali i malintenzionati tentano di sfruttare password deboli (mediante attacchi «a dizionario» e «forza bruta»). Un'altra tattica consiste nello sfruttare server non aggiornati e quindi vulnerabili. Il NCSC ha osservato la stessa procedura con altri protocolli di accesso

---

34 https://www.scmagazine.com/home/security-news/Ransomware/new-Ransomware-trends-spotted-auctioning-stolen-files-cybergangs-joining-forces/

35 https://www.bleepingcomputer.com/news/security/Ransomware-recruits-affiliates-with-huge-payouts-automated-leaks/

36 Cfr. Rapporto semestrale MELANI 2019/2, n. 4.6.1.

37 Anche l'FBI è di questa opinione e, in occasione della conferenza sulla sicurezza RSA, avvenuta a febbraio 2020, ha dichiarato che nel 70–80 per cento degli attacchi *ransomware* viene sfruttata come vettore di accesso una porta *RDP*: https://www.bleepingcomputer.com/news/security/Ransomwares-big-jump-ransoms-grew-14-times-in-one-year/

38 https://www.zdnet.com/article/hackers-target-unpatched-citrix-servers-to-deploy-Ransomware/

remoto esposti quali VPN Pulse Secure o Citrix NetScaler, le cui vulnerabilità vengono cercate ad esempio da REvil e sfruttate come vettore iniziale. L'NCSC ritiene che questi dati di accesso vengano negoziati dai criminali anche in forum dedicati e che in questo modo diversi gruppi di malintenzionati possano ottenere accesso alle reti delle vittime.

Raccomandazione

Le seguenti misure devono essere attuate primo possibile:

- tutti gli accessi remoti (*RDP*, Citrix, *VPN*) devono essere protetti con un'autentificazione a due fattori;
- inoltre, vanno configurati su una porta non standard in modo da essere più difficili da individuare (attenzione: questa misura da sola non è sufficiente);
- introdurre e applicare una direttiva che impedisca le password semplici;
- se possibile, consentire solo indirizzi IP univoci o svizzeri;
- esaminare i file di log monitorando login falliti e andati a buon fine.

Nell'anno oggetto di questo rapporto sono stati osservati alcuni attacchi ransomware che utilizzano tecniche innovative per aggirare le misure di sicurezza e rimanere più a lungo nella rete della vittima. Ad esempio, RagnarLocker ha sfruttato una propria macchina virtuale Windows XP da 280 MB («Virtual Machine», VM) per funzionare al suo interno senza essere disturbato dai programmi di monitoraggio dell'host. Tutte le unità del computer colpito sono state rese accessibili anche all'interno della VM e il ransomware ha quindi potuto criptarle.[39] NetWalker, per contro, ha perfezionato una tecnica denominata «Reflective DLL injection», già impiegata da altri tipi di malware, che consente di «iniettare» un file DLL così che il codice di esecuzione per il malware si trovi solo nella RAM. Ciò significa che il codice binario del ransomware rimane invisibile per gli strumenti di monitoraggio che analizzano solo il disco fisso.[40] Come ulteriore misura, NetWalker blocca i processi dei programmi di sicurezza.

Evoluzione degli obiettivi

Una tendenza preoccupante che sta emergendo a livello globale riguarda gli attacchi ransomware contro i sistemi di controllo industriali, a cui MELANI dedica un capitolo nel presente rapporto (cfr. n. 4.3.1).

Un'ulteriore evoluzione osservabile di recente è collegata all'infezione Maze comunicata il 18 aprile da Cognizant, uno dei maggiori MSP («*managed service provider*») al mondo.[41] Questo caso si inserisce in una lunga serie di attacchi contro i fornitori di servizi e IT nel secondo semestre 2019.[42] Secondo il rapporto di analisi delle minacce pubblicato a marzo da

39 https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/
40 https://blog.trendmicro.com/trendlabs-security-intelligence/netwalker-fileless-Ransomware-injected-via-reflective-loading/
41 https://www.bleepingcomputer.com/news/security/it-services-giant-cognizant-suffers-maze-Ransomware-cyber-attack/
42 https://www.zdnet.com/article/at-least-13-managed-service-providers-were-used-to-push-Ransomware-this-year/

CrowdStrike si può parlare di una vera e propria tendenza.[43] Tra i ransomware particolarmente attivi contro gli operatori di servizi spicca Ryuk, fra le cui vittime accertate rientrano Data Resolution (dicembre 2018), CloudJumper (maggio 2019), CorVel (luglio 2019) e TSM Consulting (agosto 2019). A marzo 2020 Ryuk ha inoltre colpito il fornitore di servizi fintech Finastra, che fornisce software e servizi a oltre 8500 clienti, fra cui 90 delle 1000 maggiori banche al mondo. Per prevenire una diffusione dell'infezione, Finastra ha rapidamente disattivato una parte dei propri server, con una conseguente interruzione temporanea dei servizi per i numerosi clienti.[44] La compromissione di un MSP o di un fornitore di servizi cloud può produrre danni enormi perché può fungere da porta di accesso in un'impresa di cui il provider gestisce l'infrastruttura informatica, ad esempio tramite software di monitoraggio e gestione remota («*remote monitoring and management*», RMM). Per questo motivo, Cognizant ha prontamente informato la propria clientela, fornendo indicatori di compromissione («*Indicators of Compromise*», IoC) per rilevare un'eventuale infezione sulla propria rete.

Per dare meno nell'occhio, alcuni autori di attacchi ransomware si sono specializzati nell'utilizzare come via di accesso i programmi di cui si serve l'MSP, come le applicazioni per la condivisione del desktop o la gestione remota. È così che in aprile è stato attaccato tramite RagnarLocker il gruppo Energias de Portugal (EDP), uno dei maggiori produttori di energia a livello europeo. Alcuni gruppi criminali dediti ai ransomware, come per esempio Sodinokibi/REvil, seguono il percorso opposto: dopo aver attaccato diversi piccoli MSP, fra cui PerCSoft (agosto 2019), Complete Technology Solutions (dicembre 2019) e Synoptek (gennaio 2020), Coveware nota che da inizio 2020 il gruppo sembra più interessato alle grandi aziende con VPN vulnerabili.

Raccomandazione

Al fine di proteggersi dagli attacchi *ransomware*, raccomandiamo di adottare le misure seguenti, dimostratesi efficaci per le imprese: assicurare l'applicazione di pratiche complete di backup. In questo modo si aumenta la certezza di poter ripristinare tutti i dati dopo un attacco *ransomware*. Ciò comprende anche testare il processo di ripristino dei dati. Documentare l'infrastruttura informatica, effettuare gli aggiornamenti poco dopo il loro rilascio e mantenere sempre attuali le direttive di sicurezza. Elaborare piani per la gestione degli incidenti, la comunicazione e la continuità operativa. Stabilirne l'efficacia effettuando regolari esercitazioni. Per una prevenzione dei ciberattacchi efficace, le misure tecniche di sicurezza dovrebbero essere accompagnate da una regolare sensibilizzazione del personale. Sorvegliare l'attuazione di queste misure è compito degli organi direttivi di un'impresa che non va delegato.

Praticamente nessuna azienda è in grado di respingere con sicurezza tutti i ciberattacchi. È dunque importante sviluppare la propria capacità di reazione e ripristino per limitare le conseguenze di un evento inevitabile.

---

43 https://www.channelfutures.com/mssp-insider/msps-under-heavy-Ransomware-attack ; https://www.crowdstrike.com/press-releases/crowdstrike-global-threat-report-reveals-big-game-hunting-telecommunication-targeting-top-adversary-trends/

44 https://www.bloomberg.com/news/articles/2020-04-08/how-finastra-survived-a-Ransomware-attack-without-paying-ransom

INFO

Nel secondo semestre del 2019 MELANI ha pubblicato le misure di sicurezza aggiornate per proteggersi dalle nuove procedure degli attacchi ransomware:

https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/update-ransomware-neue-vorgehensweise.html

4.1.2 Gozi nuovamente attivo

Il malware Gozi,[45] sviluppato per sferrare attacchi contro i sistemi di e-banking, è presente in Svizzera da oltre un decennio, sebbene negli ultimi anni sia stato attivo solo sporadicamente.

A marzo di quest'anno è stato osservato che Gozi veniva diffuso tramite e-mail in cui si faceva riferimento a una reale corrispondenza elettronica precedente della vittima (cosiddetto «*thread hijacking*»). Questo metodo è già impiegato da altri trojan bancari, fra cui Emotet. L'e-mail conteneva una password per aprire un file ZIP che tuttavia non era in allegato, ma archiviato su Google Drive. Il messaggio sosteneva che nel file compresso fosse contenuta una presentazione. In realtà si trattava di un file Javascript che scaricava ed eseguiva Gozi. Ad aprile il malware è poi stato inviato come allegato in un file XLS infetto. I messaggi, scritti in italiano, facevano riferimento a una fattura.

Negli anni Gozi e le sue varianti (acquistabili su piattaforme online illegali e pertanto utilizzati da diversi cibercriminali) sono stati diffusi in vari modi, anche tramite siti web compromessi di quotidiani online e software manipolati, pubblicizzati tramite inserzioni realizzate ad hoc. Oltre ai sistemi di e-banking, Gozi ha nel mirino anche i software di pagamento e i wallet per criptovalute.[46]

4.1.3 Un modulo di Emotet finora nascosto

All'inizio del 2020 i ricercatori sulla sicurezza di Binary Defense hanno scoperto un modulo WLAN nel malware Emotet[47]. Con questo modulo finora mai studiato vengono consultate le reti senza fili (*wireless local area network*, WLAN) con cui la vittima è collegata. Inoltre, mediante una lista predefinita di password comuni, Emotet cerca di accedere a tutte le altre reti wireless a portata. Se è priva di protezione o la relativa password è contenuta nella lista predefinita, Emotet è in grado di accedere alla rete WLAN. Partendo dalla prima vittima, il malware infetta i computer sulla rete in cui è penetrato e si diffonde.

Secondo le prime informazioni, il modulo sembra esistere dal 2018. Siccome le analisi del malware vengono svolte per la maggior parte su macchine virtuali prive di WLAN, il componente è rimasto a lungo nell'ombra. Questa scoperta dimostra come i criminali cerchino sempre nuove vie per diffondere i software nocivi e quanto siano ingegnosi.

---

45 Contributi su Gozi sul blog GovCERT: https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature; https://www.govcert.ch/blog/when-gozi-lost-its-head/ (in inglese)

46 Cfr. rapporto semestrale MELANI 2018/1, n. 4.7.3

47 https://www.binarydefense.com/emotet-evolves-with-new-wi-fi-spreader/

Emotet è una via di accesso per ulteriori malware come i trojan di crittografia (ransomware).[48]

Conclusione

La diffusione di malware è un costante gioco di guardie e ladri fra gli addetti alla sicurezza informatica e i criminali. Quando i metodi applicati hanno meno successo perché un vettore di diffusione viene contrastato meglio, gli sviluppatori di software nocivi inventano nuove varianti di infezione o ne recuperano di vecchie, a cui gli esperti della sicurezza prestano meno attenzione. In quanto primo componente di rete per il collegamento a Internet, una rete WLAN è un vettore delimitato localmente e non presenta una scalabilità immediata come gli attacchi tramite e-mail e web. Tuttavia, le reti Wi-Fi non vanno sottovalutate come vettore di attacco.

Sul nostro sito Internet trovate le raccomandazioni per WLAN:

https://www.melani.admin.ch/melani/it/home/schuetzen/sekundaere-grundschutz.html

4.2 Attacchi a siti e servizi web

4.2.1 Supercomputer HPC

A metà maggio 2020 il team di sicurezza dell'EGI («European Grid Infrastructure», un consorzio di università dotate di centri di calcolo ad alte prestazioni) ha segnalato un attacco che ha interessato diversi suoi membri.[49] I centri di calcolo ad alte prestazioni («*high-performance computing*», HPC) rappresentano uno strumento importante per risolvere calcoli complessi come i modelli aerodinamici o, attualmente, i modelli di diffusione del COVID-19. La potenza di calcolo può essere utilizzata anche per «*crypto mininig*» o decifrare dati criptati. I centri dispongono inoltre di notevoli ampiezze di banda. Gli HPC sono pertanto obiettivi allettanti per gli hacker. Grazie al rapporto del team di sicurezza EGI, numerosi centri di calcolo in tutto il mondo (fra i quali anche diversi in Svizzera[50]) sono stati in grado di rilevare gli accessi non autorizzati ai propri sistemi e di respingere gli autori degli attacchi. Al momento l'obiettivo di questi ultimi non è ancora noto.

4.2.2 Aggiornamento DDoS

In generale, negli scorsi anni si è assistito a una diminuzione degli attacchi con successo di tipo «*distributed denial of service*» (*DDoS*) mirati a limitare la disponibilità di un sistema informatico per poi estorcere denaro all'organizzazione in questione o arrecarle danno rendendo siti e servizi indisponibili. Ciò è merito degli attori che si impegnano nel campo della sicurezza informatica per la lotta agli attacchi DDoS. Per Link11, un fornitore di servizi per contrastare

48 Cfr. rapporti semestrali MELANI 2019/1, n. 3.4.1, e 2019/2, n. 4.6.1

49 https://csirt.egi.eu/academic-data-centers-abused-for-crypto-currency-mining/

50 https://www.rts.ch/info/suisse/11329094-soupcons-de-hacking-du-plus-gros-superordinateur-de-suisse-.html; https://www.tagesanzeiger.ch/eth-supercomputer-gehackt-370887112689

gli attacchi DDoS, la maggiore offensiva di questo tipo sventata nel primo trimestre 2020 era di 406 Gbit/s, mentre Cloudflare ha registrato un attacco DDoS con un valore di punta di oltre 550 Gbit/s.[51]

Rispetto al 2019, questi servizi hanno riscontrato un aumento della complessità e del volume degli attacchi. Nei primi tre mesi di quest'anno, Link11 ha registrato ben 51 attacchi con un volume superiore a 50 Gbit/s, mentre la larghezza di banda media è stata di 5,0 Gbit/s (pari a un incremento di 0,7 Gbit/s rispetto allo stesso trimestre del 2019).[52] Cloudflare riporta un aumento dei piccoli attacchi di breve durata, il 92 per cento dei quali non raggiunge i 10 Gbit/s. Inoltre, il 72 per cento delle offensive è durato fra 30 e 60 minuti, con un incremento del 19 per cento rispetto agli attacchi brevi osservati nel secondo semestre 2019.[53]

Il numero di attacchi DDoS rilevati da Cloudflare è salito soprattutto da marzo, in concomitanza con la pandemia da COVID-19. Questa constatazione è stata confermata da altre aziende di sicurezza informatica, fra cui Netscout, che afferma di non aver mai registrato prima un numero tanto elevato di attacchi DDoS in una finestra di 31 giorni come fra l'11 marzo e l'11 aprile 2020 (oltre 864 000).[54] In seguito al trasferimento delle attività quotidiane – come il lavoro (home office) e la scuola (home schooling) – a soluzioni online e alla conseguente dipendenza da connettività e disponibilità dei servizi, i cibercriminali contavano su un possibile aumento dell'efficacia di tali attacchi. La politica del distanziamento sociale in diversi Stati ha accresciuto la dipendenza delle economie dalla rete, così come l'importanza di alcuni canali di informazione online. È il caso, ad esempio, dei siti web dei servizi governativi responsabili della salute pubblica, che venivano visitati ogni giorno da numerosi cittadini in cerca di informazioni sul coronavirus. A metà marzo il sito del ministero della salute statunitense è stato vittima di un attacco DDoS che tuttavia non è riuscito a rallentare in maniera significativa i sistemi dell'autorità governativa.[55] Grazie ai fornitori di «*DDoS-as-a-service*», realizzare un'offensiva di questo tipo è rapido e conveniente. I NCSC non ha registrato in Svizzera un aumento significativo degli attacchi DDoS durante la situazione straordinaria. In generale, nella prima metà del 2020 sono state osservate in Svizzera alcune ondate di attacchi generici, perlopiù senza richiesta di riscatto. Ciò indica che i attori volevano solo testare l'infrastruttura colpita o individuare delle vulnerabilità.

Fra tutti questi attacchi deboli e brevi ci sono tuttavia stati anche due casi fra i maggiori mai registrati in questa categoria. Il primo attacco (a metà di febbraio), contenuto dalla protezione di Amazon (AWS Shield), è durato tre giorni e ha raggiunto un picco di traffico di 2,3 Tbit/s. L'offensiva era rivolta contro uno specifico cliente, che Amazon tuttavia non ha reso noto.[56] Il secondo attacco sferrato a fine giugno contro una banca europea, si è distinto non tanto per l'elevata ampiezza di banda (solo 418 Gbit/s), quanto per il flusso di pacchetti dati al secondo più intenso mai registrato: 809 milioni di p/s.[57] Prima di questo evento, respinto dal fornitore di

51 https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/
52 https://www.helpnetsecurity.com/2020/04/20/ddos-attacks-increasing/
53 https://blog.cloudflare.com/network-layer-ddos-attack-trends-for-q1-2020/
54 https://www.netscout.com/blog/asert/measuring-cruellest-month
55 https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response
56 https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/
57 https://blogs.akamai.com/2020/06/largest-ever-recorded-packet-per-secondbased-ddos-attack-mitigated-by-akamai.html

servizi infrastrutturali Akamai, l'attacco DDoS più virulento aveva raggiunto i 580 milioni di pacchetti al secondo.[58] Entrambi gli attacchi nel primo semestre del 2020 possono fregiarsi di essere i maggiori eventi DDoS mai registrati. La difficoltà nello stabilire quale dei due prevalga sull'altro sta nel fatto che i malintenzionati hanno puntato su metodi diversi per ottenere il loro obiettivo: bit al secondo (bit/s) nel primo caso e pacchetti al secondo (p/s) nel secondo. Gli attacchi con un elevato valore di bit/s mirano a paralizzare la pipeline di Internet, mentre le offensive con un elevato numero di p/s puntano a colpire dispositivi di rete o app presso centri dati o su cloud.[59] L'attacco di febbraio ha raggiunto un volume di pacchetti pari a 293 milioni di p/s, un valore molto inferiore a quello di giugno. Fra il 18 e il 21 giugno è stato registrato un terzo attacco con un picco di 754 milioni di p/s. Durato quattro giorni, è stato inviato da oltre 316 000 indirizzi IP a un indirizzo di Cloudflare.[60]

Raccomandazione

Nelle imprese fortemente dipendenti dalla disponibilità di servizi IT è necessario dare la massima priorità alla salvaguardia dei canali corrispondenti. Individuate quali servizi avrebbero conseguenze rilevanti per la vostra organizzazione in caso di interruzione. Pensate anche ai sistemi di base senza i quali le vostre applicazioni commerciali critiche non funzionerebbero. Sviluppate una strategia per gli attacchi DDoS. Devono essere noti gli uffici interni ed esterni competenti, così come le persone che possono intervenire in caso di attacco. Idealmente, un'impresa si occupa del problema delle minacce DDoS prima di un attacco, a livello di direzione nel quadro della gestione generale del rischio, stabilendo a livello aziendale un certo stato di allerta rispetto al tema DDoS. Un attacco DDoS può colpire qualsiasi organizzazione. Parlate con il vostro provider Internet delle vostre esigenze e definite misure preventive adeguate.

DOCU

Lista di controllo con le 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 Sistemi di controllo industriali

La progressiva digitalizzazione e connessione in rete nel campo dei servizi di base porta a una maggiore efficienza nella gestione di prestazioni come l'approvvigionamento di energia elettrica e acqua, ma comporta anche rischi sotto il profilo della vulnerabilità e quindi dell'affidabilità. Mentre questi sistemi tradizionalmente erano limitati a livello locale o regionale e spesso disponevano di una rete fisica, ora sono sempre più spesso controllabili a distanza tramite Internet. Idealmente, gli elementi di comando non sono direttamente raggiungibili tramite Internet, ma tutelati contro gli accessi non autorizzati mediante diverse misure di protezione.

58 https://www.imperva.com/blog/this-ddos-attack-unleashed-the-most-packets-per-second-ever-heres-why-thats-important/
59 https://www.bleepingcomputer.com/news/security/european-bank-suffers-biggest-pps-ddos-attack-new-botnet-suspected/
60 https://blog.cloudflare.com/mitigating-a-754-million-pps-ddos-attack-automatically/

4.3.1 Sistemi di controllo industriali (ICS) puntati dai ransomware

Come descritto nel capitolo 4.1.1, nell'anno in corso il numero degli attacchi con ransomware ha continuato ad aumentare in tutto il mondo. Finora, gli attacchi con ransomware hanno preso di mira l'infrastruttura informatica delle vittime e generalmente i sistemi di controllo sono stati un danno collaterale. Nel primo semestre del 2020 è stato invece osservato un ransomware appositamente progettato per colpire sistemi di gestione dei processi. Stiamo parlando di EKANS: attivo da dicembre 2019 ma noto solamente da inizio anno,[61] questo ransomware dispone capacità specifiche per attaccare i processi collegati ai sistemi di controllo industriali. Impiegato soprattutto per attacchi mirati, dopo essere penetrato nella rete EKANS verifica se i domini interni e gli indirizzi IP coincidono con il bersaglio. Prima di criptare i file, il ransomware trafuga i dati e causa l'arresto di una serie di processi, senza tuttavia manipolarli o inviare comandi. Tali processi non riguardano solo i sistemi di controllo industriali (ICS), ma anche software di sicurezza o gestione, banche dati e soluzioni di backup dei dati. Dragos, il fornitore di servizi di sicurezza che ha pubblicato un dettagliato rapporto su questa minaccia, elenca tra i prodotti ICS colpiti anche il software Proficy Historian di General Electric e i server per la concessione delle licenze di GE Fanuc ma, ma anche l'applicazione HMIWe di Honeywell e le soluzioni di gestione delle licenze FLEXNet, Sentinel HASP e ThingWorx Industrial Connectivity Suite.[62] Dopo la criptazione dei file EKANS pubblica la richiesta di riscatto.

Inizialmente EKANS è stato considerato il caposcuola di questo tipo di attacchi. Nel quadro dell'analisi del malware, Dragos ha tuttavia riscontrato analogie con una variante del ransomware MegaCortex, che aveva preso di mira i sistemi di controllo industriali già dalla scorsa estate. La scoperta di queste analogie ha relativizzato l'importanza di EKANS, anche perché la lista dei processi minacciati da MegaCortex (oltre 1000) è più lunga dell'elenco di EKANS (64). Sebbene entrambi i ransomware colpiscano gli stessi processi di controllo industriali, MegaCortex blocca anche innumerevoli processi di sicurezza. L'unico sviluppo degno di nota di EKANS sarebbe quindi l'offuscamento del codice del programma al fine di renderne più difficile il rilevamento.

Entrambi questi ransomware rappresentano una minaccia per il settore industriale e molte infrastrutture critiche. I ransomware che mirano fondamentalmente all'infrastruttura informatica possono generalmente avere effetto solo sui sistemi di controllo basati su Windows raggiungibili anche via rete e devono pertanto possedere una certa capacità di diffusione. Per contro, EKANS e MegaCortex sono stati sviluppati per colpire specificamente i sistemi di automazione industriale. Tuttavia, finora nessuna delle vittime pubblicamente note di EKANS ha confermato danni agli ICS in seguito a un attacco. Il grande gruppo automobilistico Honda,[63] ad esempio, ha ammesso di essere stato vittima di un'infezione che ha colpito la rete IT, senza tuttavia riscontrare ripercussioni sulla produzione o sulle vendite, né tantomeno conseguenze per la clientela. Il 7 giugno la multiutility Enel[64] ha rilevato una violazione del proprio sistema informatico, ma il programma antivirus è stato in grado di bloccare il ransomware prima che potesse entrare in azione. La rete aziendale è stata temporaneamente isolata a titolo precauzionale.

---

61 https://www.bloomberg.com/news/articles/2020-01-28/-snake-Ransomware-linked-to-iran-targets-industrial-controls; https://www.otorio.com/blog/snake-industrial-focused-Ransomware-with-ties-to-iran/

62 https://www.dragos.com/blog/industry-news/ekans-Ransomware-and-ics-operations/

63 https://www.bleepingcomputer.com/news/security/honda-investigates-possible-Ransomware-attack-networks-impacted/

64 https://www.bleepingcomputer.com/news/security/power-company-enel-group-suffers-snake-Ransomware-attack/

Anche in questo caso i sistemi di controllo non dovrebbero aver subito alcun danno né vi sarebbero state fughe di dati. Fra le vittime pubblicamente note di EKANS rientra anche Fresenius Medical Care, un grande fornitore europeo privato di prodotti e servizi per ospedali. Dopo l'attacco ransomware sono state pubblicate in rete informazioni altamente sensibili (come risultati di esami medici e appunti su trattamenti e allergie, ma anche nomi, professioni, numeri di telefono e indirizzi dei pazienti).[65] Secondo Kaspersky, anche i produttori di veicoli e automobili sono fra le vittime di EKANS; l'azienda di sicurezza Internet ipotizza inoltre che in almeno un caso l'infezione non si sia limitata alla rete degli uffici, visto che il software nocivo è stato rilevato e bloccato sul sistema di videosorveglianza di un'organizzazione in Cina.[66]

Tralasciando i ransomware che mirano principalmente sistemi di controllo industriali, nel primo semestre del 2020 è stato registrato un numero notevole di attacchi contro infrastrutture critiche del settore energetico. Anche questi casi comportano rischi per la produttività di un'impresa. Il 18 febbraio, ad esempio, l'autorità statunitense per la cibersicurezza (CISA) ha rilevato un attacco alla rete per le tecnologie operative (OT) di un impianto di compressione per il gas naturale. Il responsabile (che non è stato reso noto) è penetrato nella rete informatica dell'azienda tramite un link contenuto in un'e-mail mirata. Successivamente, ha potuto spostarsi sulla rete («lateral movement») ed è riuscito ad accedere alla rete OT. L'attore ha quindi avviato la criptazione su entrambe le reti. Fra i processi OT compromessi rientrano interfacce uomo-macchina («*human machine interface*», HMI), la cronologia dei dati e i cosiddetti «server di polling». La vittima è stata costretta a interrompere l'attività per cancellare ogni traccia del malware, con conseguenti perdite di produttività e utili.[67]

Riportiamo di seguito una panoramica sugli attacchi ransomware andati a segno e resi noti, sferrati nel 2020 contro organizzazioni nel settore energetico.

Data	Ransomware	Vittima	Ripercussioni
1° aprile	Maze	Berkine, un gruppo che comprende la società petrolifera statale algerina Sonatrach e il suo partner commerciale statunitense Anadarko	Sono stati pubblicati oltre 500 MB di documenti con informazioni strettamente confidenziali (fra cui l'elenco dei salari e coordinate degli impiegati, informazioni sulle quantità di produzione, budget e finalità).[68]
14 aprile	Ragnar Locker	Energias de Portugal (EDP), multiutility portoghese (energia elettrica e gas)	Dopo la criptazione dei dati aziendali, gli operatori del ransomware hanno chiesto un riscatto di 11 milioni di dollari. Sembra inoltre che i cibercriminali abbiano trafu-

65 https://www.bleepingcomputer.com/news/security/snake-Ransomware-leaks-patient-data-from-fresenius-medical-care/
66 https://ics-cert.kaspersky.com/media/Kaspersky_ics_cert_alert_Snake_EN.pdf
67 https://us-cert.cisa.gov/ncas/alerts/aa20-049a
68 https://www.inter-lignes.com/des-documents-hyper-confidentiels-de-sonatrach-derobes-par-des-hackers/

			gato 10 TB di documenti sensibili minacciandone la pubblicazione e la diffusione di una parte come avvertimento. Secondo le dichiarazioni, l'attacco non dovrebbe aver avuto ripercussioni sull'approvvigionamento elettrico.[69]
30 aprile	NetWalker	Northwest Territories Power Corporation NTPC, azienda elettrica canadese	Secondo l'azienda, i sistemi elettrici non hanno subito interruzioni. Il sito è stato colpito e modificato tramite «defacement» per pubblicare un messaggio dei cibercriminali.[70]
4 maggio	Sconosciuto, le autorità taiwanesi sospettano che i responsabili siano cinesi.[71]	CPC Corp, raffineria petrolifera statale taiwanese	Il sito è stato colpito e diverse stazioni di servizio sono state temporaneamente chiuse perché non era più possibile elaborare i pagamenti con la carta CPC Corp.[72] L'attacco non ha avuto ripercussioni sulla produzione energetica.
14 maggio	REvil / Sodinokibi	Elexon, un intermediario importante della rete elettrica di distribuzione in Gran Bretagna	L'episodio ha riguardato la rete IT interna e ha messo fuori servizio il server e-mail. I sistemi per la distribuzione dell'energia elettrica non hanno subito danni.[73] All'inizio di giugno i responsabili hanno pubblicato sulla darknet una cartella contenente 1280 file rubati.[74]

69 https://www.bleepingcomputer.com/news/security/ragnarlocker-Ransomware-hits-edp-energy-giant-asks-for-10m/
70 https://www.cbc.ca/news/canada/north/ntpc-apparent-Ransomware-attack-1.5551603
71 https://www.cyberscoop.com/cpc-Ransomware-winnti-taiwan-china/
72 https://www.taiwannews.com.tw/en/news/3927869
73 https://www.elexonportal.co.uk/news/view/27108?cachebust=ebf1vtjsp0
74 https://www.theregister.com/2020/06/01/elexon_Ransomware_was_revil_sodinokibi/

Misure di sicurezza

Dove possibile, i gestori dei sistemi di controllo industriali dovrebbero mantenere separati i sistemi IT aziendali e la rete OT. Per quest'ultima bisogna impiegare una struttura a più livelli in cui i processi meno critici siano staccati da quelli realmente critici. Allo stesso modo, occorre verificare che a poter accedere agli ICS sia esclusivamente il personale autorizzato, allo scopo di limitare l'accesso ai sistemi critici a livello sia virtuale sia fisico.

Sul suo sito il NCSC ha pubblicato la lista di controllo «Misure di protezione dei sistemi di controllo industriali (ICS)»:

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

Recentemente la Cybersecurity and Infrastructure Security Agency statunitense ha messo in rete raccomandazioni su questo argomento:

https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf

4.3.2 Attacchi di sabotaggio nell'ambito dei conflitti nel Vicino Oriente

Il 3 gennaio 2020 il generale iraniano Qassem Soleimani, comandante delle forze Quds delle Guardie Rivoluzionarie, e Jamal Jaafar Ibrahim, da anni leader del gruppo Kataib Hezbollah e vicecapo delle Forze di mobilitazione popolare, sono stati uccisi da un attacco aereo statunitense all'aeroporto di Bagdad.[75] Questo attacco cinetico va considerato nel contesto più ampio del conflitto nel Vicino Oriente. Nell'ambito di quest'ultimo, ad ogni modo, gli scontri non avvengono più solo a livello fisico: da anni le parti in causa lottano regolarmente anche nel cyberspazio, senza tirarsi indietro di fronte alle ripercussioni fisiche di questi attacchi o addirittura mirando intenzionalmente a produrli.[76]

A dover sopportare le conseguenze dei ciberattacchi con motivazioni distruttive è stata alla fine del 2019 la società petrolifera nazionale del Bahrein (Bapco).[77] Diversi dispositivi dell'ambiente di sistema sono stati resi inservibili tramite malware. Nonostante Bapco non confermi, si ipotizza una relazione con un avvertimento[78] dell'autorità saudita per la sicurezza relativamente al virus cancellino (*wiper)* Dustman.[79] Il punto di accesso originario sembra essere un sistema di accesso remoto. Nel suo rapporto sull'offensiva Fox Kitten,[80] l'azienda di cyber intelligence Clearsky descrive intromissioni riuscite in reti aziendali tramite accessi *RDP* scarsamente protetti o server VPN non aggiornati e quindi vulnerabili di Pulse Secure, Fortinet o Palo Alto. Nell'arsenale di questi criminali, attivi prevalentemente nel Vicino Oriente, c'è anche lo

75 https://www.defense.gov/Newsroom/Releases/Release/Article/2049534/statement-by-the-department-of-defense/

76 Cfr. rapporto semestrale MELANI 2019/2, n. 5.2.

77 https://www.zdnet.com/article/new-iranian-data-wiper-malware-hits-bapco-bahrains-national-oil-company/

78 https://www.scribd.com/document/442225568/Saudi-Arabia-CNA-report

79 https://malpedia.caad.fkie.fraunhofer.de/details/win.dustman

80 https://www.clearskysec.com/fox-kitten/

script PowDesk,[81] in grado di compromettere i sistemi con il software LANDesk Management Agent. Microsoft ha scoperto ad esempio attacchi tramite il cloud del gruppo HOLMIUM.[82] In tale contesto sono stati utilizzati ulteriori strumenti specifici come POWERTON.[83] Secondo il fornitore di servizi di sicurezza Yoroi, l'attore APT34/Oilrig ha attaccato un server e-mail del governo libanese con l'aiuto del Karkoff Implant.[84] Una volta che questi tentativi di attacco hanno successo e viene stabilito un accesso alla rete finiscono sotto tiro anche i sistemi di controllo. Ad aprile il governo israeliano ha messo in guardia[85] da attacchi contro i sistemi SCADA nel campo dell'approvvigionamento idrico. In seguito sono stati resi noti ulteriori offensive rivolte contro i sistemi di gestione idrica dell'agricoltura israeliana[86] e si ritiene che i ciberattacchi contro il porto iraniano sullo Stretto di Hormuz[87] siano una rappresaglia per questi episodi.

Se il tentativo con le diverse varianti non va direttamente a segno, i criminali si spostano lungo la catena di distribuzione per individuare un eventuale punto di accesso più lontano. A febbraio l'FBI ha messo in guardia contro gli attacchi ai fornitori di software[88] tramite il trojan di accesso remoto Kwampirs.[89] L'attenzione era rivolta in particolare alle aziende attive nel campo dei sistemi di controlla industriale per la produzione, il trasporto e la distribuzione dell'energia.

Nota

Le organizzazioni che operano nel contesto di questi conflitti devono essere consapevoli che sussiste la possibilità di essere colpite (direttamente o indirettamente) da attacchi di questo tipo.

4.3.3 Continuano gli attacchi ricognitivi contro le aziende di approvvigionamento energetico

I gestori delle reti di distribuzione delle aziende elettriche europee collaborano nel quadro dell'associazione ENTSO-E al fine di coordinare l'approvvigionamento elettrico a livello paneuropeo. Nella primavera del 2020 è stato reso noto che nell'ultimo anno questo network ha subito un ciberattacco con tentativo di penetrazione nella rete dei propri uffici. «La rete amministrativa ENTSO-E non è collegata ai sistemi operativi dei gestori delle reti di distribuzione». È quanto ha sottolineato ENTSO-E in un breve comunicato stampa nel marzo 2020.[90] Molti

81 https://www.clearskysec.com/powdesk/
82 https://www.microsoft.com/security/blog/2020/06/18/inside-microsoft-threat-protection-mapping-attack-chains-from-cloud-to-endpoint/
83 https://attack.mitre.org/software/S0371/
84 https://securityaffairs.co/wordpress/98802/apt/karkoff-malware-lebanon.html
85 https://www.gov.il/he/departments/publications/reports/scadaalert
86 https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/
87 https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html
88 https://www.zdnet.com/article/fbi-warns-about-ongoing-attacks-against-software-supply-chain-companies/
89 https://malpedia.caad.fkie.fraunhofer.de/details/win.kwampirs
90 https://www.entsoe.eu/news/2020/03/09/entso-e-has-recently-found-evidence-of-a-successful-cyber-intrusion-into-its-office-network/

dei 42 membri provenienti da 35 Paesi europei (cfr. fig. 6), fra cui anche i rappresentanti svizzeri di Swissgrid,[91] confermano la stima dell'associazione in merito alla portata dell'attacco. L'attacco non avrebbe dunque potuto provocare danni diretti all'approvvigionamento elettrico in Europa.

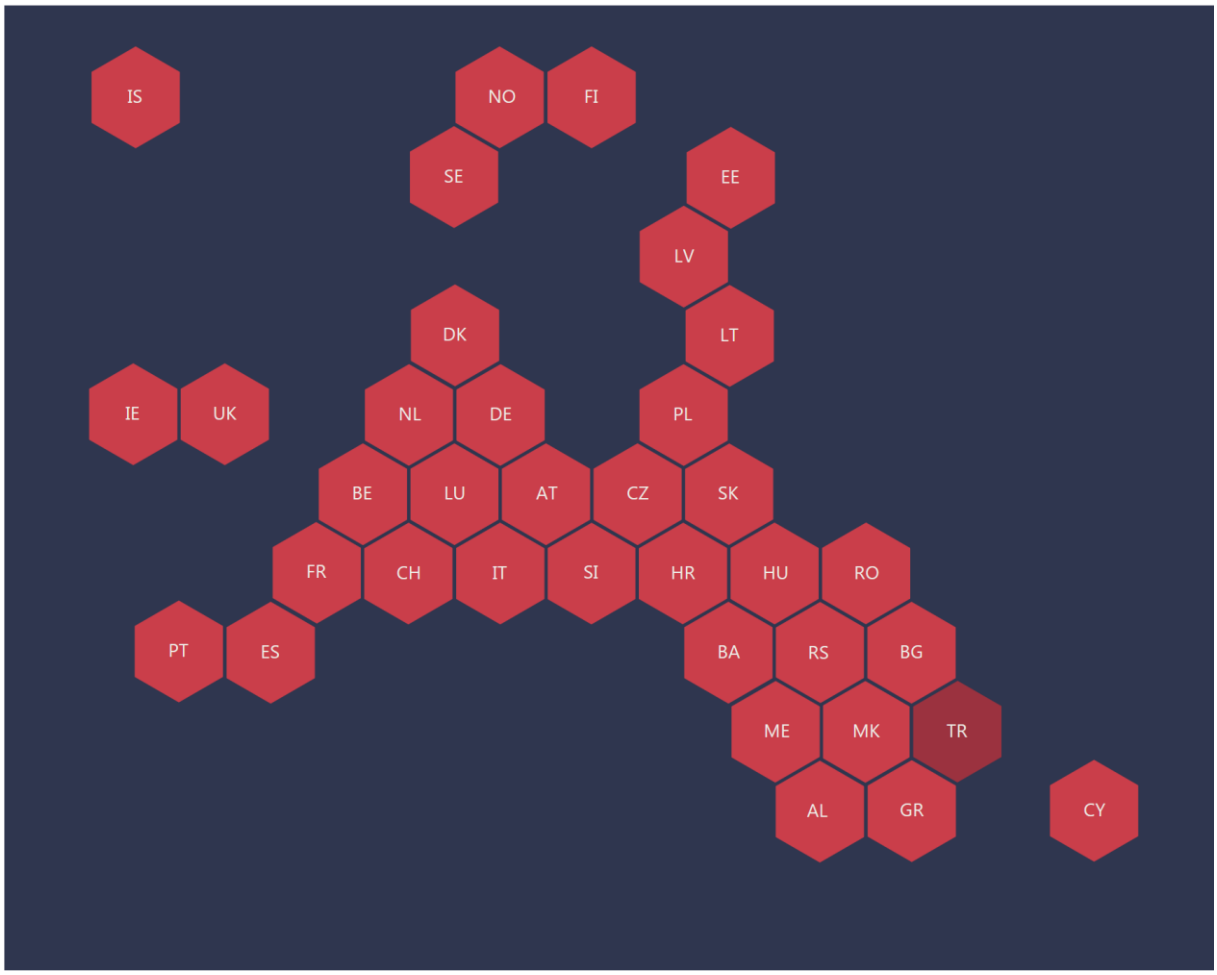

Figura 6: I membri di ENTSO-E[92]

Questo episodio evidenzia la presenza di attori interessati a scoprire come è organizzato il settore dell'energia elettrica in diverse parti del mondo. Il rapporto semestrale precedente conteneva ulteriori riferimenti in merito.[93] L'esempio appena esposto dimostra che nemmeno l'Europa viene risparmiata. I giornalisti specializzati di Cyberscoop[94] riscontrano una relazione tra un'analisi di RecordedFuture[95] e il caso dell'ENTSO-E: in passato il malware impiegato, Pupy RAT, era stato sfruttato anche da gruppi che non avevano esitato a condurre attacchi wiper distruttivi. Questo tipo di offensive è stato registrato finora solo nel contesto di conflitti in atto,

91 https://www.swissgrid.ch/it/home/about-us/newsroom/newsfeed/20200309-01.html
92 https://www.entsoe.eu/about/inside-entsoe/members/
93 Cfr. Rapporto semestrale MELANI 2019/2, n. 4.2.1
94 https://www.cyberscoop.com/europe-grid-pupy-rat/
95 https://www.recordedfuture.com/pupyrat-malware-analysis/

come quelli descritti al numero 4.3.2 sulle tensioni nel Vicino Oriente. In considerazione dei possibili sviluppi geopolitici, ogni Paese e ogni azienda che eroga energia elettrica devono essere preparati ad affrontare attacchi in maniera proporzionata al rischio. Oltre al tentativo di ricognizione osservato in Europa, anche le aziende elettriche statunitensi si sono dovute confrontare con tentativi di violazione delle loro reti[96] nei quali è stato impiegato il malware Flowcloud.[97]

Un recente caso di ransomware, anch'esso senza ripercussioni sui sistemi di controllo operativo, ha riguardato Elexon, l'autorità britannica di sorveglianza sul mercato dell'energia elettrica. Di fronte al rifiuto di cedere alle richieste, il gruppo di Sodinokibi/REvil ha pubblicato i dati precedentemente trafugati.[98] Per il momento sembra che Elexon se la sia cavata piuttosto bene. Bisogna tuttavia considerare che le informazioni pubblicate potrebbero essere utilizzate anche da attori che non perseguono solo interessi finanziari per organizzare futuri attacchi. Ulteriori esempi di stampo simile sono gli episodi citati al numero 4.3.1 che hanno visto in azione RagnarLocker in Portogallo o il ransomware contro la raffineria della CPC Corp a Taiwan. Questi attacchi ransomware rappresentano al momento la minaccia più critica, specialmente nelle versioni che cercano anche di disturbare i sistemi operativi di controllo dei processi fisici.

Nota

Nella cerchia chiusa di clienti di MELANI, il NCSC è in regolare contatto con i rappresentanti delle aziende elettriche svizzere e lavora insieme a loro per riconoscere e prevenire tempestivamente questo tipo di attacchi in Svizzera o per contenerne il più possibile le conseguenze.

4.4 Vulnerabilità

Nel primo semestre del 2020 sono state rese note alcune vulnerabilità particolarmente critiche in relazione al lockdown. In questo periodo molte imprese hanno infatti concesso con maggiore frequenza la possibilità del lavoro a domicilio. L'infrastruttura necessaria a tal fine è complessa e anche in una situazione normale (ossia senza tempistiche straordinariamente ristrette) non è facile da allestire in sicurezza.

La vulnerabilità CVE-2019-19781 comunicata il 17 dicembre 2019 e relativa all'*Application Delivery Controller* (ADC) e ai prodotti *Gateway* di Citrix ha pertanto riguardato molte imprese svizzere, fra le quali anche infrastrutture critiche. Tale vulnerabilità consente all'aggressore di eseguire un codice su dispositivi per i quali non dispone di alcun diritto. Siccome questi prodotti Citrix sono spesso impiegati lungo il perimetro esterno della rete, tramite questa criticità un malintenzionato poteva procurarsi un accesso non autorizzato. Nonostante l'avvertenza di sicurezza e la viva raccomandazione di Citrix di mettere in sicurezza i prodotti, non tutti i clienti hanno provveduto. Il 10 gennaio 2020 sono stati resi noti diversi *exploit* che sfruttavano questa vulnerabilità. Nel giro di qualche ora la ricerca dei prodotti Citrix esposti su Internet e vulnerabili

96 https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new

97 https://www.proofpoint.com/us/blog/threat-insight/flowcloud-version-413-malware-analysis

98 https://www.theregister.com/2020/06/01/elexon_ransomware_was_revil_sodinokibi/

è fortemente aumentata e nei giorni successivi i criminali hanno sfruttato gli *exploit* per compromettere reti aziendali ed estorcere denaro tramite attacchi ransomware. Dopo la pubblicazione di tali *exploit*, il NCSC ha informato in modo risoluto oltre 50 gestori di infrastrutture critiche in merito al potenziale pericolo e alle misure preventive da adottare.

Gli aggressori prendono di mira anche router o server VPN che contengono versioni software con vulnerabilità e non sono protetti da misure supplementari. La loro strategia consiste nel trovare una via di accesso per penetrare nella rete aziendale e successivamente poter ad esempio utilizzare un ransomware. Negli ultimi anni sempre più organizzazioni hanno subito notevoli perdite perché un'applicazione o un prodotto contenente una vulnerabilità resa nota da poco era esposta a Internet.[99]

Raccomandazione

Le imprese dovrebbero tenere un inventario sempre aggiornato della propria infrastruttura informatica. La massima priorità va data ai prodotti esposti a Internet. Il secondo passo consiste nel monitorare vulnerabilità e update con acquisizione, analisi e priorizzazione delle corrispondenti indicazioni dei produttori nel quadro di una gestione del rischio in tempo reale. Infine, occorre pianificare settori e procedure per gli aggiornamenti urgenti degli elementi chiave (in particolare lungo il perimetro).

Le vulnerabilità note sono elencate nella banca dati *Common Vulnerabilities and Exposures* (CVE), disponibile al seguente link: https://nvd.nist.gov

4.5 Fughe di dati

Il fenomeno della fuga di dati non è nuovo, ma nel periodo in esame la frequenza di questo evento è aumentata. Si può inoltre supporre che la tendenza si confermerà anche in futuro. Trafugare o vendere dati aziendali è una delle attività principali di alcuni cibercriminali. Secondo uno studio, nei prossimi due anni una impresa su quattro cadrà vittima di una fuga di dati.[100]

A maggio di quest'anno EasyJet ha dovuto rendere noto di essere stata vittima di un ciberattacco altamente sviluppato che ha riguardato i dati di circa nove milioni di clienti (fra cui indirizzi e-mail, informazioni di viaggio e dati delle carte di credito). Secondo le dichiarazioni dell'azienda ci è voluto tempo per comprendere l'entità dell'attacco e identificare le persone coinvolte. EasyJet non ha fornito dettagli sul tipo di attacco o sulle motivazioni, ma ha affermato che secondo gli accertamenti effettuati gli hacker avrebbero mirato alle proprietà intellettuale dell'impresa e non a informazioni che potrebbero essere utilizzate per furti di identità. Ciononostante, la società ha avvertito i propri clienti dei possibili attacchi phishing, raccomandando come sempre un'elevata attenzione. Secondo il regolamento europeo sulla protezione dei dati (RGPD), EasyJet rischia una sanzione pecuniaria fino al 4 per cento della propria cifra d'affari annua mondiale qualora venisse riscontrato l'errato trattamento dei dati dei clienti. Nel caso in

99 Cfr. rapporti semestrali MELANI 2019/2, n. 4.6.1, e 2020/1, n. 4.1.1

100 https://www.itgovernance.co.uk/blog/do-you-have-a-data-breach-response-plan

cui potesse venir dimostrata una negligenza, sarebbe possibile anche un'azione di risarcimento del danno da parte dei clienti, che aumenterebbe notevolmente i costi per la compagnia aerea.

Nel mese di febbraio, anche la catena di alberghi Marriott International ha comunicato una violazione che potenzialmente ha riguardato i dati personali di 5,2 milioni di ospiti. Marriot International ritiene che l'attacco sia iniziato a metà gennaio 2020. Il caso è stato tuttavia scoperto solo verso la fine di febbraio, quando una quantità insolita di dati degli ospiti è stata richiamata utilizzando le informazioni di accesso di due impiegati di un'affiliata in franchising. Marriott International ha avviato un'indagine, potenziato il monitoraggio e organizzato le risorse per informare e assistere gli ospiti, mettendo anche a disposizione un portale dove le persone potenzialmente potevano chiedere informazioni sulle violazioni della protezione dei dati. Si tratta già del secondo episodio segnalato da Marriot International negli ultimi due anni. Nel novembre 2018 l'impresa aveva infatti reso nota la violazione della banca dati delle prenotazioni di Starwood Hotels.

Secondo un nuovo sondaggio, circa l'80 per cento delle aziende ha dovuto denunciare almeno una violazione dei dati su cloud nei 18 mesi precedenti, e circa il 43 per cento ha notificato dieci o più violazioni.[101] Secondo i 300 responsabili della sicurezza informatica (CISO) che hanno partecipato al sondaggio, le maggiori fonti di preoccupazione in relazione ai dati in ambienti cloud sono le errate configurazioni di sicurezza (67 %), la trasparenza carente nelle impostazioni e nelle attività di accesso (64 %) così come gli errori relativi ai diritti nella gestione delle identità e degli accessi (61 %).[102] Anche le troppe autorizzazioni rappresentano un'insidia e possono passare a lungo inosservate poiché spesso vengono concesse di default quando una nuova risorsa o un nuovo servizio viene aggiunto all'ambiente cloud. Si tratta di un bersaglio primario per gli autori degli attacchi, visto che possono essere utilizzati per attività malevole come il furto di dati sensibili e l'introduzione di malware. Le maggiori priorità nel campo della sicurezza per l'accesso al cloud sono pertanto la tutela della riservatezza dei dati sensibili, il rispetto delle disposizioni legali e l'assicurazione del corretto livello di accesso.

La motivazione per il furto di dati può essere non solo finanziaria, ma anche di natura ideologica. Il 19 giugno 2020, il gruppo Distributed Denial of Secrets (DDoSecrets) ha ad esempio rilasciato un dump di dati da 269 GB contenente 24 anni di informazioni registrate da oltre 200 centrali di polizia negli Stati Uniti.[103] L'obiettivo dichiarato era avere libero accesso ai dati di interesse pubblico, così come la trasparenza collettiva. Il probabile movente dietro alla fuga di dati rimanda invece a una ritorsione nel quadro dell'attuale protesta antirazzista contro la polizia negli Stati Uniti. Un leak di questa entità a danno delle autorità di perseguimento penale è senza precedenti. Fra gli innumerevoli documenti, come ad esempio rapporti e bollettini dell'FBI contenenti dati personali, si trovano anche dati bancari completi, foto di sospettati, numeri di telefono e indirizzi e-mail di vittime e autori dei reati. È ovvio che i dati potranno essere utilizzati anche in futuro da hacktivisti e cibercriminali. In questo caso a preoccupare le autorità è soprattutto il rischio per le vittime. L'autenticità dei dati è stata nel frattempo confermata. La fonte del leak è una fuga di dati presso Netsential, un'azienda che sviluppa software con sede a Houston in Texas. Al momento non è ancora chiaro in che misura questa violazione avrà ripercussioni sugli altri clienti.

---

101 https://www.helpnetsecurity.com/2020/06/03/cloud-data-breach/

102 https://www.itgovernance.co.uk/blog/do-you-have-a-data-breach-response-plan; https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

103 https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/

Come già ricordato al numero 4.1.1, ormai anche nei casi di ransomware bisogna sempre mettere in conto il rischio di una fuga di dati. Uno dei motori di questa evoluzione è il gruppo Maze, che ha creato uno speciale sito (Maze News) sul quale vengono resi pubblicamente accessibili i dati delle vittime che non hanno ceduto alle richieste di riscatto. Questa tattica estorsiva è stata presto adottata anche da altri gruppi criminali, tra i quali Nefilim, Sekhmet e Sodinokibi/REvil. Con il pagamento di riscatti che ammontano in media a oltre 100 000 dollari e alcune vittime che avrebbero pagato milioni, singoli gruppi avrebbero tratto grandi profitti già solo con le estorsioni alle imprese. Tuttavia, recentemente è stata segnalata da vari rapporti una collaborazione tra i gruppi Maze e Lockbit, nonché gli operatori di Sodinokibi/REvil, che quando le vittime non pagano non si limitano a pubblicare i dati rubati ma li vendono all'asta al miglior offerente. L'organizzazione dei gruppi basata sulla suddivisione del lavoro, lo scambio di consigli e tattiche, nonché una piattaforma centralizzata per le fughe di dati consentono alle bande di ricattatori di concentrarsi maggiormente sullo sviluppo di attacchi sempre più raffinati e tentativi di estorsione sempre più efficaci. Questa divisione dei compiti è già stata riscontrata in alcuni casi. Sono infatti emersi leak di informazioni provenienti non da un attacco ransomware tramite Maze ma da un altro episodio, di cui era responsabile LockBit.

Nel campo dei ransomware e delle fughe di dati si profila chiaramente una tendenza alla «prestazione di servizi»: la criptazione tramite ransomware e la fuga di dati possono essere acquistate sulla darknet come servizio. Un'ulteriore novità è il fatto che i dati non vengono semplicemente pubblicati, bensì venduti o addirittura messi all'asta.

Conclusione / Raccomandazione

La gestione attenta e responsabile dei dati è un campo minato che le imprese non devono sottovalutare. Se, da un lato è in gioco la reputazione dell'azienda e i costi conseguenti sono notevoli, dall'altro le persone e i clienti hanno il diritto di pretendere che imprese e organizzazioni trattino in modo sicuro e responsabile i loro dati personali. Un'importante misura consiste nell'elaborazione di un piano di risposta alle violazioni («*data breach response*»). La sola preparazione di un piano di questo tipo permette di identificare i settori che presentano rischi specifici e come questi possono essere ridotti al minimo.

La descrizione di cui sopra mette in luce quanto diversi siano gli approcci che possono sfociare in una fuga di dati. Ogni impresa dovrebbe prepararsi per uno scenario di questo tipo, prevedendo tra l'altro le seguenti misure: inventario di sistema, analisi delle minacce e delle vulnerabilità, stima, valutazione e minimizzazione del rischio, perfezionamento costante dei meccanismi di controllo e monitoraggio.

Nel caso in cui l'impresa sia comunque colpita da una fuga di dati, deve assolutamente essere già predisposto un piano di risposta alle violazioni che consenta un'azione rapida e coordinata. Oltre alle classiche misure di gestione degli attacchi, il piano deve comprendere anche processi volti a rilevare l'entità del danno (quali dati sono interessati dal leak e in che misura), nonché all'informazione delle vittime e al reporting. Se sono necessarie prestazioni esterne (consulenza, supporto operativo ecc.) è importante conoscere in anticipo i partner e aver concordato il servizio mediante un contratto. La comunicazione (sia con gli interessati sia con i media) è un altro punto centrale che deve essere disciplinato non solo nei contenuti, ma per il quale occorre stabilire anche la disponibilità delle risorse (ad es. supporto per la gestione di un'ondata di telefonate e e-mail). Oltre a un'analisi tecnica e a una stima dell'evento, potrebbe essere necessaria una tempestiva valutazione giuridica della situazione e delle possibili conseguenze legali e finanziarie. Infine, occorre considerare anche la gestione della reputazione.

4.6 Spionaggio

Come hanno dimostrato una volta di più gli eventi degli ultimi mesi, lo spionaggio continua a essere una minaccia molto reale. Il ruolo di protagonisti spetta ancora a gruppi statali o sponsorizzati dagli Stati. Esistono tuttavia già anche imprese private che possono essere ingaggiate per azioni volte a carpire informazioni in modo mirato (cfr. n. 4.6.3).

4.6.1 Lo spionaggio ai tempi della COVID-19

Secondo Kaspersky, nel primo semestre del 2020 *APT* come Kimsuky, APT27, Lazarus, ViciousPanda e altri ciberattori hanno sfruttato la crisi del coronavirus per i propri interessi.[104] Nonostante la pandemia non abbia avuto alcuna influenza su tattiche, tecniche e procedure impiegate («tactics, techniques and procedures», TTP) da questi gruppi in diversi scenari di attacco il virus è stato il tema principale (cfr. n. 3.1 sull'ingegneria sociale).

Durante una pandemia l'interesse per le informazioni si concentra necessariamente sul settore sanitario nel suo significato più ampio. L'OMS, uno degli attori chiave durante la crisi globale, è stata ad esempio attaccata con una frequenza nettamente maggiore rispetto ai periodi normali. Come ha dichiarato a Reuters il responsabile della sicurezza informatica dell'OMS, i tentativi di spionaggio sono stati opera di hacker d'élite.[105] Oltre all'OMS, nel mirino di questi attacchi sono finiti anche diversi istituti di ricerca che lavorano per trovare un vaccino contro la COVID-19. Si è infatti scatenata una vera e propria corsa alla scoperta di questo vaccino. Stati Uniti, Canada e Gran Bretagna hanno accusato un servizio segreto russo di spiare le istituzioni dei loro Paesi.[106] Gli Stati Uniti hanno inoltre denunciato due cittadini cinesi, accusati di aver effettuato operazioni di spionaggio per conto del ministero cinese della sicurezza pubblica.[107] Tali tentativi miravano a società statunitensi nel campo delle biotecnologie attive nella ricerca di un vaccino contro la COVID-19.[108] Sembra che gli hacker accusati facciano parte di un gruppo criminale che svolge campagne di spionaggio in molti settori perlomeno dal 2009 e ha ottenuto ingenti profitti in particolare attraverso il furto di proprietà intellettuali.

4.6.2 Lo spionaggio economico è realtà anche in Svizzera

Lo spionaggio economico consiste nell'acquisizione di informazioni o dati economici, scientifici o tecnologici su cui viene consapevolmente mantenuto il segreto (segreti commerciali). L'entità dello spionaggio economico in Svizzera è difficile da valutare considerata l'estrema sensibilità dell'argomento e la quasi totale mancanza di dati pubblicamente disponibili. Per dare maggiore visibilità al problema, il Servizio delle attività informative della Confederazione (SIC) ha commissionato uno studio sulla situazione in Svizzera. A gennaio 2020 è stato pubblicato lo studio

---

104 https://securelist.com/apt-trends-report-q1-2020/96826/

105 https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN

106 Gran Bretagna: https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development; Stati Uniti: https://us-cert.cisa.gov/ncas/current-activity/2020/07/16/malicious-activity-targeting-covid-19-research-vaccine-development; Canada: https://cse-cst.gc.ca/en/media/2020-07-16

107 https://www.courtlistener.com/recap/gov.uscourts.waed.91446/gov.uscourts.waed.91446.15.0.pdf

108 https://www.cisa.gov/publication/fbi-cisa-psa-prc-targeting-covid-19-research-organizations; https://www.nytimes.com/2020/07/21/us/politics/china-hacking-coronavirus-vaccine.html

qualitativo e quantitativo sullo spionaggio economico contro le imprese svizzere di diverse dimensioni in diversi rami economici condotto dall'Istituto di diritto penale e criminologia dell'Università di Berna.[109]

I risultati dello studio dimostrano che tra il 15 e il 33 per cento delle imprese svizzere (a seconda delle loro dimensioni) è interessato dal fenomeno dello spionaggio economico. Particolarmente a rischio sono i settori dell'informatica, delle telecomunicazioni, delle scienze della vita, della meccanica, dell'industria e della farmacologia. Nel 40 per cento dei casi erano coinvolti collaboratori (passati o attuali) dell'impresa in questione. In altri settori, a finire nel mirino dello spionaggio economico possono essere soprattutto aziende che realizzano un prodotto di nicchia o uno speciale prodotto rilevante per la sicurezza. Le imprese che hanno partecipato allo studio segnalano la difficoltà di distinguere gli attacchi che mirano direttamente a ottenere un profitto finanziario da quelli che puntano ad acquisire dati a fini di spionaggio. Altrettanto difficile è l'attribuzione dei casi, tanto che per il 38 per cento di essi questa operazione è impossibile. Fra i danni causati, i più frequenti sono stati: perdita di vantaggi competitivi (18 %), avaria dei sistemi informatici (14 %), nonché perdita di clienti e commesse (11 %). Nell'11 per cento dei casi l'esistenza stessa dell'impresa è stata messa in pericolo.

4.6.3 Spionaggio su commissione

A giugno 2020 il laboratorio di ricerca canadese Citizen Lab ha pubblicato un rapporto su massicce attività di spionaggio «hack for hire» da parte del gruppo Dark Basin,[110] che dal 2017 prende di mira giornalisti e attivisti, ma anche banche, fondi speculativi e imprese attive in altri settori. Secondo le dichiarazioni di Citizen Lab è molto probabile che vi sia un collegamento con l'azienda indiana BellTroXInfoTech Services. Pare che il gruppo abbia agito per conto di diversi committenti non identificati.

In una di queste operazioni una grande offensiva di phishing ha preso di mira diverse organizzazioni non profit accomunate dal fatto di aver partecipato alla campagna «#exxonknew». Quest'ultima accusava il gruppo statunitense Exxon, attivo nel settore degli oli minerali, di aver consapevolmente minimizzato per decenni le conseguenze dei cambiamenti climatici. Un'altra campagna di Dark Basin ha colpito gli impiegati dell'azienda tedesca attiva nella tecnofinanza Wirecard AG, come pure i giornalisti che stavano indagando sulla sospetta truffa commessa in relazione a questa impresa.[111]

4.6.4 Novità da Winnti

Il fornitore di servizi di sicurezza FireEye ha scoperto una vasta azione di spionaggio da parte del gruppo cinese APT41,[112] che fra il 20 gennaio e l'11 marzo 2020 ha cercato di sfruttare vulnerabilità presso 75 clienti FireEye nelle applicazioni Citrix NetScaler/ADC, Cisco-Router e Zoho ManageEngine Desktop Central. L'attacco ha colpito molti paesi, tra cui anche la Svizzera, e ha interessato i settori più disparati, compresi quello governativo e quello finanziario.

---

109 https://boris.unibe.ch/139072/

110 https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/

111 https://www.ft.com/content/19c6be2a-ee67-11e9-bfa4-b25f11f42901

112 https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html

APT41 è un attore altamente sviluppato che diversifica regolarmente le proprie attività. Il gruppo è noto anche con il nome di Winnti ed era già stato menzionato nello rapporto semestrale precedente.[113]

4.6.5 Sandworm prende di mira popolari server e-mail Linux

Il 28 maggio 2020 il servizio di intelligence statunitense NSA ha pubblicato raccomandazioni per difendersi dai tentativi di penetrazione tramite vulnerabilità dell'*Exim Mail Transfer Agent (MTA).*[114] Nel suo comunicato stampa, l'NSA attribuisce la responsabilità degli attacchi al gruppo Sandworm, associandolo al Centro principale per le tecnologie speciali (GTsST) del GRU, i servizi segreti militari russi. Sandworm è sospettato di aver quanto meno partecipato agli attacchi contro la rete elettrica ucraina alla fine del 2015[115] e nel 2016[116].

La vulnerabilità CVE-2019-10149 era nota già da un anno e da tempo erano disponibili aggiornamenti per i sistemi interessati.[117] Tuttavia, al momento dell'avvertimento tramite il motore di ricerca dedicato Shodan si contavano ancora circa 2,5 milioni di sistemi a rischio.[118] Exim MTA viene impiegato di frequente perché è il software che garantisce la funzione e-mail predefinita in molte distribuzioni Linux. I sistemi vulnerabili consentono agli aggressori di introdurre ed eseguire da remoto qualsiasi codice.

4.6.6 La minaccia costante di Berserk Bear

Da quando gli Stati Uniti nella primavera del 2018 avevano avvertito dei tentativi di ricognizione del gruppo[119] condotti all'epoca prevalentemente contro aziende elettriche statunitensi, gli autori di questi attacchi sono finiti ripetutamente nei titoli dei giornali.[120] Infine, è stata resa nota la compromissione del sito dell'aeroporto di San Francisco,[121] attraverso la quale gli autori avevano cercato di carpire dati di accesso di ignari visitatori.[122]

Dopo che già il giorno precedente i giornalisti specializzati di Cyberscoop avevano riportato l'avvertimento delle autorità tedesche,[123] il 27 maggio 2020 i telegiornali tedeschi hanno annunciato con frasi a effetto che gli «orsi russi» erano sospettati di essere i responsabili di attacchi hacker.[124] In un documento non destinato alla divulgazione, i servizi segreti federali (BND), l'Ufficio federale per la protezione della costituzione (BfV) e l'Ufficio federale per la sicurezza delle tecnologie dell'informazione (BSI) mettono in guardia da continui tentativi di

---

113 Cfr. rapporto semestrale MELANI 2019/2, n. 4.1.2.

114 https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2196511/exim-mail-transfer-agent-actively-exploited-by-russian-gru-cyber-actors/

115 Cfr. rapporto semestrale MELANI 2015/2, n. 5.3.1.

116 Cfr. rapporto semestrale MELANI 2016/2, n. 5.3.1.

117 https://www.qualys.com/2019/06/05/cve-2019-10149/return-wizard-rce-exim.txt

118 https://www.bleepingcomputer.com/news/security/nsa-russian-govt-hackers-exploiting-critical-exim-flaw-since-2019/

119 https://us-cert.cisa.gov/ncas/alerts/TA18-074A

120 https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112

121 https://www.bleepingcomputer.com/news/security/russian-hackers-tried-to-steal-san-francisco-airport-windows-accounts/

122 https://attack.mitre.org/techniques/T1187/

123 https://www.cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/

124 https://www.tagesschau.de/investigativ/br-recherche/hacker-angriff-infrastruktur-101.html

attacco da parte del gruppo noto con lo pseudonimo Berserk Bear.[125] La minaccia è rivolta in particolare contro aziende del settore energetico, idrico e delle telecomunicazioni.

Il BfV aveva messo in guardia da questi attacchi, diretti anche contro imprese tedesche, già nell'estate 2018.[126] Secondo le ricerche della radio bavarese, le autorità tedesche sono state costrette a segnalare ancora una volta il pericolo con una certa enfasi a causa del perdurare dei tentativi di compromissione, in parte andati anche a buon fine.

Nota

Berserk Bear è un attore che in passato si era già fatto strada più volte nelle reti fino ai sistemi con collegamenti ai controlli di processo, ad esempio l'approvvigionamento elettrico. Una volta lì non manca molto per poter attuare un cibersabotaggio con conseguenze anche fisiche.

4.6.7 L'Australia bersaglio di ciberattacchi

Secondo le dichiarazioni del governo, negli ultimi mesi l'Australia è stata bersaglio di un'intensa ondata di attacchi altamente sviluppati con un gran numero di istituzioni governative, politiche, del settore dell'istruzione e di quello sanitario, nell'industria e presso i gestori di infrastrutture critiche. Nonostante l'Australia sia già finita spesso nel mirino degli autori di attacchi, questa ondata si è contraddistinta per l'elevata frequenza, l'entità, la tecnologia perfezionata e le potenziali conseguenze.

Secondo un rapporto dell'Australian Cyber Security Centre,[127] i criminali impiegavano una tattica «copy-paste-compromise» per penetrare nei sistemi delle proprie vittime. Ciò significa che gli aggressori hanno sfruttato prevalentemente *exploit* preesistenti e altri strumenti open-source che potevano semplicemente «copiare e incollare». Per accedere alle reti prese di mira sono state ad esempio sfruttate vulnerabilità nelle versioni non aggiornate di Telerik UI, Microsoft Internet Information Services (IIS), Sharepoint o Citrix (cfr. n. 4.4). Là dove ciò non era possibile, gli hacker hanno impiegato tecniche di *spear phishing*. Attraverso identità rubate i malintenzionati ottengono accessi remoti legittimi. Tramite *webshell* e traffico *HTTP/HTTPS* hanno poi sfruttato siti web compromessi come server *«command and control»*. Una volta penetrati nella rete venivano impiegati strumenti open source o sviluppati su misura, mirati a garantire persistenza («persistence») e interazione sulla rete.

Il governo australiano ritiene di avere a che fare con attacchi da parte di uno Stato, anche se il primo ministro Scott Morrison non ha fatto nomi. Successivamente, fonti governative hanno indicato la Cina come presunta responsabile dell'attacco.[128]. Il governo cinese ha prontamente smentito, accusando lo Strategic Policy Institute di aver formulato accuse intenzionalmente false.[129]

---

125 https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf

126 https://www.wirtschaftsschutz.info/SharedDocs/Kurzmeldungen/DE/ITSicherheit/Cyberbrief_1_18_dow.html

127 https://www.cyber.gov.au/sites/default/files/2020-06/ACSC-Advisory-2020-008-Copy-Paste-Compromises.pdf

128 https://www.theguardian.com/australia-news/2020/jun/19/australia-cyber-attack-attacks-hack-state-based-actor-says-australian-prime-minister-scott-morrison

129 https://www.abc.net.au/news/2020-06-19/china-responds-to-accusation-of-australia-cyber-attack/12375324

Meno di un mese dopo che gli attacchi sono stati resi noti, un gruppo di esperti incaricato dal governo australiano ha pubblicato un rapporto contenente raccomandazioni per la strategia australiana per la cibersicurezza 2020.[130] Le raccomandazioni riguardano cinque ambiti:

- deterrenza: dissuadere gli attori malintenzionati dal compiere attacchi contro obiettivi australiani;
- prevenzione: impedire la compromissione online di persone e settori;
- rilevamento: riconoscere le ciberminacce e reagire rapidamente;
- resilienza: ridurre al minimo le conseguenze dei casi rilevanti per la cibersicurezza;
- investimenti: investire nella cibersicurezza.

Per l'attuazione della nuova strategia, l'Australia intende investire nei prossimi dieci anni ben 1,35 miliardi di dollari australiani (c. 900 mio. fr., una cifra senza precedenti). Circa un terzo della cifra sarà destinato all'assunzione di 500 specialisti della cibersicurezza presso il governo australiano.[131]

4.6.8 L'Austria nel mirino

L'Austria è stata teatro di due attacchi di spionaggio resi noti negli ultimi mesi. All'inizio del 2020 un'offensiva condotta a quanto pare da un attore statale ha colpito il ministero degli esteri austriaco. Non sono stati divulgati ulteriori dettagli.[132]

Lo scorso mese di giugno A1 Telekom Austria, il maggiore operatore telefonico austriaco, ha confermato un attacco dopo che una fonte vicina all'azienda aveva avvisato un esperto di sicurezza.[133] Sembra che l'operazione, scoperta nel dicembre 2019, sia avvenuta già nel mese di novembre. Ci sono voluti sei mesi prima che A1 Telekom Austria si liberasse definitivamente dagli hacker.[134] Secondo l'azienda, i malintenzionati hanno compromesso solo una parte della sua rete e la complessità dei sistemi ha evitato problemi più gravi. Come si è visto, i malintenzionati si sono ad ogni modo potuti espandere notevolmente, ottenendo prima i diritti di un amministratore locale e successivamente quelli di dominio, accedendo così alla rete Windows.[135] A1 Telekom Austria ha dichiarato che gli intrusi non hanno sottratto alcun dato. L'informatore afferma per contro che gli autori dell'attacco avrebbero messo le mani su dati sensibili dei clienti. A1 Telekom Austria non è stata in grado di individuare la provenienza dei responsabili, diversamente dalla fonte anonima che ha ascritto l'episodio al gruppo di hacker di Stato cinesi Gallium, specializzato in gruppi attivi nel campo delle telecomunicazioni.

130 https://www.homeaffairs.gov.au/cyber-security-subsite/files/2020-cyber-security-strategy-iap-report.pdf
131 https://www.itnews.com.au/news/govt-reveals-135bn-investment-into-cybersecurity-over-next-decade-549856
132 https://www.bbc.com/news/world-europe-50997773
133 https://blog.haschek.at/2020/the-a1-telekom-hack.html
134 https://www.zdnet.com/article/hackers-breached-a1-telekom-austrias-largest-isp/
135 https://www.heise.de/hintergrund/Massiver-Angriff-auf-A1-Telekom-Austria-4775451.html

4.7 Ingegneria sociale e phishing

4.7.1 Phishing

I sistemi come Google reCAPTCHA v3 hanno rivoluzionato il funzionamento dei CAPTCHA. Si tratta di sistemi di sicurezza che consentono a un sito web di escludere che dietro all'apparente utente si celi un robot ricorrendo a puzzle da completare o scritte distorte da interpretare. In questo modo si vuole per esempio evitare che un modulo possa essere compilato numerose volte in maniera automatizzata. I reCAPTCHA agevolano questo processo semplicemente invitando i visitatori del sito a confermare di non essere robot con un click nella casella corrispondente.

I ricercatori dell'azienda di sicurezza informatica Barracuda hanno rilevato che i cibercriminali sfruttavano i reCAPTCHA di Google per rendere meno facili da individuare i propri attacchi.[136] Grazie a questa misura, i sistemi automatici di sicurezza per la verifica dei link nelle e-mail non possono accedere alla pagina di phishing vera e propria e quindi non riescono a riconoscerla come tale. L'inserimento di un reCAPTCHA prima della pagina di phishing offre ai criminali un ulteriore vantaggio, visto che questa viene percepita dai visitatori come una misura di sicurezza, confermando in loro l'errata convinzione di essere su un sito web legittimo. Nel quadro dell'attacco osservato da Barracuda, i cibercriminali hanno inviato un'e-mail con un messaggio vocale in allegato, affermando che fosse stato registrato dalla segreteria. Cliccando sull'allegato, il destinatario veniva reindirizzato a una pagina Internet contenente solo il reCAPTCHA. Dopo aver confermato di non essere un robot si giungeva su una pagina camuffata da pagina di login di Microsoft.[137]

Attacchi simili dotati di CAPTCHA sono stati osservati anche in Svizzera, ma non contro marchi svizzeri quanto contro sistemi internazionali di pagamento utilizzati anche dai cittadini svizzeri (ad es. PayPal).

Phishing as a service

Il «cybercrime as a service» (CaaS) è un concetto diffuso da anni in tutti i settori della cibercriminalità. Sulla darknet si può trovare un'ampia gamma di strumenti di attacco. Secondo l'azienda di sicurezza informatica singalese Group-IB, sono sempre più richiesti i set per attacchi phishing, con un raddoppiamento delle offerte rispetto all'anno precedente. È stato inoltre riscontrato un rincaro di questi prodotti. L'espressione «set per attacchi phishing» indica set di script che consentono di gestire un sito web di phishing. Fra i marchi più popolari usati nel 2019 a scopi di phishing si possono citare Amazon, Google, Instagram, Office 365 e PayPal. Ciò significa che i set di phishing per marchi molto noti con un gran numero di utenti sono i più richiesti. Questi strumenti vengono per così dire venduti chiavi in mano a cibercriminali con limitate capacità tecniche e consentono la realizzazione di innumerevoli pagine di phishing.[138]

---

136 https://blog.barracuda.com/2020/04/30/threat-spotlight-malicious-recaptcha/

137 https://hotforsecurity.bitdefender.com/blog/cybercriminal-are-using-google-recaptcha-to-hide-their-phishing-attacks-23156.html

138 https://securityaffairs.co/wordpress/101616/cyber-crime/underground-market-phishing-kits.html

La situazione in Svizzera

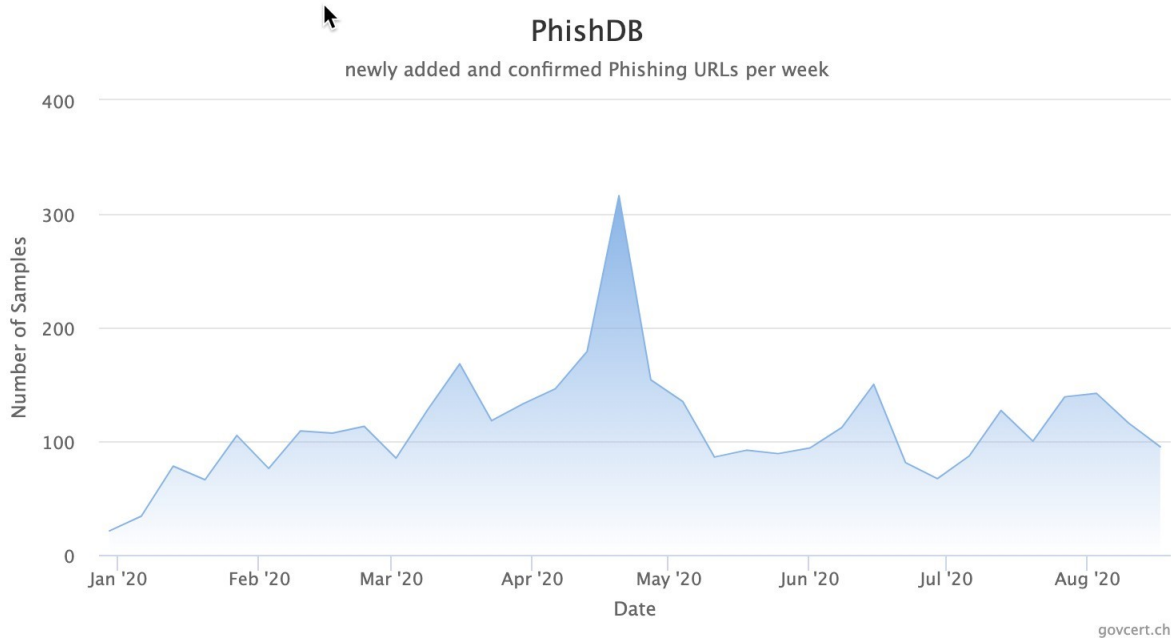

Figura 7: Pagine di phishing segnalate e confermate settimanalmente su antiphishing.ch nel primo semestre del 2020

Nel primo semestre del 2020 sul portale antiphishing.ch gestito dal NCSC sono stati segnalati complessivamente 3029 casi di siti riconosciuti senza dubbio come phishing. La figura 7 mostra i siti di phishing notificati settimanalmente nel primo semestre del 2020.

Dallo scorso aprile il NCSC ha registrato un aumento degli attacchi phishing contro gestori di siti e proprietari di domini. Per ottenere i dati di accesso per l'amministrazione dei siti, i cibercriminali hanno inviato a relativi gestori e proprietari dei domini e-mail di phishing apparentemente spedite dai corrispondenti hosting provider. La maggior parte di queste e-mail conteneva un link personalizzato che tramite un sito web infetto reindirizzava sulla pagina di phishing finale. Qui era già precompilato il nome di dominio e/o il nome del fornitore del servizio di hosting e la vittima veniva invitata a inserire i propri dati di accesso.

Raccomandazione

INFO

Sul proprio blog, GovCERT ha pubblicato un articolo (in inglese) che descrive nel dettaglio gli attacchi rivolti contro i webmaster, assieme a raccomandazioni generali per gli utenti e specifici consigli per gli hosting provider.

4.7.2 Spoofing: mittente contraffatto

In campo informatico, spoofing (dall'inglese «to spoof» = ingannare qualcuno o falsificare qualcosa) indica la simulazione d'identità, in particolare modificando elementi dell'indirizzo come il mittente di un'e-mail o un numero di telefono; tuttavia, anche siti web, indirizzi IP, indirizzi MAC («Media Access Protocol») o messaggi ARP («Address Resolution Protocol») possono essere

contraffatti[139]. Lo spoofing viene impiegato per trasmettere ai destinatari la sensazione di affidabilità e indurli a tenere un determinato comportamento. Siamo pertanto in presenza di una tecnica di ingegneria sociale.

Le tecniche di spoofing vengono costantemente sviluppate e migliorate parallelamente alle possibilità digitali. Per questo motivo, nonostante le misure di protezione disponibili in alcuni casi, si tratta di un fenomeno ampiamente diffuso. Tanto i cibercriminali quanto gli hacker di Stato impiegano con successo un gran numero di diversi metodi di spoofing in differenti contesti. A tale scopo falsificano indirizzi e-mail, numeri di telefono, mittenti di SMS, loghi e denominazioni aziendali per sfruttare la fiducia umana e le esigenze di informazione dei destinatari. Durante la pandemia di COVID-19, ad esempio, sono stati inviati alla popolazione svizzera software nocivi via e-mail utilizzando l'Ufficio federale della sanità pubblica (UFSP) come mittente contraffatto (cfr. n. 3.1.1).

Spoofing di indirizzi e-mail: lo spoofing di indirizzi e-mail è facile da realizzare, visto che il protocollo SMTP («Simple Mail Transfer Protocol») utilizzato non verifica l'indirizzo del mittente. Se un server e-mail è liberamente disponibile su Internet senza protezioni, qualsiasi utente può collegarsi e inviare messaggi di posta elettronica. Il nome del mittente visualizzato può essere impostato a piacimento. A meno che sul server e-mail non siano configurate limitazioni, è possibile definire liberamente anche l'indirizzo del mittente, che può contenere un nome di dominio non associato al server in questione, come ad esempio fatture@ncsc.ch.

È tuttavia possibile adottare alcune misure tecniche di protezione:

- nel sender policy framework (SPF) è possibile registrare i server autorizzati a inviare e-mail con un determinato dominio come indirizzo mittente. I server di invio, trasmissione e ricezione possono verificare le e-mail sulla base dell'SPF, scartandole se necessario;

- il metodo DKIM («DomainKeys Identified Mail») associa a un'e-mail una firma digitale tramite la quale il sistema di destinazione può verificare che il dominio contenuto nell'indirizzo del mittente sia corretto e che l'e-mail non abbia subito modifiche durante il percorso di recapito. Se il controllo non va a buon fine, l'e-mail viene respinta;

- il sistema DMARC («Domain-based Message Authentication and Conformance») si basa sull'autenticazione del mittente (SPF) nonché sulla verifica dell'integrità (DKIM) e presuppone una verifica della firma.

Spoofing di numeri di telefono e mittenti di SMS: grazie alla telefonia via Internet («Voice over IP», VoIP), al giorno d'oggi è relativamente semplice contraffare o mascherare i numeri. Esiste addirittura un mercato per i servizi che offrono la falsificazione del numero chiamante («Caller ID Spoofing»). Tramite i servizi Internet è inoltre possibile anche inviare SMS. Siccome a tale scopo non sono necessari né un cellulare né un corrispondente numero, alcuni fornitori di servizi consentono di scegliere a piacimento il nome visualizzato. Alcune iniziative internazionali cercano di impedire lo spoofing dei numeri chiamanti[140]. Attualmente, tuttavia, non esiste ancora una misura tecnica trasversale a tutti gli operatori che consenta di evitare

[139] Cfr. ad es. https://www.cybersecurityintelligence.com/blog/beware-spoofing-attacks-4890.html

[140] Ad es. STIR/SHAKEN, v. https://www.metaswitch.com/knowledge-center/reference/what-is-stir/shaken

questa pratica. L'introduzione di uno standard in tal senso potrebbe farsi attendere ancora a lungo. Nella maggior parte degli Stati (come anche in Svizzera) lo spoofing del numero di telefono non è penalmente vietato, ma è materia di diritto privato. Con la prevista revisione della legge sulla protezione dei dati dovrebbe tuttavia essere inserita nel Codice penale una norma che sanzioni il furto di identità e, pertanto, anche determinate forme di spoofing del numero di telefono.

Spoofing di siti web: i siti web possono essere copiati e ripubblicati a un altro indirizzo. Anche su pagine contraffatte è possibile ottenere un effetto di riconoscibilità mediante l'integrazione di loghi originali. Se non verificano il nome di dominio indicato nella riga dell'indirizzo e non si rendono conto che il certificato è falso o mancante, gli utenti possono essere tratti in inganno da questi siti. I truffatori registrano spesso dei domini contenenti piccoli refusi (*typosquatting*), che differiscono solo in maniera quasi impercettibile dall'indirizzo originale come ad esempio «svvisscom.ch» anziché «swisscom.ch». Il *typosquatting* può essere utilizzato anche per l'invio di e-mail e sfruttato quindi per phishing, frodi o diffusione di software nocivi.

Alcuni criminali impiegano con successo anche una combinazione dei metodi di spoofing: il gruppo Retefe sfrutta chiamate con numeri di telefono contraffatti per convincere con un pretesto le proprie vittime ad aprire un file PDF inviato loro via e-mail prima, durante o dopo la conversazione telefonica (cfr. n. 4.7.4). Se la vittima clicca sul link contenuto al suo interno, il computer viene infettato con il trojan bancario Retefe. Per proteggere le imprese svizzere e la popolazione, il NCSC mette a disposizione dei provider Internet informazioni su come bloccare i tentativi di accesso da parte dei loro clienti a siti tramite i quali viene diffuso Retefe. Per mascherare i link malevoli, spesso vengono utilizzati metodi di accorciamento dei link, i cosiddetti «*shortener services*» come bit.ly o goo.gl.

Nota / raccomandazione

In linea di massima, l'indirizzo del mittente di qualsiasi messaggio può essere contraffatto.

In particolare quando si ricevono messaggi nuovi o inusuali è sempre opportuna una buona dose di scetticismo. Anziché cliccare sui link ricevuti, dovreste se possibile effettuare il login all'account utente nel modo consueto. Prima di inserire dati personali, password o informazioni sulle carte di credito verificate di trovarvi effettivamente sul sito desiderato.

Non cliccate sui link contenuti nei messaggi sospetti, nemmeno per curiosità, poiché rischiereste di infettare il vostro dispositivo con software nocivi o di finire su siti sospetti. In caso di dubbi contattate l'apparente mittente tramite un canale di contatto già noto o indicato sul rispettivo sito web chiedendo informazioni e se l'e-mail proviene effettivamente da lui.

4.7.3 Smishing

Il termine «smishing» deriva dall'unione delle parole «SMS» e «phishing» e in generale indica l'abuso di SMS (ma sempre più spesso anche di applicazioni di messaggistica istantanea come WhatsApp) come vettore di attacco per il furto di informazioni sensibili come dati di accesso, password, numeri di carte di credito e informazioni sui conti correnti. Spesso a tale scopo vengono falsificati il numero e il nome del mittente (cfr. n 4.7.2 sullo spoofing). Lo smishing viene impiegato dai criminali anche per abusare dei servizi di pagamento in mobilità, carpire il codice *mTAN* e aggirare l'autenticazione a due fattori, ad esempio con un *SMS Stealer*. In Svizzera e all'estero è stata osservata anche la combinazione di tecniche di ingegneria

sociale. Le vittime sono state invitate tramite un breve messaggio a inviare un codice di autenticazione appena ricevuto via SMS affermando che quest'ultimo fosse stato inviato per errore o simulando un'emergenza. Teoricamente, questo metodo consente di compromettere tutti i servizi protetti dall'autenticazione a due fattori qualora l'autore dell'attacco sia precedentemente venuto a conoscenza di nome utente, password e numero di telefono della vittima. Nel caso di WhatsApp, in base alle impostazioni standard basta un codice di autenticazione di questo tipo per poter acquisire l'intero account utente di una persona.[141]

Nel primo semestre del 2020 a finire nel mirino dei truffatori sono stati in particolare i fornitori di servizi di pagamento tramite cellulare. Questi servizi consentono di pagare le fatture addebitandole sul conto del cellulare. A tale scopo il fornitore invia un codice via SMS al telefono, che deve poi essere inserito sul sito come conferma. In questo caso, alle vittime veniva fatto credere che ci fosse un pacco che non poteva essere consegnato. Per finalizzare il recapito era necessario inserire il numero di telefono e successivamente scaricare un'app. Quest'ultima era un *SMS Stealer*. I truffatori effettuavano a quel punto pagamenti con il numero di cellulare della vittima e l'app inoltrava loro direttamente il codice di conferma.

Sempre più spesso si osserva anche la diffusione tramite SMS di software nocivi come Emotet o EventBot, con l'obiettivo di rubare i dati di accesso alle applicazioni finanziarie e di e-banking.[142] Nell'ambito dello smishing vengono utilizzati in generale anche mittenti contraffatti e, come già ricordato, tecniche di ingegneria sociale allo scopo di indurre un determinato comportamento nelle persone prese di mira. A tale scopo, gli autori degli attacchi si servono anche di grandi eventi di attualità e delle loro conseguenze, come nel caso della pandemia di COVID-19: nel marzo 2020, le autorità sudcoreane hanno ad esempio messo in guardia da casi di smishing in relazione a informazioni sulla diffusione della COVID-19. Fino a metà febbraio erano stati inviati quasi 10 000 messaggi apparentemente provenienti da aziende che promettevano di mettere a disposizione mascherine di protezione gratis.[143]

Gli attacchi smishing costituiscono una minaccia crescente sia per la popolazione che per le imprese. Negli Stati Uniti nel primo trimestre del 2020 è stato registrato un aumento del phishing sui dispositivi mobili pari al 37 per cento nel solo segmento delle imprese.[144] In Svizzera i casi pubblicamente noti sono ancora piuttosto limitati: fino a luglio 2020 sono stati segnalati al NCSC 16 episodi di smishing in totale, quasi la metà dei quali registrati nel mese di giugno. Per il prossimo semestre l'NCSC prevede tuttavia una crescita di questo fenomeno.

Tramite SMS e servizi di messaggistica circolano anche truffe: messaggi con mittente contraffatto di note aziende svizzere come Coop, Migros o La Posta inducono il destinatario a stipulare servizi a valore aggiunto a pagamento, per esempio con il pretesto di un concorso o di un buono (cfr. n. 3.1.3).

---

141 Cfr. anche https://www.20min.ch/story/mit-diesem-code-bist-du-dein-whatsapp-8203-8203-konto-los-252382069481 e https://www.mimikama.at/allgemein/vorsicht-wenn-ein-whatsapp-kontakt-einen-verifizierungscode-verlangt/

142 Riguardo EventBot: https://www.zdnet.de/88379272/cybereason-warnt-vor-neuem-mobilen-banking-trojaner/; riguardo Emotet: https://threatpost.com/sms-attack-spreads-emotet-bank-credentials/153015/

143 https://www.zdnet.com/article/south-korea-sees-rise-in-smishing-with-coronavirus-misinformation/;

144 https://blog.lookout.com/global-mobile-phishing-encounters-surged-by-37-percent-amid-wfh-shift

Nota / raccomandazione

In linea di massima, l'indirizzo del mittente di qualsiasi messaggio può essere contraffatto.

Per quanto riguarda l'infrastruttura e-mail sono stati sviluppati negli anni metodi di filtrazione molto efficienti, in particolare per lo smistamento dei messaggi di spam. Questa tecnologia non può tuttavia essere applicata direttamente agli SMS. Nel caso dei servizi di messaggistica come WhatsApp o Threema non potrà essere introdotto un meccanismo corrispondente, visto che i messaggi vengono trasferiti in maniera cifrata dal mittente al destinatario e nessun intermediario può verificare il contenuto.

Non cliccate sui link contenuti nei messaggi sospetti, nemmeno per curiosità, poiché rischiereste di infettare il vostro dispositivo con software nocivi o di finire su siti sospetti. In caso di dubbi contattate l'apparente mittente tramite un canale di contatto già noto o indicato sul rispettivo sito web chiedendo informazioni e se il messaggio proviene effettivamente da lui.

Prima di inserire dati personali, password o informazioni sulle carte di credito verificate di trovarvi effettivamente sul sito desiderato.

4.7.4 Malware al telefono

Fig. 8: Procedura di infezione con il trojan Retefe. Lo scenario impiegato per la telefonata può variare.

Il fatto che i truffatori si diano molto da fare per installare malware sui dispositivi delle loro vittime è dimostrato da casi segnalati al NCSC 64 volte in diverse varianti nel primo semestre del 2020. Tutte le varianti erano accomunate dalla circostanza che oltre a ricevere un'e-mail la vittima è stata anche contattata per telefono. In alcuni casi i truffatori partivano con una telefonata in cui si annunciava un'e-mail contenente un documento in PDF, in altri la vittima veniva contattata in seguito per accertarsi che facesse effettivamente caso all'e-mail, aprisse

il documento allegato e cliccasse sul link contenuto al suo interno. Quest'ultima azione avviava a quel punto l'installazione di un software nocivo.

Fra i nomi usati spesso dalla ditta che effettuava la chiamata spacciandosi per un servizio di consegne, c'erano CH-Express, Delivery Experts o Delivery Schweiz. A finire sotto tiro sono state soprattutto le aziende piuttosto piccole come studi di architettura, ditte di giardinaggio o falegnamerie. Generalmente, il recapito riguardava richieste di offerte. In molti casi i responsabili si sono spacciati per una scuola universitaria, utilizzando per la spedizione delle e-mail un nome di dominio tanto simile a quello autentico da non notare la differenza (*typosquatting*). In una fase successiva, i tentati attacchi si sono ad ogni modo rivolti anche contro persone private.

Anche la pandemia in corso è stata sfruttata per convincere le vittime a installare il malware, per esempio dicendo loro che a causa del pericolo di infezione la ricezione di un pacco non poteva essere confermata tramite firma e che sarebbe quindi stato inviato un codice di conferma via e-mail che il destinatario avrebbe dovuto comunicare al corriere. Anche in questo caso al telefono veniva fatto credere che il codice fosse contenuto nel file PDF allegato all'e-mail, su cui bastava cliccare (cfr. n. 4.7.2).

Indicazioni dettagliate in merito sono riportate sul sito cybercrimepolice.ch.[145]

Conclusione / raccomandazione

È sorprendente che gli autori degli attacchi si prendano la briga di chiamare ogni singola vittima. A quanto pare, per i criminali non è più così facile portare il malware sui dispositivi, e quindi devono darsi maggiormente da fare. Altrettanto sorprendente è il fatto che il link malevolo non sia contenuto direttamente nell'e-mail, ma si trovi nel PDF allegato. L'effettiva efficacia di questa tattica non è certa. Questo approccio potrebbe per contro essere piuttosto controproducente, visto che rende l'attacco più complicato e dà alla vittima tempo per riflettere sulla plausibilità della storia. Solo poche persone, tuttavia, sono diventate scettiche dopo l'apertura del file PDF e hanno interrotto la procedura. Per questo motivo occorre fare più che mai attenzione quando si aprono link e allegati e, soprattutto, non farsi spingere a svolgere in fretta una determinata azione.

4.7.5 Estorsioni ai danni dei gestori di siti

Nel periodo in esame numerosi gestori di siti web hanno ricevuto e-mail ricattatorie fraudolente in cui i criminali affermavano di aver colpito il sito grazie a una vulnerabilità e di aver rubato l'intera banca dati alla sua base.[146] Minacciavano quindi di informare i clienti, di pubblicare o vendere i dati rubati e di danneggiare in questo modo la reputazione della vittima, a meno che questa non pagasse un riscatto in bitcoin. In Svizzera sono state osservate e-mail redatte in inglese e in tedesco. In un caso il mittente ha detto che il supposto attacco era stato commissionato da un'impresa concorrente con l'intenzione di sabotare il destinatario dell'e-mail. Tuttavia, il committente avrebbe cercato di mercanteggiare il prezzo concordato in precedenza, irritando i cibercriminali e facendo sì che questi contattassero l'apparente vittima con l'offerta

145 https://www.cybercrimepolice.ch/de/fall/online-betrueger-aufforderung-packetsendung-freischalten-nicht-nur-per-mail-sondern-neu-auch-per-telefon/

146 https://www.watchlist-internet.at/news/website-betreiberinnen-aufgepasst-erpressungsmails-im-umlauf/

di restituire i dati trafugati, naturalmente a fronte di un lauto indennizzo. In questa variante vengono citati come ulteriore strumento di pressione i problemi legali che la vittima dovrebbe affrontare in caso di violazione del RGPD (cfr. anche n. 4.5 sulle fughe di dati).

Nel quadro di questa truffa, i cibercriminali sfruttano la paura dei gestori dei siti rispetto alle conseguenze di un'eventuale fuga di dati nella speranza di convincerli in questo modo a pagare il riscatto. I siti web, tuttavia, non sono realmente compromessi, perlomeno nei casi di cui il NCSC è a conoscenza. Queste e-mail ricordano fortemente le ondate di *fake sextortion*, trattate più volte nei rapporti semestrali precedenti. In quel caso i truffatori sostengono di aver violato la webcam della vittima e di averla sorpresa durante il consumo di pornografia.[147] Anche negli episodi in questione i computer non sono in realtà stati attaccati e i cibercriminali non possiedono alcun materiale con cui danneggiare la persona ricattata. I malintenzionati sfruttano però i metodi dell'ingegneria sociale per convincere comunque le vittime a pagare un determinato importo in bitcoin.

Raccomandazione

Quando ricevete una lettera ricattatoria, mantenete la calma. Non fatevi mettere fretta. Molto spesso i ricatti sono privi di fondamento e vengono inviati a un gran numero di persone nella speranza che alcuni dei destinatari si lascino intimorire e paghino in maniera avventata. I tentativi di estorsione sono per principio penalmente perseguibili e possono essere denunciati alla polizia.

4.8 Misure preventive e perseguimento penale

4.8.1 Denuncia contro un host «bulletproof» tedesco

Per *«bulletproof hosting»* si intendono i centri dati progettati per sottrarsi all'accesso delle autorità (in particolare degli organi di perseguimento penale). Da un lato vengono spesso scelte sedi in Paesi in cui la giustizia non è ancora molto efficace, dall'altro (o in aggiunta) la sede viene mascherata mediante i più diversi dati falsi e prestanome per quanto riguarda il collegamento tecnico e amministrativo a Internet. Il *bulletproof hosting* è funzionale a forme di criminalità molto differenti tra loro.

Lo scorso autunno, dopo quattro anni di indagini penali, le autorità tedesche sono riuscite ad accedere a uno di questi host, che per anni aveva operato da un ex bunker della NATO mettendo la sua piattaforma a disposizione di vari cibercriminali. Sui suoi server erano ospitati fra l'altro il portale per il traffico di droga Wall Street Market, il market sulla darknet Flugsvamp, tramite il quale era gestito il 90 per cento del commercio di droga online svedese, così come

[147] Cfr. rapporti semestrali MELANI, n. 4.4.2, e 2019/2, n. 4.4.3; Sito web MELANI: https://www.melani.admin.ch/melani/it/home/meldeformular/formular0/meldeformularhaeufigefragen/FakeSextortion.html

la botnet Mirai. Nell'autunno dello scorso anno, oltre 700 agenti hanno perquisito l'area del bunker a Traben-Trarbach, disattivando più di 800 server. Ora la procura generale sta procedendo contro otto persone per complicità in numerosi reati fra cui ricettazione di dati, attacchi tramite botnet e traffico di droga. Sono stati inoltre trovati collegamenti con pedopornografia e mandati di omicidio. La complessa procedura comprende supporti dati con una capacità complessiva pari a due petabyte e ha portato gli investigatori ai limiti delle proprie risorse.

Secondo il diritto tedesco, la complicità prevede sempre anche la presenza di un reato principale. Ciò significa che gli investigatori devono per prima cosa accertare i reati commessi tramite i siti web ospitati nel ciberbunker. Accedere al sistema interno di posta elettronica del bunker attraverso il quale avveniva la comunicazione tra host e clienti è stato una versa sfida. Questa comunicazione è decisiva per dimostrare che i gestori accusati non hanno agito unicamente come fornitori di servizi tecnici senza alcuna responsabilità, bensì hanno volontariamente partecipato ai reati, rendendosi quindi colpevoli di complicità.[148]

4.8.2 Cibercriminali arrestati dalle autorità svizzere di perseguimento penale

Nell'aprile 2020 le autorità di perseguimento penale svizzere e polacche hanno eliminato – con il supporto dell'Europol – il gruppo di hacker InfinityBlack. Quest'ultimo comprendeva cibercriminali coinvolti nella divulgazione di dati utente rubati, nell'elaborazione e nella diffusione di malware e strumenti per hacker, così come in truffe.

La polizia ha sequestrato dispositivi elettronici, hard disk esterni e portafogli hardware con criptovalute per un valore di circa 100 000 euro. Due piattaforme con banche dati contenenti oltre 170 milioni di voci sono state anch'esse sequestrate e chiuse dalla polizia.

Il modello commerciale di questo gruppo di hacker consisteva nella creazione di piattaforme online per la vendita di dati di accesso degli utenti (cosiddette «combo»). Il gruppo presentava un'efficiente organizzazione in tre team definiti. Gli sviluppatori creavano gli strumenti per testare la qualità delle banche dati rubate, mentre i tester analizzavano l'idoneità dei dati di autorizzazione. I responsabili di progetto, infine, vendevano i dati ricevendo pagamenti in criptovaluta. In questo modo, gli hacker hanno avuto accesso a un gran numero di account cliente svizzeri. Nonostante le perdite stimate ammontino a soli 50 000 euro, gli hacker avevano accesso a conti dai quali avrebbero potuto trafugare oltre 610 000 euro. La fonte principale di guadagno per il gruppo di hacker consisteva nel rubare i dati di accesso al programma fedeltà di un'azienda svizzera della grande distribuzione per poi rivenderli ad altri gruppi criminali con una minore abilità tecnica, che successivamente convertivano i punti fedeltà in costosi dispositivi elettronici. Truffatori e hacker, fra i quali minorenni e giovani adulti, sono stati scoperti quando hanno tentato di utilizzare i punti rubati per ottenere merci in negozi svizzeri. Dopo l'arresto dei responsabili, la polizia ha scoperto collegamenti con un gruppo di hacker in Polonia. La trasmissione dei dati dei computer perquisiti alle autorità polacche ha infine condotto a ulteriori arresti di membri di InfinityBlack in Polonia[149].

---

148 https://www.heise.de/newsticker/meldung/Cyberbunker-Staatsanwaltschaft-erhebt-Anklage-gegen-Betreiber-4698785.html

149 https://www.europol.europa.eu/newsroom/news/hacker-group-selling-databases-millions-of-user-credentials-busted-in-poland-and-switzerland ; https://www.blick.ch/news/cyberkriminalitaet-treuepunkte-hacker-nach-polizeioperation-in-waadt-in-polen-gefasst-id15877097.html; https://www.watson.ch/!158091108

5 Ricerca e sviluppo

5.1 SCION: Internet sicuro ad alte prestazioni

Ilona Wettstein, Adrian Perrig, ETH di Zurigo, Network Security Group

La progressiva digitalizzazione di tutti i settori della vita e dell'economia richiede un Internet sicuro. Ogni giorno, miliardi di persone fanno affidamento sul fatto di poter inviare dati senza che questi vengano persi, deviati o analizzati durante il percorso. Al tempo stesso, la sicurezza non deve comportare perdite a livello di prestazioni; ciò significa che i meccanismi di protezione non devono ridurre la capacità della rete o rallentare il recapito dei dati.

Internet si basa sul *Border Gateway Protocol (BGP)*, praticamente invariato da 30 anni, che instrada i pacchetti dati attraverso la rete. A ogni nodo della rete, decide quale rotta deve prendere il pacchetto dati. In seguito alla forte espansione di Internet, oggi questo protocollo presenta numerose vulnerabilità e appare dunque evidente come le fondamenta di Internet si stiano per così dire sbriciolando. Il traffico dati viene deviato da hacker di Stato o attori criminali, che possono spiarlo o interromperlo.

SCION è un'architettura Internet innovativa[150] e sta per «**S**calability, **C**ontrol, and **I**solation **O**n **N**ext-Generation Networks». Sviluppata al Politecnico federale di Zurigo questa architettura sostituisce il *BGP* tramite un protocollo più sicuro ed efficiente, risolve numerosi altri problemi di sicurezza come i certificati di sicurezza contraffatti o gli attacchi *DDoS*. Contrariamente all'Internet attuale, in cui tutte le decisioni di routing avvengono a cura dei nodi di rete, SCION offre agli utenti trasparenza e controlli sulle rotte. I percorsi precisi attraverso Internet vengono assegnati ai pacchetti dati già al momento dell'invio e questi ultimi non possono pertanto essere dirottati. Con questo approccio, mediante una scelta intelligente delle rotte è inoltre possibile ottimizzare il tempo di trasmissione dei pacchetti dati. Usando diversi percorsi, SCION è per giunta in grado di passare a un nuovo percorso in pochi millisecondi in caso di problemi di comunicazione.

150 https://www.scion-architecture.net/

L'architettura sviluppata è già impiegata dalle scuole universitarie federali e da numerose banche. Un collegamento SCION offre una serie di vantaggi decisivi:

- comunicazione garantita e sovranità in Internet: la comunicazione non può essere interrotta tramite attacchi dall'estero o condotti da singoli attori (nessun *«kill switch»*);
- possibilità di una limitazione organizzativa o geografica del traffico dati. In questo modo si impedisce che informazioni confidenziali attraversino reti non affidabili;
- uso contemporaneo di diversi collegamenti ai fini di ottimizzare la comunicazione e aumentare l'affidabilità, anche in caso di interruzione dei collegamenti («business continuity»);
- maggiore capacità attraverso l'uso di diversi percorsi di rete.

L'Internet di prossima generazione promette dunque non solo una maggiore sicurezza, ma anche performance migliori rispetto allo stato attuale. Diversi fornitori di servizi Internet riuniti in un consorzio fungono da integratori e offerenti di collegamenti in Svizzera e all'estero. Attualmente l'architettura SCION è commercializzata e implementata da Anapaya Systems, uno spin-off del Politecnico federale di Zurigo.[151]

6 Previsioni e tendenze

6.1 Lavorare ovunque, non necessariamente in ufficio

Come già indicato nel tema principale (n. 3.5), la pandemia di COVID-19 ha prodotto cambiamenti soprattutto per gli impiegati d'ufficio. Molti di loro hanno potuto o dovuto lavorare da casa. In questo modo, molte imprese e lavoratori hanno raccolto esperienze con il telelavoro e altri modelli di occupazione che consentono di lavorare non più solo in ufficio, ma anche da qualsiasi altro luogo a scelta. Ciò porterà a una maggiore accettazione generale – se non addirittura a una richiesta – del lavoro indipendente dal luogo. Non possiamo ancora prevedere quando l'attuale pandemia finirà e sarà possibile tornare alla normalità. A tale proposito occorre considerare che il ritorno alle condizioni di lavoro pre-pandemia potrebbe non essere né possibile né auspicabile. Mentre alcune imprese hanno allestito già da diverso tempo un'infrastruttura stabile e sicura per lavorare a prescindere dal luogo, altre dispongono per ora solo di soluzioni attuate in tempi stretti e quindi piuttosto improvvisate. Vale la pena far fruttare fin d'ora delle esperienze raccolte e verificare le soluzioni impiegate per migliorarle o avviare un progetto per la completa riorganizzazione per poter considerare adeguatamente fin dall'inizio («security by design») non solo le necessarie capacità dell'infrastruttura, ma anche la sicurezza di dispositivi, reti e dati.

Le infrastrutture di accesso remoto offrono un vettore di attacco per la compromissione delle reti aziendali. Tanto i collegamenti tramite *VPN* quanto quelli via *RDP* devono essere configurati in modo sicuro e adeguatamente protetti. Già da qualche tempo gli attori scandagliano Internet alla ricerca di soluzioni di accesso remoto implementate con qualche vulnerabilità. Dopo la crescita nell'uso delle soluzioni di accesso remoto dovuto alla pandemia, le corrispondenti attività di scansione sono significativamente aumentate (cfr. n. 3.5). Prima o poi ogni

[151] https://www.anapaya.net/

sistema vulnerabile verrà individuato e attaccato. Tramite l'accesso remoto può fra l'altro essere introdotto sulla rete aziendale un ransomware (cfr. n. 4.1.1 sul ransomware e n. 4.4 sulle vulnerabilità).

Le piattaforme di collaborazione tramite cloud e i software per videoconferenze sono strumenti importanti per il lavoro indipendente dal luogo. Nel loro utilizzo devono essere selezionate configurazioni adeguatamente sicure e il personale deve essere formato per una gestione affidabile di questi strumenti.

Il lavoro tramite dispositivi privati («*bring your own device*», BYOD) non sottoposti alla manutenzione del servizio IT dell'impresa riduce il controllo di quest'ultima sulla sicurezza dei propri dati e attribuisce maggiori obblighi ai lavoratori. Affinché questi ultimi possano adempiervi adeguatamente, devono conoscere e comprendere le disposizioni dell'impresa, nonché essere sensibilizzati a intervalli regolari su minacce e pericoli.

Raccomandazione

Considerati i molteplici rischi che il lavoro mobile comporta, è necessario elaborare una strategia chiara e un piano di implementazione completo. Oltre alle misure tecniche di sicurezza, devono essere considerati anche aspetti legati all'utenza, visto che con il proprio comportamento gli utenti possono contribuire in modo determinante alla riduzione dei rischi.

DOCU

Prendete ispirazione dalle liste di controllo MELANI per il telelavoro:

Per le imprese: https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/fernzugriff.html

Per gli utenti: https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/fernzugriff-enduser.html

6.2 La geopoliticizzazione di Internet

Chi si occupa degli inizi di Internet si ritrova ben presto in un mondo di ricercatori abili sotto il profilo puramente tecnico, organi di standardizzazione altamente burocratizzati e primi utenti con una certa affinità per i temi dell'IT. Tutti loro avevano molte cose in mente, ma di certo non concetti come politica di sicurezza internazionale, geopolitica e politica di potere, ONU e diplomazia. Organizzazioni come l'Advanced Research Projects Agency (ARPA), l'Unione internazionale delle telecomunicazioni (UIT), la Internet Assigned Numbers Authority (IANA), la Internet Corporation for Assigned Names and Numbers (ICANN) e l'Organizzazione europea per la ricerca nucleare (CERN) con sede a Ginevra sono stati o sono ancora oggi i fondatori determinanti o i tutori dell'attuale Internet. Un'infrastruttura globale che la maggior parte delle persone nel 2020 dà per scontata e che, come suggeriscono i nomi delle organizzazioni coinvolte, fu considerata innanzitutto un semplice sviluppo tecnico in materia di comunicazione e tecnologia, che sarebbe stato gestito al meglio da esperti tecnici non politici.

Ormai Internet rappresenta l'elemento centrale di quasi qualsiasi sviluppo economico e sociopolitico, in particolare naturalmente della digitalizzazione. Consente per esempio il controllo a distanza di centrali elettriche, il molto discusso Internet delle cose («Internet of Things», IoT),

l'industrializzazione 4.0 e – specialmente in tempi di coronavirus – il mantenimento della produttività mediante il telelavoro a domicilio. Quella che inizialmente era pensata come una tecnologia ridondante che consentiva di condividere facilmente le informazioni e di continuare a funzionare anche in caso di guasto a un sistema parziale, si è trasformata nella spina dorsale globale dei processi critici in tutti i settori. Questa considerazione non si è certo affermata solo nel 2020, ma ha raggiunto il livello della politica di sicurezza internazionale già molto prima. Tuttavia, la crisi della COVID-19 ci ha ricordato in maniera evidente che a causa della forte interconnessione e della digitalizzazione le infrastrutture critiche (come ad es. gli ospedali) possono finire nel mirino di ciberattacchi.

La risoluzione ONU «Developments in the field of information and telecommunications in the context of international security» presentata dalla Russia nel 1998 ha portato sulla scena internazionale tale progressiva interconnessione e digitalizzazione. Da allora gli Stati membri dell'ONU sono chiamati a confrontarsi regolarmente su come impedire il possibile abuso e lo sfruttamento delle tecnologie dell'informazione e della comunicazione a livello internazionale. Di conseguenza, nel 2004 l'ONU ha attivato un «Group of Government Experts» (GGE) composto da 15 Stati membri. Quest'ultimo ha concentrato la propria attenzione fra l'altro sulla questione se nel campo delle tecnologie dell'informazione e della comunicazione l'attenzione debba concentrarsi anche sui contenuti o solo sull'infrastruttura che consente lo scambio di questi ultimi. Vista questa controversa situazione di partenza, non sorprende che al termine del proprio mandato nel 2005 il primo GGE non abbia prodotto alcun rapporto di consenso.

Le discussioni su cosa debba comprendere di preciso la definizione di «tecnologie dell'informazione e della comunicazione», su cosa sia concretamente un'infrastruttura critica e su come sia applicabile il diritto internazionale nel ciberspazio si dipanano come un filo conduttore attraverso il dibattito dei successivi GGE. Nel 2015 è stato possibile elaborare norme di validità generale – anche se non legalmente vincolanti per gli Stati membri dell'ONU – inerenti al «buon comportamento» nella gestione delle tecnologie dell'informazione e delle comunicazioni. Ciò comprendeva per esempio il fatto che non debbano essere effettuati ciberattacchi a infrastrutture critiche. Allo stesso modo, è stata confermata l'applicabilità del diritto internazionale nel ciberspazio. Simili sforzi e discussioni sono condotti anche a livello regionale, ad esempio in seno all'OSCE.

Quello che era iniziato come progetto puramente tecnico per allestire reti IT ridondanti e resistenti, è oggi nella sua forma globale caduto in balia di interessi nazionali – in parte contrapposti – nel campo della politica di sicurezza. Nell'attuale rigido clima internazionale, anche i progressi a tale riguardo a livello sovranazionale sono rari. Dopo il rapporto del GGE nel 2015 non è praticamente più stato possibile ottenere risultati concreti. Il GGE del 2017 si è chiuso senza un consenso. Il nuovo GGE è stato avviato nel 2019. Parallelamente, nel 2019 ha cominciato la sua attività di consulenza anche l'Open Ended Working Group (OEWG) diretto dalla Svizzera. Nondimeno – o proprio per non interrompere i diversi processi e dialoghi – questo impegno a livello diplomatico è nell'interesse di tutti. La Svizzera ha riconosciuto già da qualche tempo la necessità di affrontare il tema del ciberspazio anche nel contesto internazionale e della politica di sicurezza. Essendo una piccola economia aperta con una solida rete internazionale, la Svizzera ha bisogno di prevedibilità e ordine nel contesto internazionale della politica di sicurezza. Per questo motivo la Svizzera è stata membro dei GGE del 2017 e del 2019, così come dell'OEWG, e svolge un ruolo attivo nell'elaborazione di norme e misure mirate a rafforzare la fiducia nel quadro dell'OSCE. Questa è anche di un'opportunità, visto che la Svizzera è ben posizionata in campo internazionale per condurre dibattiti su digitalizzazione, ciberspazio e relativa governance; la Ginevra internazionale è praticamente predesti-

nata a tale scopo. Ciò comprende contributi molto concreti, come il «Geneva Dialogue on Responsible Behavior in Cyberspace» avviato dalla Svizzera nel 2018, che nel 2020 viene proficuamente portato avanti con numerosi rappresentanti del mondo economico internazionale. In oltre dieci incontri virtuali è stato possibile sviluppare buone pratiche nel campo della cibersicurezza che rispecchiano un nuovo consenso suddiviso a livello mondiale fra aziende IT attive su scala globale e settori affini in questo ambito. In questo modo la Svizzera fornisce un importante contributo a rendere più precise le norme internazionali e i principi del ciberspazio, per esempio le norme dei GGE o i principi del «Paris Call for Trust and Security in Cyberspace».[152] Allo stesso tempo, così facendo si sottolinea ancora una volta il ruolo di Ginevra quale centro della politica digitale e tecnologica mondiale.

7 Prodotti MELANI pubblicati

7.1 GovCERT.ch Blog (in inglese)

7.1.1 Analysis of an Unusual HawkEye Sample

20.02.2020 - Currently, we are observing HawkEye samples being distributed by large malspam waves. HawkEye is a keylogger which has been around quite a long time (since 2013) and has evolved since then and gained more functionality. There are several good blog posts about HawkEye in general. Recently we observed an interesting obfuscation method in a HawkEye binary, which we are going to describe in this blog post.

➔ https://www.govcert.admin.ch/blog/analysis-of-an-unusual-hawkeye-sample/

7.1.2 Phishing Attackers Targeting Webmasters

22.04.2020 - Since the beginning of April 2020, we are seeing an increase in phishing attacks against webmasters and domain owners in Switzerland. Unknown threat actors are phishing for credentials for accounts on web admin panels of at least three major hosting providers in Switzerland.

➔ https://www.govcert.admin.ch/blog/phishing-attackers-targeting-webmasters/

7.2 Bollettino d'informazione MELANI

7.2.1 Attenzione: i rischi di sicurezza per le PMI causati da ransomware continuano a essere elevati

19.02.2020 - Nelle ultime settimane MELANI / GovCERT ha trattato oltre una dozzina di casi di ransomware in cui criminali sconosciuti hanno criptato e di conseguenza reso inutilizzabili i sistemi di PMI e grandi aziende svizzere. Gli aggressori hanno chiesto un riscatto di diverse decine di migliaia di franchi, in alcuni casi addirittura dell'ordine di milioni.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/sicherheitsrisiko-durch-ransomware.html

[152] https://pariscall.international/en/

7.2.2 Avvertimento: false e-mail inviate a nome dell'UFSP

14.03.2020 - Da venerdì pomeriggio (13 marzo 2020) cibercriminali cercano di sfruttare l'incertezza della popolazione provocata dagli sviluppi legati al coronavirus. Utilizzando false e mail, nelle quali l'USFP figura come mittente, tentano di diffondere programmi dannosi. La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI mette in guardia la popolazione. Queste e-mail devono essere cancellate immediatamente.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/gefaelschte-emails-im-namen-des-bag.html

7.2.3 Vulnerabilità critica in Microsoft Windows Server (SIGRed)

15.07.2020 - Martedì scorso (14 luglio 2020) Microsoft ha rilasciato un aggiornamento di sicurezza per una vulnerabilità critica nel Windows Domain Name System (winDNS). Microsoft valuta la vulnerabilità a 10.0 punti del CVSS (Common Vulnerability Scoring System), che corrispondono al valore massimo della scala.

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

7.2.4 Il trojan Emotet è di nuovo attivo

23.07.2020 - MELANI osserva nuovamente diverse ondate di e-mail con documenti word infetti in allegato. Si tratta di un trojan ormai noto da tempo, Emotet (anche detto Heodo). Originariamente conosciuto come trojan e-banking, oggi Emotet viene utilizzato soprattutto per l'invio di spam e per scaricare altri malware. Emotet prova – con e-mail fasulle a nome di collaboratori, soci d'affari o conoscenti – tramite ingegneria sociale cioè, a convincere il destinatario ad aprire un documento word e ad attivare le macro Office in esso contenute.

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

7.3 Liste di controllo e guide

7.3.1 Telelavoro: Assicurare l'accesso remoto

24.03.2020 - In considerazione dell'aumentato utilizzo di soluzioni di accesso remoto, desideriamo ricordarvi alcune best practice per ridurre al minimo il rischio associato a queste tecnologie. Riteniamo che i rischi stiano aumentando con il numero di accessi remoti in una rete di organizzazioni. Gli aggressori conoscono la situazione attuale e possono tentare di utilizzare diversi modi per ottenere l'accesso alla rete di un'organizzazione.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/fernzugriff.html

7.3.2 Telelavoro: Guida per l'utente finale

02.04.2020 - In aggiunta al documento "Telelavoro: proteggere l'accesso remoto" desideriamo fornire alcune informazioni all'utente finale su come proteggere al meglio il proprio ambiente e, di conseguenza, ridurre il rischio per il datore di lavoro.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/fernzugriff-enduser.html

8 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.
Advanced Persistent Threat (APT)	Questa modalità di attacco prevede l'uso di diverse tecniche e tattiche. Si tratta inoltre di attacchi estremamente mirati contro una singola organizzazione o un Paese. Il più delle volte essi possono provocare danni ingenti. Ecco perché l'aggressore è disposto a investirvi molto tempo, denaro e conoscenze e a tal fine dispone generalmente di notevoli risorse.
App	Il concetto di app (dall'abbreviazione inglese di «application») indica in generale ogni forma di programmi di applicazione. Nell'uso linguistico si fa nel frattempo perlopiù riferimento alle applicazioni per i moderni smartphone e computer tablet.
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.
Autenticazione a due fattori (2FA)	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 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.

Termine	Descrizione
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.
Cryptomining	Uso della potenza di calcolo di un computer per trovare e convalidare nuove unità di criptomoneta, p.e. Bitcoin.
DDoS	Attacco di Distributed-Denial-of-Service. Un attacco DoS in cui la vittima è attaccata simultaneamente da numerosi sistemi diversi.
Defacement	Deturpamento di pagine web.
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	Un programma, uno script o una linea di codice che può essere utilizzato per sfruttare le vulnerabilità dei sistemi informatici.
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 informatici.

Termine	Descrizione
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.
Infostealer	Malware in grado di raccogliere le sequenze di tasti, le schermate, l'attività di rete e altre informazioni
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 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.

Termine	Descrizione
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 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.

Termine	Descrizione
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.
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.

Termine	Descrizione
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.
Spyware	Lo spyware è destinato a raccogliere all'insaputa dell'utente informazioni sulle sue abitudini di navigazione oppure sulle configurazioni di sistema per trasmetterle a un indirizzo predefinito.
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.
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).

Termine	Descrizione
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.
VPN	Virtual Private Network Consente per il tramite della cifratura del traffico di dati una comunicazione sicura tra computer su una rete pubblica (ad es. Internet).
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.