Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

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

SICUREZZA DELLE INFORMAZIONI

LA SITUAZIONE IN SVIZZERA E A LIVELLO INTERNAZIONALE

Rapporto semestrale 2018/I (gennaio – giugno)

8 NOVEMBRE 2018

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

1 Indice

2 Editoriale

Dr. Bruce Nikkel
Head of Cybercrime Intelligence & Forensic Investigation, UBS
Chairman of the European FI-ISAC
Professor of Digital Forensics, Berner Fachhochschule

Care lettrici, cari lettori,

La Svizzera poggia storicamente su rapporti di fiducia tra singoli Cantoni, i quali collaborano al fine di proteggersi da minacce comuni. A partire da quest'esempio di fiducia tra diversi gruppi d'interesse è risultata la costante evoluzione di una società sicura. Nel nostro mondo digitale la fiducia gioca un ruolo centrale. Una collaborazione basata sulla fiducia tra gruppi che perseguono gli stessi obiettivi è ormai diventata essenziale in ogni settore industriale. I suddetti gruppi lavorano insieme per affrontare, impedire e combattere le minacce informatiche e le attività criminali in ambito cyber.

Esistono dei gruppi ad hoc i cui membri si incontrano informalmente per discutere di minacce tecniche attuali e di possibili soluzioni. Inoltre gli uffici governative e le imprese costituiscono dei gruppi più formali basati sulla fiducia, si tratta dei cosiddetti ISAC (Information Sharing and Analysis Centres) o CERT (Computer Emergency Response Teams). In Svizzera MELANI assicura la coordinazione di gruppi di gestori di infrastrutture d'importanza vitale all'interno di diversi settori come quello dell'energia, delle telecomunicazioni, della finanza e di altri settori critici per la società. Tali gruppi riuniscono i dipendenti di aziende concorrenti che in questo frangente cooperano per raggiungere un obiettivo generale più ampio, che in ultima analisi è al servizio della sicurezza della società.

Inoltre, poiché le minacce informatiche superano i confini nazionali, la cooperazione deve essere estesa anche a persone e comunità al di fuori della Svizzera. Esistono numerose iniziative internazionali basate sulla fiducia per analizzare le minacce alla società su base globale. MELANI prende parte a queste iniziative internazionali insieme a molte altre organizzazioni svizzere. Normalmente simili gruppi comprendono membri del settore industriale, i CERT governativi (come MELANI), le forze dell'ordine e altri specialisti della sicurezza.

La sicurezza della nostra società digitale si basa su simili gruppi fidati, sia informali che formali. Noi dobbiamo sostenere lo sviluppo di gruppi del genere. Le minacce e il crimine informatici non possono essere fermati da una sola organizzazione ma necessitano di una collaborazione tra imprese e organizzazioni concorrenti e tra il settore privato e pubblico. La fiducia tra le persone è la chiave per il successo. Essa può essere raggiunta soltanto tramite la continua evoluzione e la costante cura dei rapporti tra imprese e organizzazioni sia nazionali che internazionali. Il contributo di MELANI per lo sviluppo di simili gruppi aggiunge preziosa sicurezza nel nostro mondo cyber.

Dr. Bruce Nikkel

3 Tema principale: vulnerabilità dell'hardware

3.1 Spectre e Meltdown

Nel settore delle TIC i problemi legati alla vulnerabilità sono ormai all'ordine del giorno. Ogni settimana vengono rese note delle falle di sicurezza, che però non presentano tutte lo stesso grado di criticità e molte hanno degli effetti minimi o molto specifici. A finire in prima pagina sono principalmente le vulnerabilità che possono essere sfruttate dall'esterno e dunque da chiunque sia attivo su Internet («Remote Code Execution»). In questi casi il rischio di danno è davvero molto elevato. È quanto accaduto ad esempio con il bug di sicurezza Heartbleed o con il ransomware Wannacry, che sfruttavano una lacuna nel Protocollo SMB. Fortunatamente gli aggiornamenti dei software sono generalmente disponibili in tempi brevi dopo la pubblicazione delle vulnerabilità. Le aziende produttrici di software si sono infatti organizzate di conseguenza, ottimizzando i processi per l'eliminazione delle vulnerabilità. Ma che cosa succede se anziché un software, una falla riguarda l'hardware? È già successo ad esempio nel 1994 con Pentium-FDIV-Bug[1] e nel 2014 con Rowhammer[2], che permette di alterare il contenuto di specifiche chip di memoria RAM attraverso la lettura ripetuta di una specifica riga di memoria fino a modificare lo stato elettrico di una riga adiacente. Tuttavia, l'impatto delle vulnerabilità hardware Spectre e Meltdown, rese pubbliche nella prima settimana di gennaio del 2018, è stato molto più grave. Un errore di progettazione nei processori consente ai criminali informatici di leggere i dati salvati sullo stesso. E questo tipo di errori non può essere eliminato semplicemente aggiornando il software.[3]

3.2 Perché questi errori di progettazione?

Per velocizzare le applicazioni, i produttori di processori hanno sviluppato le seguenti idee: i processori effettuano delle supposizioni sulle operazioni aritmetiche che saranno necessarie in seguito, le eseguono e memorizzano i risultati («speculative execution» e out of «order execution»). Se l'ipotesi non è corretta, i risultati sono scartati, al contrario, il risultato è disponibile più rapidamente. I computer memorizzano nella cosiddetta cache le istruzioni e i dati utilizzati di frequente. Questa memoria è implementata direttamente sul processore in modo da potervi accedere molto rapidamente. Un aggressore può ora dedurre l'indirizzo di memoria dei dati dal tempo di calcolo richiesto per l'accesso ai dati. Un valore che si trova già nella cache ed è stato calcolato in precedenza, viene letto più velocemente che se dovesse essere ricalcolato. Per accedere ad informazioni protette, an aggressore approfitta del fatto che delle informazioni sulle quali non avrebbe alcun diritto, si trovano nella memoria. La verifica avviene soltanto quando vengono richiesti i relativi risultati. In assenza dei necessari diritti l'operazione viene interrotta con un messaggio di errore. Le informazioni rimangono però nella memoria per un breve momento e potranno essere lette fintanto che la memoria corrispondente non sarà soprascritta.

La procedura è in uso da 20 anni. Porta a prestazioni del computer più veloce e quindi al risparmio di tempo. Vent'anni fa, i computer erano per lo più sistemi chiusi. Nell'era del cloud computing e dei sistemi virtuali, la scoperta di queste vulnerabilità acquista una gravità

---

1 https://it.wikipedia.org/wiki/Pentium_FDIV_bug (stato: 31 luglio 2018)

2 https://en.wikipedia.org/wiki/Row_hammer (stato: 31 luglio 2018)

3 https://meltdownattack.com (stato: 31 luglio 2018)

maggiore in quanto avviene in un periodo in cui più utenti accedono a un processore. Perciò, nella ricerca di soluzioni, ci si è concentrati soprattutto sui fornitori di servizi cloud, per i quali vari sistemi virtuali condividono lo stesso hardware.

Ma la problematica riguarda anche la maggior parte dei computer, server, smartphone e tablet. In pratica, questa falla potrebbe riguardare tutti gli utenti di tali apparecchi. I sistemi infettati diventano disponibili per gli hacker a livello di processore e consentono così un accesso più ampio alle informazioni presenti nel sistema.

3.3 Approccio risolutivo

Generalmente se un apparecchio presenta lacune rilevanti sotto il profilo della sicurezza, il fabbricante lo ritira dal mercato. Nell'industria automobilistica accade regolarmente che vengano ritirati veicoli per la sostituzione di parti difettose. Nel mondo dei computer un simile approccio è difficilmente attuabile, poiché sostituire la componente hardware interessata, in questo caso il processore è una vera e propria sfida. Invero, nel caso dell'errore Pentium-FDIV, nel 1994, dietro pressione degli utilizzatori si arrivo ad effettuare una sostituzione della componente colpita. Oggigiorno però il numero degli apparecchi interessati e il conseguente onere logistico sarebbero troppo elevati. Inoltre, si correrebbe il rischio di avere implementazioni difettose, poiché i sistemi non sono normalizzati come invece avviene nell'industria automobilistica, ma vengono configurati in modo molto diversificato. I fabbricanti di processori hanno pertanto deciso di rimuovere l'errore hardware con un insieme di aggiornamenti per software e microcodice (codice per il controllo delle operazioni in un processore), anche se questo approccio può sembrare paradossale. L'aggiornamento riduce ad esempio la precisione della risoluzione temporale o disattiva le porzioni di memoria in cui i processori eseguono i calcoli in anticipo e la relativa accelerazione. In questo modo l'errore viene corretto a distanza con un notevole calo, fino al 30 per cento, delle prestazioni del processore. Il calo può comportare gravi ripercussioni sulla stabilità dei sistemi e deve a sua volta essere compensato da una maggiore potenza di calcolo. Un approccio di questo tipo non è perciò adatto per una soluzione a lungo termine.

Per il futuro è quindi necessario un cambiamento di paradigma nella progettazione dei microprocessori e l'architettura del processore dovrà essere completamente rivista. Per farlo ci vorranno probabilmente molti anni. Per aumentare la sicurezza si potrebbero ad esempio avvicinare le porzioni della memoria all'unità di calcolo. La memoria e la comunicazione sono funzionali al processore, che costituisce il nucleo degli attuali sistemi ed è l'elemento maggiormente ottimizzato.[4] In una nuova architettura la memoria, e dunque anche la sicurezza, dovrebbero essere integrate maggiormente e meglio nel sistema («Security by Design», SbD). Si pone la questione di quali metodi sono generalmente utilizzati per garantire una maggiore sicurezza nello sviluppo di elementi hardware.

[4] https://www.netzwoche.ch/storys/2018-03-07/wie-meltdown-und-spectre-zukuenftige-computerarchitekturen-beeinflussen (stato: 31 luglio 2018)

3.4 Possibili sviluppi

Le vulnerabilità Spectre e Meltdown hanno suscitato discussioni sulle falle nell'hardware. Sempre più ricercatori che si occupano di sicurezza in tutto il mondo lavorano a questa tematica per scovare altre falle. Spectre NG («Spectre Next Generation»), resa pubblica a maggio, comprende complessivamente otto nuove vulnerabilità basate sul metodo di Spectre e Meltdown.[5] Tra queste "Foreshadow" alias "L1 Terminal Fault" con cui un aggressore può leggere da una macchina virtuale la memoria, presumibilmente protetta, di un'altra macchina virtuale che gira sullo stesso computer. Nel luglio 2018 sono stati annunciati tre ulteriori falle CPU ret2spec, SpectreRSB e NetSpectre.

È facile supporre che saranno scoperte nuove vulnerabilità hardware, visto che la maggior parte dei sistemi informatici continua a basarsi su sviluppi che datano 20 anni e più. Per ragioni di compatibilità, i sistemi e le architetture non sono mai stati ristrutturati. Si è invece tentato di sviluppare ulteriormente quanto già c'era, sebbene il sistema e l'architettura in parte non siano stati pensati per queste nuove funzioni. Proprio in un settore dinamico come quello delle TIC, ciò è degno di nota e svolgerà un ruolo rilevante quando verranno rese pubbliche delle nuove falle. Contrariamente a quanto accade con i software, una sostituzione dell'hardware su scala mondiale è irrealistico. Sarà determinante stabilire in che modo è possibile ridurre al minimo il rischio di queste lacune e come sopportare i conseguenti peggioramenti di prestazione.

Raccomandazione

INFO

Misure riguardanti le vulnerabilità hardware sulla pagina web di MELANI
https://www.melani.admin.ch/melani/it/home/themen/hardwareluecken.html

4 La situazione a livello nazionale

4.1 Spionaggio

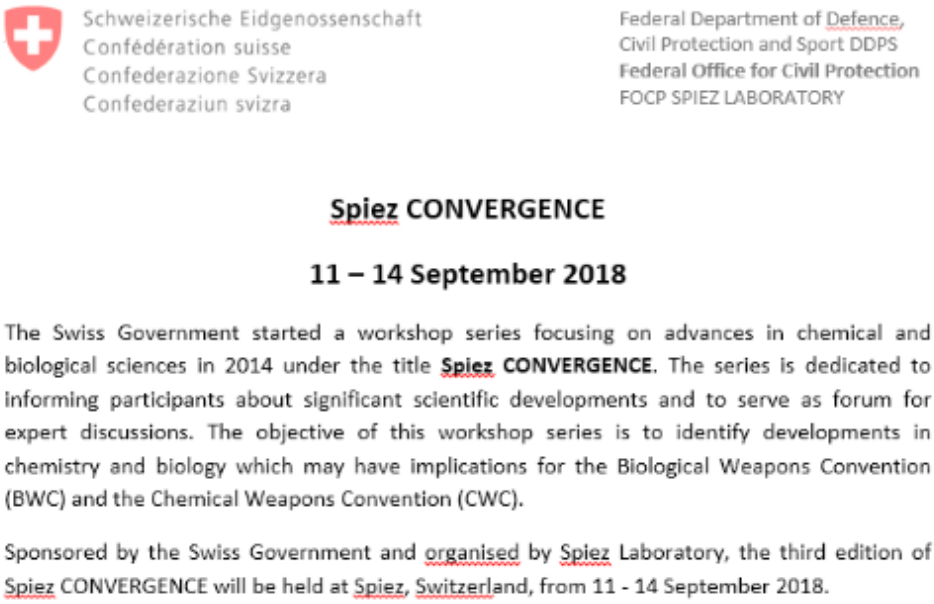
4.1.1 Il nome del Laboratorio Spiez utilizzato per inviare Olympic Destroyer

Il 19 giugno 2018 il fornitore di servizi di sicurezza Kaspersky Lab ha pubblicato un rapporto sull'impiego del malware Olympic Destroyer, comparso per la prima volta nel 2018 in Corea del Sud durante i Giochi olimpici invernali di Pyeongchang. Il worm di rete era servito per sabotare l'infrastruttura dell'organizzatore durante la cerimonia d'apertura. Diversi esperti in materia di sicurezza hanno pensato a un'operazione «false flag» e sospettato che gli aggressori volessero depistare le indagini facendo ricadere i sospetti su un terzo (in questo caso la Corea del Nord). Tale correlazione o attribuzione, a prima vista ovvia, a posteriori si è rivelata infatti errata e ha mostrato una volta di più che nel settore informatico attribuire

[5] https://www.heise.de/ct/artikel/Super-GAU-fuer-Intel-Weitere-Spectre-Luecken-im-Anflug-4039134.html (stato: 31 luglio 2018)

responsabilità non è semplice. Nel frattempo Kaspersky Lab ha collegato Olympic Destroyer al gruppo di hacker Sofacy (v. cap. 5.1.1).

Nel maggio e nel giugno del 2018 sono state scoperte e-mail di phishing mirate («spear phishing»). I documenti allegati all'e-mail sono stati collegati con elementi di Olympic Destroyer del febbraio 2018. Secondo Kaspersky Lab, gli obiettivi di questi attacchi erano organizzazioni finanziarie in Russia nonché laboratori di prevenzione delle minacce biochimiche. Se il destinatario apre l'e-mail, il malware tenta di infettare il computer per aggiungerlo a una rete botnet. L'infezione è complessa e si basa su varie tecnologie quali VBA, PowerShell e MS HTA con JavaScript. Kaspersky Lab ha pubblicato i dettagli tecnici sul proprio blog.[6] In questa occasione non sono state osservate azioni di sabotaggio. Per sferrare un attacco mirato e indurre i destinatari a cliccare sull'allegato, in un caso gli hacker hanno preso quale modello per la loro e-mail un invito, disponibile pubblicamente, del Laboratorio Spiez a una conferenza internazionale. L'e-mail è stata in seguito spedita con mittente falsificato a vari destinatari a nome dell'Ufficio federale della protezione della popolazione (UFPP) e del Laboratorio Spiez. Non sono mai stati coinvolti server dell'Amministrazione federale. Contrariamente a quanto comunicato da diversi media, il Laboratorio Spiez non è stato attaccato. Il nome del laboratorio è stato utilizzato in modo indebito unicamente per l'attacco, al fine di conferirgli maggiore credibilità.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS
Federal Office for Civil Protection
FOCP SPIEZ LABORATORY

Spiez CONVERGENCE

11 – 14 September 2018

The Swiss Government started a workshop series focusing on advances in chemical and biological sciences in 2014 under the title **Spiez CONVERGENCE**. The series is dedicated to informing participants about significant scientific developments and to serve as forum for expert discussions. The objective of this workshop series is to identify developments in chemistry and biology which may have implications for the Biological Weapons Convention (BWC) and the Chemical Weapons Convention (CWC).

Sponsored by the Swiss Government and organised by Spiez Laboratory, the third edition of Spiez CONVERGENCE will be held at Spiez, Switzerland, from 11 - 14 September 2018.

Figura 1: L'e-mail inviata ai destinatari a nome dell'UFPP (fonte: Kaspersky Lab)

Il 12 e il 14 marzo 2018, utilizzando un metodo analogo, sono state inviate a organizzazioni governative europee e-mail di spear phishing contenenti un presunto invito a una conferenza internazionale. All'e-mail era allegato un documento Word («Defence & Security 2018 Conference Agenda.docx»). Anche in questo caso gli hacker hanno copiato l'agenda dalla pagina web e l'hanno inviata a potenziali partecipanti alla conferenza. Il documento conteneva

6 https://securelist.com/olympic-destroyer-is-still-alive/86169/ (stato: 31 luglio 2018)

un oggetto flash con un linguaggio ActionScript che tentava di scaricare il vero malware («payload»). La particolarità di questo attacco è stata l'attivazione della componente dannosa soltanto dopo che la vittima aveva fatto scorrere sullo schermo la terza pagina del documento.[7] Questo metodo è stato probabilmente scelto per rendere più difficile l'individuazione dell'attacco. Gli specialisti di sicurezza di PaloAlto sospettano che sia opera del gruppo Sofacy.[8]

Valutazione

Gli inviti a conferenze sono molto utilizzati negli attacchi mirati. Da un lato, in genere queste informazioni sono pubbliche e dunque liberamente disponibili per l'hacker. In questo modo un attacco può essere particolarmente mirato, poiché all'invito si interesseranno soltanto le persone che lavorano in quell'ambito. Dall'altro, gli hacker non devono svolgere grandi lavori di ricerca. La storia è autentica e, di norma, non contiene generalmente errori di contenuto o linguistici.

4.2 Sistemi di controllo industriali

4.2.1 Sistemi aperti in rete: minaccia o «normale amministrazione»?

La crescente interconnessione e la penetrazione dell'informatica in pressoché tutti gli ambiti della vita offrono potenziali economici e sociali ai quali un Paese altamente sviluppato e industrializzato come la Svizzera non può rinunciare. Nel contempo, però, l'aumento della digitalizzazione comporta nuovi rischi.

I sistemi di controllo industriali («Industrial Control Systems», ICS), che finora funzionavano isolati, sono sempre più connessi ad Internet. Questa interconnessione comporta dei vantaggi. Tuttavia, non tutti questi apparecchi sono stati progettati a questo scopo e la maggior parte di essi dispone ancora di sistemi operativi obsoleti e non più supportati. Per garantire un funzionamento sicuro è quindi necessario adottare diverse misure di sicurezza.

Alcuni sistemi poggiano su funzioni centrali e importanti che tuttavia presentano vulnerabilità per ragioni storiche o perché non sono state progettate per l'impiego di sistemi critici. Individuare ed eliminare eventuali lacune diventa quindi sempre più importante. Gli approcci collaborativi aiutano a scoprire i malfunzionamenti sulla base di algoritmi euristici. Una soluzione di questo tipo è stata presentata nel febbraio del 2018 dall'Ufficio federale dell'armamento (armasuisse): al momento molti servizi si basano sul sistema GPS. Droni, elicotteri e perfino aerei si orientano con l'aiuto dei segnali GPS. L'emissione di segnali finalizzati a interferire con i sistemi GPS o ad ingannarli, può far deviare i droni dalla loro rotta. Per impedirlo, il sistema innovativo Crowd-GPS-Sec[9] sorveglia costantemente lo spazio aereo servendosi dei segnali di navigazione provenienti da velivoli e droni. Utilizzando un nuovo tipo di algoritmi, i ricercatori hanno dimostrato che il sistema è in grado di smascherare falsi segnali

[7] https://www.zdnet.com/article/hackers-are-using-a-flash-flaw-in-fake-document-in-this-new-spying-campaign/ (stato: 31 luglio 2018)

[8] https://researchcenter.paloaltonetworks.com/2018/03/unit42-sofacy-uses-dealerschoice-target-european-government-agency/ (stato: 31 luglio 2018)

[9] https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-69896.html (stato: 31 luglio 2018)

GPS in pochi secondi. Dopo qualche minuto, l'aggressore può essere localizzato con un margine di errore di pochi metri.

Anche gli oggetti della vita quotidiana sono sempre più connessi a una rete interna o ad Internet: webcam, «interruttori intelligenti», frigoriferi o smart tv dispongono sempre più spesso di un'interfaccia di rete. Ciò origina un aumento non soltanto degli utenti interconnessi su Internet, ma anche dei dispositivi vulnerabili agli attacchi degli hacker. Sono problematici, in particolare, gli apparecchi con connessione aperta e senza protezione, o le cui falle di sicurezza possono essere sfruttate direttamente via Internet. Il motore di ricerca Shodan indicizza questi sistemi e li mappa in base alla loro esposizione al rischio («exposure maps»). Secondo Shodan, in Svizzera 478 sistemi di controllo industriali sono visibili dall'esterno e la lacuna di sicurezza che si può sfruttare più spesso, sempre dall'esterno, rimane Heartbleed.[10] Il motore di ricerca mostra anche che 405 dispositivi con il software Cisco Smart Install Client (strumento per installare nuovi switch di Cisco) sarebbero accessibili pubblicamente (v. anche cap. 5.1.6).

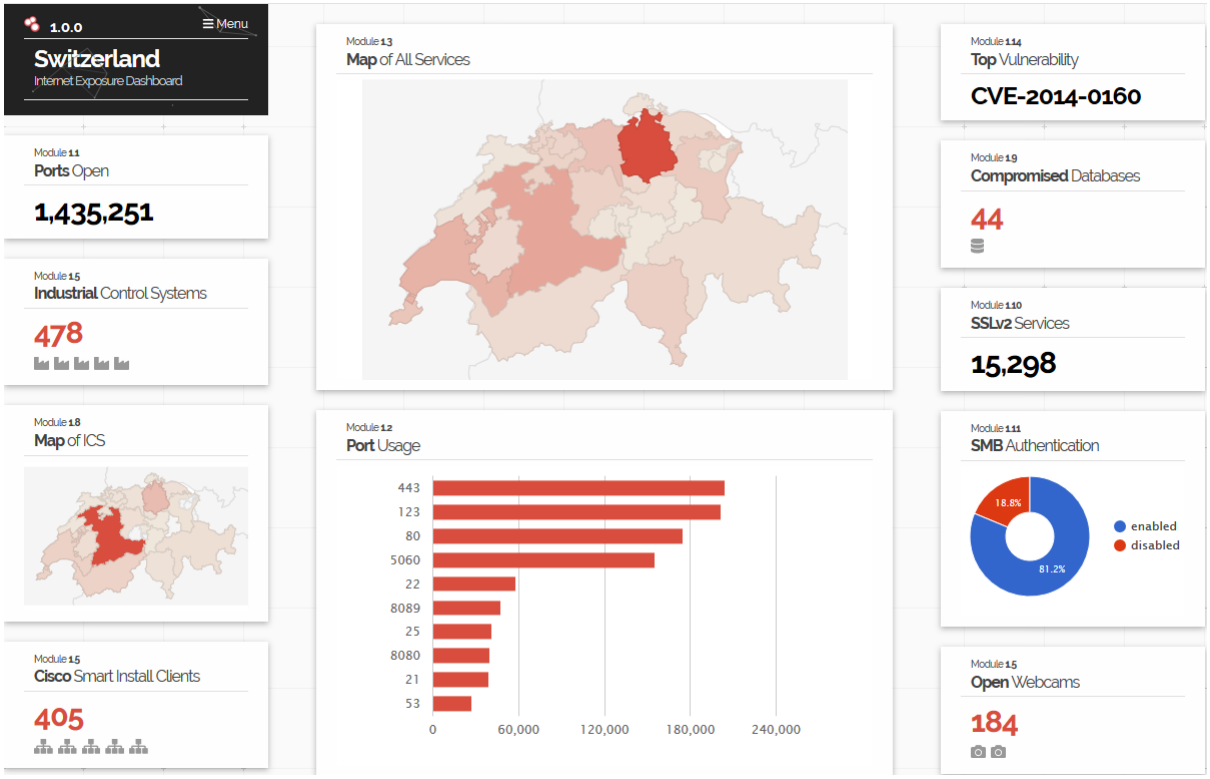


Figura 2: Panoramica sui sistemi vulnerabili e accessibili tramite Internet in Svizzera (fonte: https://www.shodan.io/. Giorno di riferimento: 31 agosto 2018)

Gli hacker hanno a disposizione strumenti sempre migliori per sfruttare simili lacune anche senza avere grandi conoscenze tecniche. All'inizio del 2018 ha suscitato scalpore in tal senso Autosploit, un nuovo tool che collega il motore di ricerca Shodan con il framework Metasploit. Quest'ultimo è uno strumento per lo sviluppo e l'esecuzione di exploit contro un computer

[10] Giorno di riferimento: 31 agosto 2018

preso di mira da un attacco. Combinando questi due servizi è possibile sfruttare automaticamente le falle di sicurezza, senza avere conoscenze specifiche. Il programma inizia con una ricerca in Shodan di un servizio speciale, ad esempio di un server Apache o dell'Internet Information Service di Microsoft. Un ulteriore comando lancia in seguito gli attacchi. Lo script serve a selezionare automaticamente gli exploit giusti dalla biblioteca Metasploit.

Finora, oltre all'energia criminale, gli hacker dovevano avere anche conoscenze appropriate. Con i tools appena descritti questo requisito è ormai superfluo e la cerchia dei potenziali autori si estende notevolmente.

A volte non è semplice valutare il livello di criticità dei sistemi aperti e nemmeno se e in che misura sono toccati i sistemi sensibili[11]. Due anni fa, al Chaos Communication Congress (CCC), alcuni hacker hanno pubblicato molte schermate di sistemi in cui sarebbero penetrati. Tra di essi c'era anche il servizio idrico di un piccolo Comune svizzero. Dopo un'analisi più accurata e una richiesta di informazioni allo stesso Comune è tuttavia emerso che, sebbene l'accesso non fosse pubblico, i cittadini interessati erano autorizzati a vedere questi dati. Sui grafici si vedeva quanta acqua affluisce dalle singole fonti nel bacino di raccolta. Tra i dati pubblicati non vi erano informazioni sensibili e non erano possibili manipolazioni a distanza.

[11] https://www.suedostschweiz.ch/zeitung/wasserwerk-wurde-gehackt (stato: 31 luglio 2018)

Valutazione / Raccomandazione

In linea di massima, gli oggetti e gli apparecchi connessi via Internet possono essere rilevati da chiunque (ad es. con un «port scan» o un motore di ricerca come Shodan) e offrono perciò maggiormente il fianco agli attacchi. I dispositivi connessi a Internet devono essere protetti (con l'aiuto di password individuali o di un accesso limitato) e aggiornati regolarmente. È importante effettuare sempre gli aggiornamenti appena sono disponibili. Tutti sanno che un computer fisso o uno smartphone devono essere aggiornati, mentre quasi nessuno pensa a questa necessità nel caso di un interruttore intelligente o di un frigorifero.

Nell'ambito della «Strategia nazionale per la protezione della Svizzera contro i cyber-rischi» (SNPC), varata dal Consiglio federale nel 2012, l'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) ha analizzato la vulnerabilità ai cyber-rischi in diversi settori d'importanza vitale. Sono stati esaminati l'approvvigionamento di elettricità, acqua potabile e derrate alimentari, ma anche i trasporti su gomma e ferrovia. In base ai risultati l'UFAE ha elaborato uno «standard minimo per rafforzare la resilienza informatica». Esso è pensato in particolare per i gestori di infrastrutture critiche in Svizzera, ma può essere applicato da qualsiasi azienda.

Lo standard minimo per rafforzare la resilienza informatica comprende diverse funzioni (identificare, proteggere, intercettare, reagire e ripristinare) e offre agli utenti 106 istruzioni concrete per migliorare la resilienza informatica ai cyber-rischi:

Lo standard minimo per rafforzare la resilienza informatica

https://www.bwl.admin.ch/bwl/it/home/themen/ikt/ikt_minimalstandard.html

Raccomandazione

Se scoprite sistemi di gestione in Internet accessibili dall'esterno o protetti in modo inadeguato, trasmetteteci i dati necessari per darci modo di informare il gestore.

Formulario d'annuncio MELANI

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

Misure di protezione dei sistemi industriali di controllo:

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

4.3 Attacchi (DDoS, Defacement, Drive-By)

In Svizzera i cittadini, le organizzazioni e le imprese continuano a essere il bersaglio di diversi tipi di attacchi.

4.3.1 Attività di Apophis Squad in Svizzera

Il gruppo Apophis Squad è noto per aver rivendicato falsi allarme bomba in alcune scuole americane e inglesi nei mesi di marzo e aprile del 2018.

In giugno 2018 il gruppo ha fatto parlare di sé a causa di un altro tipo di attività, rivendicando attraverso il proprio account Twitter diversi attacchi di tipo DDoS promuovendo così il suo servizio di booter (o stresser), tramite il quale è possibile rendere inutilizzabile un sito. Generalmente gli attacchi hanno una durata molto breve, ma nel caso di ProtonMail un provider svizzero di posta elettronica crittografata, si sono susseguiti sull'arco di più giorni e hanno generato dei periodi di inaccessibilità al servizio. L'accanimento contro il servizio ProtonMail è probabilmente dovuto al tweet di un responsabile dell'impresa che avrebbe definito «pagliacci» i responsabili degli attacchi, provocandoli. Le differenti attività hanno avuto seguito legale dando luogo a un arresto alla fine del mese di agosto del 2018.

Queste attività e l'eco mediatica che ne è derivata sembrano aver incoraggiato alcuni opportunisti ad utilizzare il nome del gruppo Apophis Squad per sferrare attacchi DDoS a scopo di ricatto. In agosto, infatti, numerose imprese attive nel settore finanziario hanno dovuto affrontare un tentativo di estorsione da parte del gruppo Apophis Squad. Le imprese hanno ricevuto un'e-mail in cui si menzionavano esplicitamente gli attacchi precedenti del gruppo e si chiedeva il versamento del curioso importo di 2,01 bitcoin, entro una determinata scadenza. In caso di mancato pagamento il gruppo avrebbe sferrato un attacco DDoS di grande entità. Alla prima e-mail ne sono seguite altre di richiamo. Sulla base di diversi elementi, MELANI ha rapidamente pensato che dietro queste e-mail si nascondesse qualcuno che agiva sfruttando la reputazione del gruppo Apophis Squad senza però avere realmente intenzione o addirittura la capacità di sferrare un attacco. I criminali in questione, infatti, utilizzavano frequentemente gli stessi indirizzi bitcoin, rendendo impossibile tracciare l'origine di un eventuale pagamento. Inoltre, Apophis Squad aveva comunicato su Twitter che alcuni imitatori («copycat») agivano a loro nome utilizzando però un modus operandi differente.

Allo scadere dell'ultimatum non è stata segnalata nessuna attività, confermando così l'ipotesi di MELANI. Tuttavia, considerato l'alto numero di gruppi in grado di sferrare attacchi DDoS, le imprese devono essere ben preparate ad affrontarli.

Raccomandazione

Sul sito Internet di MELANI è pubblicata una lista di misure da adottare per far fronte a questo tipo di attacco

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

4.4 Social engineering e phishing

Il presupposto di un buon attacco è un racconto credibile che induca la potenziale vittima a compiere una determinata azione. I cosiddetti attacchi di «social engineering» funzionano meglio se l'utente malintenzionato riesce a raccogliere molte informazioni sulla vittima designata. I truffatori utilizzano sia fonti accessibili a chiunque, sia informazioni provenienti da furti di dati. I dati rubati vengono esaminati, collegati ad altri dati rubati o di pubblico dominio, preparati e rivenduti ad altri criminali.

4.4.1 Phishing

Anche nel primo semestre del 2018 sono state inviate numerose e-mail di phishing. Il contenuto delle e-mail non cambia molto: alcune chiedono i dati della carta di credito per poterli «verificare», altre invitano a cliccare su un link per collegarsi a un certo sito dove inserire la password al fine di usufruire di servizi Internet. In questi messaggi di phishing si abusa regolarmente dei loghi di aziende conosciute o del servizio interessato per conferire una parvenza di ufficialità alle e-mail.

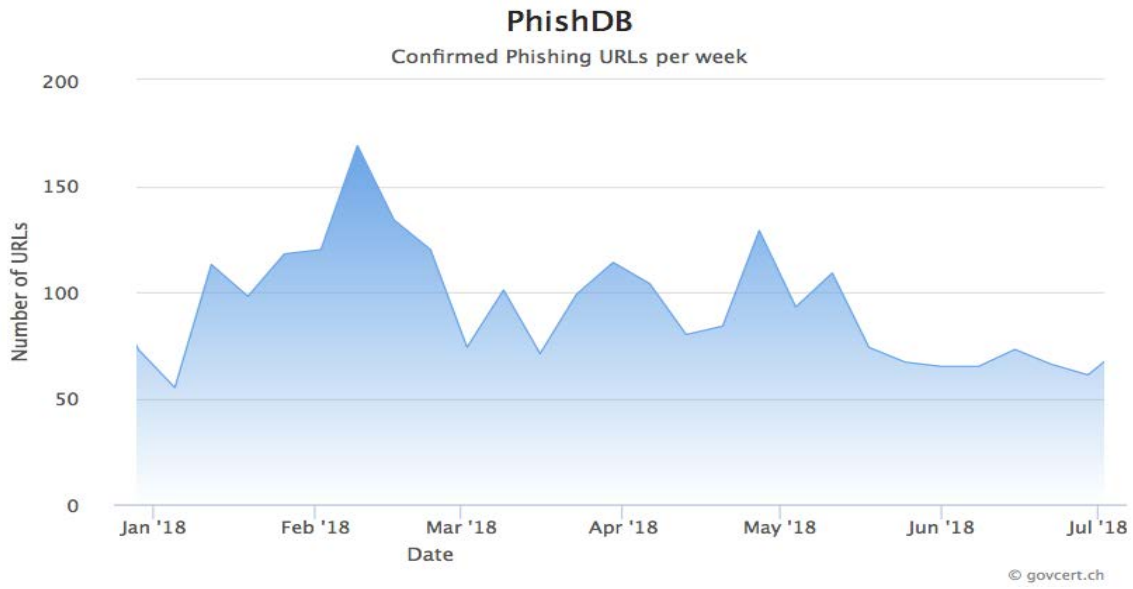


Figura 3: I siti di phishing segnalati e confermati ogni settimana su antiphishing.ch nel primo semestre del 2018

Nel primo semestre del 2018, sul portale antiphishing.ch, gestito da MELANI, sono stati segnalati complessivamente 2501 diversi casi inequivocabili di pagine web di phishing. La figura 3 mostra il numero di siti di phishing segnalati ogni settimana, che varia nel corso dell'anno. I motivi delle oscillazioni sono disparati: alcune sono dovute a periodi di ferie, in cui vi sono meno segnalazioni, mentre altre sono dovute al fatto che i criminali spostano periodicamente la loro attenzione da un Paese all'altro.

4.4.2 Telefonate a nome di banche

È stata constatata una recrudescenza di telefonate fraudolente alle imprese in cui i criminali si spacciano per collaboratori di una banca. I truffatori incitano la ditta a effettuare un pagamento oppure sostengono di dovere svolgere un update dell'e-banking seguito da un test del servizio.

Abitualmente i criminali tentano di convincere i collaboratori della ditta ad installare un programma per l'accesso remoto (ad es. NTR-Cloud o TeamViewer), quindi si collegano con il dispositivo della vittima e fingono di installare un aggiornamento del sistema di e-banking. Infine, i truffatori affermano che l'installazione dell'aggiornamento dev'essere verificata simulando un pagamento e inducono la vittima a inserire nel sistema i dati di accesso al servizio e-banking della ditta. Se i versamenti sono protetti dalla firma collettiva, i criminali tentano di persuadere la vittima ad organizzare la presenza di tutti i collaboratori aventi diritto di firma in modo da poter attivare il pagamento.

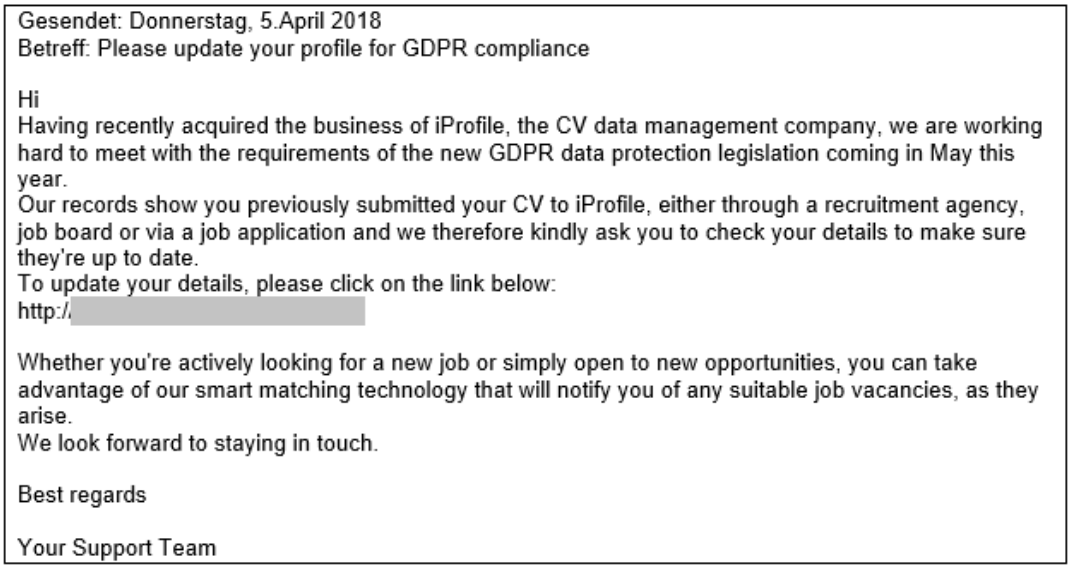
In un'altra variante, alla vittima viene raccomandato di non utilizzare il servizio di e-banking per alcuni giorni, a causa di un necessario aggiornamento della piattaforma. I truffatori si premurano poi di comunicare un numero al quale rivolgersi nel caso in cui si debba effettuare una transazione urgente. Se la vittima si mette in contatto con il finto collaboratore della banca per registrare un pagamento, le verranno richiesti il nome utente, la password personale e la one-time password (OTP). In questo modo i criminali ottengono l'accesso alla piattaforma e-banking. Il procedimento può essere ripetuto varie volte, finché la vittima non fiuta l'inganno.

Valutazione

Gli esempi mostrano come i metodi di social engineering siano tuttora attuali. La sensibilizzazione all'interno delle singole ditte, l'osservanza dei processi TIC nonché la verifica delle informazioni rivelate online concernenti i collaboratori, la direzione e il consiglio d'amministrazione sono l'elemento chiave per prevenire efficacemente simili tentativi di truffa.

4.4.3 Phishing RGPD

Dopo un periodo transitorio di due anni, il 25 maggio 2018 è entrato in vigore il Regolamento generale dell'Unione europea sulla protezione dei dati (RGPD UE / EU GDPR) (v. cap. 7.3). Come previsto, il termine del periodo transitorio per l'introduzione del RGPD è stato sfruttato a scopi di phishing per perpetrare degli abusi: nel periodo precedente il 25 maggio 2018 moltissime imprese hanno spedito ai loro clienti e-mail contenenti informazioni sui provvedimenti in vista dell'attuazione del RGPD. Truffatori scaltri hanno saputo sfruttare questo lasso di tempo, contando sul fatto che i destinatari fossero informati sull'introduzione del RGPD e si sentissero obbligati ad adeguare i loro profili di conseguenza (v. es. figura 4).



Gesendet: Donnerstag, 5.April 2018
Betreff: Please update your profile for GDPR compliance

Hi
Having recently acquired the business of iProfile, the CV data management company, we are working hard to meet with the requirements of the new GDPR data protection legislation coming in May this year.
Our records show you previously submitted your CV to iProfile, either through a recruitment agency, job board or via a job application and we therefore kindly ask you to check your details to make sure they're up to date.
To update your details, please click on the link below:
http:/

Whether you're actively looking for a new job or simply open to new opportunities, you can take advantage of our smart matching technology that will notify you of any suitable job vacancies, as they arise.
We look forward to staying in touch.

Best regards

Your Support Team

Figura 4: Esempio di e-mail fraudolenta che prende a pretesto il RGPD per ottenere i dati di una vittima

La corretta applicazione del regolamento e l'imposizione di pesanti sanzioni pecuniarie in caso di violazione della protezione dei dati non soltanto continuerà a preoccupare le imprese, ma indurrà pure i criminali a ideare nuovi metodi estorsivi. Analogamente a quanto avviene nel settore del «social engineering» le informazioni di dominio pubblico vengono sistematicamente utilizzate per creare nuove opportunità.

4.4.4 Tentativi di truffa sfruttando il calendario

Tutti i tentativi di truffa iniziano con la ricerca di una via per contattare la potenziale vittima adducendo motivazioni diverse. Generalmente, il metodo privilegiato è l'invio di e-mail, ma i criminali non esitano a diversificare la loro strategia: l'invio di SMS, di messaggi WhatsApp o l'aggancio tramite i social media è sempre più diffuso. Un altro modus operandi in circolazione nel periodo in esame consiste nell'invio di inviti destinati al calendario della vittima. In base alle impostazioni del programma PIM (ad es. Outlook), l'invito verrà visualizzato anche se non è ancora stato accettato e sull'e-mail verranno inviati dei promemoria. Nella fattispecie, la vittima vedeva l'invito nel suo calendario Google. Si trattava di un'offerta di prestito per la quale la vittima era invitata a mettersi in contatto via e-mail o WhatsApp alle coordinate indicate nel messaggio. Non è stato possibile stabilire lo scopo dell'attacco, ma si è ipotizzato un tentativo di phishing o di truffa. In ogni caso, questo esempio dimostra che l'utente deve essere prudente su qualsiasi piattaforma. Perfino gli eventi nel suo calendario possono infatti celare un contenuto pericoloso. Non si può però escludere che alcuni internauti si lascino ingannare, reputando una registrazione o una notifica del calendario personale come legittima ed agendo di conseguenza in modo avventato. È tuttavia consigliabile impostare il calendario in modo che vengano mostrati solo gli eventi approvati.

4.4.5 Presunte vincite – catene di sant'Antonio a nome di IKEA, Milka e Co

Cioccolata per un anno intero, un buono di IKEA o un nuovo iPhone. A intervalli regolari circolano messaggi Whatsapp, SMS ed e-mail che promettono questo genere di vincite, anche se per finire invece della cioccolata c'è solo frustrazione. Dietro e-mail di questo genere si celano dei raccoglitori di dati. In tutti questi giochi a premi le domande sono scelte in modo tale che chiunque possa rispondervi facilmente. Al fine di ottenere la maggior quantità possibile

di dati, gli autori vogliono infatti che il maggior numero possibile di concorrenti «vinca». Per ottenere la vincita, si devono inserire su un sito web falsificato dati personali quali nome, età, indirizzo di posta elettronica o numero di cellulare e talvolta anche l'indirizzo di domicilio. Questo tipo di truffa prevede anche l'impiego di domini internazionali (v. cap. 4.4.7). Così, in una variante di un gioco a premi del marchio Milka, nel dominio di «Milka» è stata utilizzata una «i» senza punto, come la si trova in turco. In un primo momento gli utenti non se ne accorgono e pensano di trovarsi sulla pagina ufficiale del marchio di cioccolata.

Un'altra astuzia in questi giochi a premi è l'inoltro del messaggio a un determinato numero di contatti come requisito fondamentale all'ottenimento della vincita. La forma della catena di sant'Antonio consente al promotore di non doversi neppure curare dell'invio. È la vittima stessa a occuparsene. Il fatto che il messaggio giunga da una persona che il destinatario conosce è un ulteriore vantaggio di questo metodo, perché aumenta la possibilità che una vittima si fidi del gioco a premi e vi partecipi.

Raccomandazione

I messaggi contenenti promesse di vincite allettanti devono essere analizzati in modo critico e non vanno assolutamente inoltrati. La cosa migliore da fare, in sostanza, è ignorarli.

4.4.6 Da Internet al mondo reale – quando gli hacker si presentano di persona

I reati su Internet offrono il vantaggio di potere essere commessi a distanza. Il più delle volte gli autori si trovano all'estero, eludendo il rischio di essere arrestati dalle autorità di perseguimento penale locali. Poiché i truffatori possono commettere i reati a partire da un ambiente a loro familiare, cala anche la soglia d'inibizione. Per una rapina in banca occorre molta più energia criminale che per l'invio di e-mail di phishing. Nel periodo in rassegna ci sono stati tuttavia segnalati alcuni episodi che richiedevano la presenza fisica sul posto. In giugno 2018 sono stati pubblicati degli avvisi inerenti truffatori telefonici che si spacciavano per collaboratori di Google[12]. Apparentemente in alcuni casi si è tentato anche di organizzare un incontro sul luogo. In un caso è stato comunicato a delle ditte che «Google» auspicava un appuntamento di persona per verificare i dati da loro rilevati. Anche se una simile procedura potrebbe apparire sensata a primo acchito, una visita di persona dei collaboratori di Google sembra però un po' eccessiva. Non è stato possibile chiarire l'intenzione dei truffatori.

In un altro caso sono state effettuate telefonate a nome dell'Ufficio federale dell'energia (UFE). Gli autori delle chiamate hanno finto di volere controllare il consumo energetico in loco. Non è dato sapere se lo scopo fosse spiare la vittima, venderle qualcosa (un software ad esempio) o accedere al suo computer.

12 https://www.itmagazine.ch/Artikel/67409/Polizei_warnt_vor_Anrufen_von_falschen_Google-Mitarbeitern.html (stato: 31. luglio 2018).

Raccomandazione

All'interno di molte ditte in cui si lavora a contatto con la clientela, vengono utilizzati dispositivi informatici nelle stesse aree alle quali anche i clienti hanno accesso. Quando i collaboratori devono allontanarsi dal computer, per comodità spesso non lo bloccano. In questo lasso di tempo i potenziali aggressori hanno la possibilità di attivare programmi con chiavette USB o di aprire una pagina Web dannosa. Il computer dovrebbe sempre essere bloccato, anche in caso di assenza brevissima. Anche la protezione delle interfacce USB può aumentare la sicurezza, soprattutto se non vengono utilizzate. I sistemi operativi sono ormai impostati in modo da non eseguire più automaticamente i file presenti su queste chiavette. L'utente deve confermare di volere svolgere l'azione. Ciò nonostante vi sono sempre delle vulnerabilità che permettono di aggirare questo elemento di sicurezza.

4.4.7 Dominio «look alike»

Già nel 2005 MELANI mise in guardia dal seguente trucco di phishing: i truffatori creavano degli URL fasulli molto simili agli originali facendo ricorso a cosiddetti «nomi di dominio internazionalizzati» (IDN). Il dominio www.epic.com con caratteri cirillici è ad esempio quasi indistinguibile dalla pagina web www.epic.com del fabbricante di software Epic. Se in più si rilascia il relativo certificato di sicurezza, è anche possibile stabilire una connessione protetta da «https://». Grazie al lucchetto presente nella barra degli indirizzi del browser, la pagina Internet appare così «sicura» all'internauta e perciò degna di fiducia. Moltissimi caratteri internazionali sembrano praticamente identici a quelli nel nostro alfabeto e ciò favorisce gli abusi. Questo metodo è noto come «attacco omografico». Se negli ultimi anni questo tipo di aggressione sembrava scomparso, nel periodo in esame in Svizzera sono stati osservati nuovi casi.

L'alfabeto cirillico è quello che viene utilizzato più spesso negli attacchi omografici, poiché le lettere a, c, e, o, p, x ed y sembrano identiche alle lettere a, c, e, o, p, x ed y di quello latino. Possono essere utilizzate anche le lettere ԧ, i, j ed s. Nell'alfabeto greco soltanto «omicron» («o») e «Ni» («v») assomigliano a una lettera minuscola latina. Più raramente vengono utilizzati caratteri armeni ed ebraici.[13]

Nel 2005 il rimedio adottato dai singoli produttori di browser è stato di rappresentare i caratteri speciali nella barra degli indirizzi con il sistema punycode, in modo da rendere facilmente riconoscibile un dominio fasullo. Il nome di dominio paypal.com con una «a» cirillica diventa così xn-pypal-4ve.com. Nel browser Firefox è inoltre stata introdotta una «whitelist» con i domini verificati nei quali non è stata inserita nessuna sequenza punycode. Questa strategia è stata modificata nel 2012 in quanto, sulla scia della diffusione di domini IDN, la manutenzione e le dimensioni della whitelist erano diventate troppo importanti. Da allora gli IDN vengono rappresentati se tutti i caratteri appartengono allo stesso set di caratteri o se il dominio di primo livello («Top Level Domain», TLD) limita l'impiego degli IDN. Si opera in modo analogo anche in Internet nei browser Explorer e Opera. Anche Safari rappresenta i set di caratteri problematici con sequenze punycode.

A venir presi di mira sono in particolare i TLD transnazionali quali .com, .net o.biz. In questi casi gli hacker fanno in modo che tutte le lettere provengano da un solo set di caratteri, in

[13] https://it.wikipedia.org/wiki/Attacco_omografico (stato: 31 luglio 2018)

modo tale che il browser non inserisca la sequenza punycode. Ciò pone loro dei limiti, ma le lettere summenzionate permettono di ottenere delle combinazioni che si prestano ad attacchi omografici.

Nel caso dei TLD specifici per un Paese i set di caratteri vengono generalmente limitati, come nel TLD .ch[14], che autorizza solo 32 caratteri speciali. Eppure, anche in questo caso gli hacker possono prendere lettere simili. Una «î» con accento circonflesso è difficilmente distinguibile da una «i» normale e se il set di caratteri è limitato il browser non inserisce nessuna sequenza punycode.

Figura 5: I 32 caratteri speciali ammessi in Svizzera per i nomi di dominio (fonte:nic.ch).

Valutazione / Raccomandazione

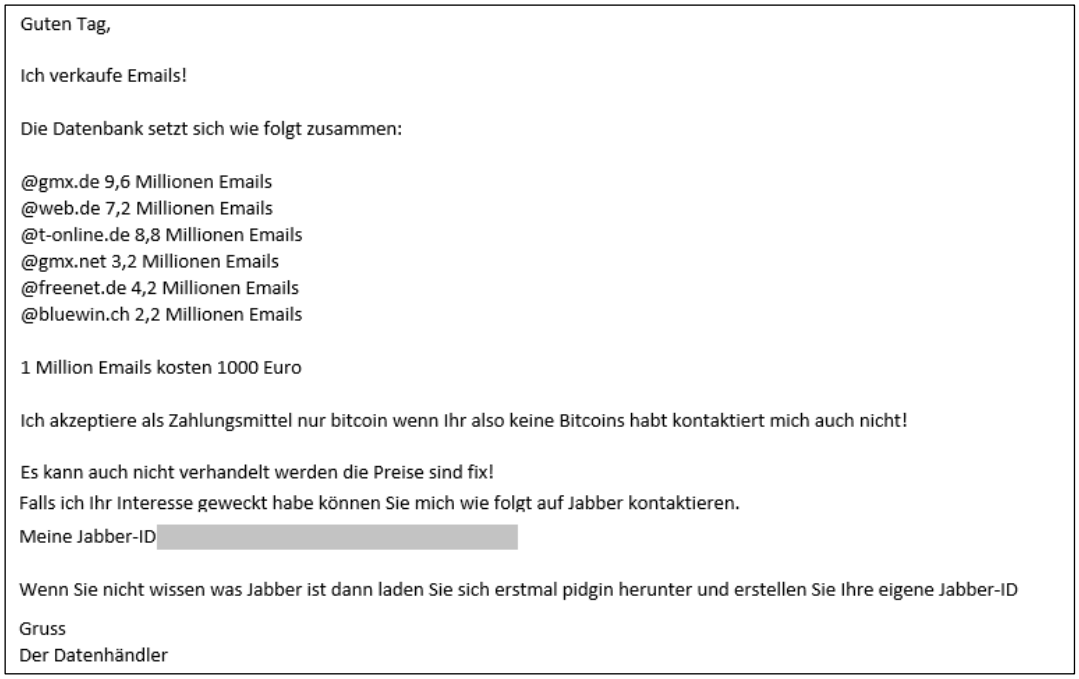
I provvedimenti adottati dai produttori di browser risolvono gran parte del problema. Per esperienza, gli hacker non si sforzano eccessivamente per generare pagine di phishing. Generalmente piratano siti Web esistenti per inserivi pagine fraudolente. Nessuno si preoccupa di avere un URL corretto. Il discorso cambia nel caso di attacchi mirati. Questo metodo potrebbe senz'altro rivelarsi idoneo per l'invio di un trojan di spionaggio a una vittima specifica.

In Firefox si possono disattivare completamente gli IDN. Così facendo, nella barra dell'indirizzo tutti gli URL sono visualizzati in sequenze punycode. Per disattivare gli IDN, si deve cambiare la variabile «network.IDN_show_punycode» da «false» a «true» nella pagina di configurazione (about:config).

4.4.8 Indirizzi e-mail in vendita

Già nel dicembre del 2017 una grande quantità di indirizzi e-mail è stata messa in vendita su Internet. Nel maggio del 2018 molti destinatari svizzeri hanno ricevuto un'offerta di acquisto di indirizzi di posta elettronica. Non è dato sapere se il mittente fosse effettivamente in possesso del numero di indirizzi indicato.

[14] https://www.nic.ch/it/faqs/idn/ (stato: 31 luglio 2018)



Guten Tag,

Ich verkaufe Emails!

Die Datenbank setzt sich wie folgt zusammen:

@gmx.de 9,6 Millionen Emails
@web.de 7,2 Millionen Emails
@t-online.de 8,8 Millionen Emails
@gmx.net 3,2 Millionen Emails
@freenet.de 4,2 Millionen Emails
@bluewin.ch 2,2 Millionen Emails

1 Million Emails kosten 1000 Euro

Ich akzeptiere als Zahlungsmittel nur bitcoin wenn Ihr also keine Bitcoins habt kontaktiert mich auch nicht!

Es kann auch nicht verhandelt werden die Preise sind fix!
Falls ich Ihr Interesse geweckt habe können Sie mich wie folgt auf Jabber kontaktieren.
Meine Jabber-ID

Wenn Sie nicht wissen was Jabber ist dann laden Sie sich erstmal pidgin herunter und erstellen Sie Ihre eigene Jabber-ID

Gruss
Der Datenhändler

Figura 6: Nel maggio del 2018 molti destinatari svizzeri hanno ricevuto un'offerta di acquisto di indirizzi di posta elettronica.

La compilazione di liste di indirizzi di posta elettronica al fine di rivenderle è un modello operativo lucrativo per i cyber criminali. I truffatori utilizzano sia dati rubati che informazioni liberamente disponibili. Gli spammer passano al setaccio automaticamente Internet a caccia di indirizzi e-mail validi pubblicati su pagine web (ad es. in forum o albi degli ospiti). Anche gli account e-mail compromessi sono una buona fonte di indirizzi. Sia dalle rubriche, sia dalle e-mail possono infatti venir sottratti degli indirizzi. Un ulteriore metodo consiste nel tentare con nomi e cognomi comuni. Quando un'e-mail è inviata a questi indirizzi creati a caso, la maggior parte dei server di posta elettronica segnala che l'indirizzo non esiste, quindi in tutti gli altri casi il mittente può supporre che l'indirizzo esista. Questi tentativi sono completamente automatizzati.

Nei mercati illegali in rete le raccolte con indirizzi e-mail validi abbondano. Di norma, anche la vendita di questi dati si svolge all'interno di questi mercati. Queste «offerte di vendita» sono raramente inviate in gran numero indistintamente agli utenti Internet «ordinari». Non è chiaro che cosa spinga gli hacker a effettuare gli invii in massa. Probabilmente è un tentativo per indurre i destinatari a pagare in anticipo degli indirizzi e-mail di cui i criminali non sono realmente in possesso. O forse essi vogliono verificare l'attualità di una banca dati spam esistente e vedere quali indirizzi e-mail vengono rifiutati dai server di posta elettronica.

Valutazione / Raccomandazione

L'ondata di e-mail del maggio 2018 ha portato a numerose segnalazioni a MELANI e anche a una certa confusione, poiché in molti casi si è supposto che anche la password relativa all'indirizzo e-mail fosse stata rubata e venduta, il che, per fortuna, non era il caso. Non fa certo piacere vedere comparire il proprio indirizzo in una simile banca dati, ma difficilmente si può impedire, poiché l'indirizzo di posta elettronica è il perno e l'asse portante di tutti i servizi di Internet e perciò è ampiamente utilizzato. Nondimeno, non c'è una diminuzione del livello di sicurezza, purché ci si attenga alle direttive corrette nella gestione delle e-mail.

Regole di comportamento nella manipolazione delle e-mail sulla pagina web di MELANI

https://www.melani.admin.ch/melani/it/home/schuetzen/verhaltensregeln.html

In questi casi MELANI raccomanda di ignorare l'e-mail e di non rispondere assolutamente. Una risposta conferma agli spammer che l'indirizzo e-mail scelto funziona e i messaggi si leggono. Ciò può comportare un aumento delle e-mail di spam.

4.5 Fuga di dati

4.5.1 Sottratti a un partner commerciale i dati clienti di Swisscom

Nell'autunno del 2017 i cyber criminali hanno sottratto circa 800 000 contatti di clienti Swisscom. Tuttavia, la rete di Swisscom non è stata direttamente compromessa: gli hacker hanno ottenuto – non si sa come – i diritti di accesso di un partner di distribuzione al quale era stata affidata l'elaborazione dei dati clienti di Swisscom. Il furto è stato scoperto, in occasione di un controllo di routine.[15]

Sono state sottratte informazioni che servono ad identificare i clienti come nome, indirizzo postale, numero di telefono e data di nascita. Esse rientrano in quel genere di informazioni, che si trovano perlopiù anche negli elenchi telefonici o sui social media, non sono considerate «dati personali degni di particolare protezione». Secondo Philippe Vuilleumier, responsabile Group Security presso Swisscom, non sono stati toccati dati di persona classificati dalla legge federale sulla protezione dei dati come «degni di particolare protezione» e cioè, ad esempio, password, conversazioni o dati di pagamento. I dati sensibili come questi sono protetti da meccanismi molto rigidi.[16]

Quale misura immediata Swisscom ha bloccato gli accessi della società partner e in una seconda fase ha inasprito le misure di sicurezza. In particolare, sono stati introdotti una

[15] https://www.srf.ch/news/wirtschaft/massnahmen-eingeleitet-datendiebstahl-bei-swisscom (stato: 31 luglio 2018)

[16] https://www.swisscom.ch/it/about/medien/attualita/intervista-philippe-vuilleumier-responsabile-group-security.html (stato: 31 luglio 2018)

sorveglianza potenziata degli accessi da parte di società partner, un sistema d'allarme in caso di attività sospette e un'autenticazione a due fattori.[17]

Anche la comunicazione trasparente fa parte delle misure immediate adottate. L'incaricato federale della protezione dei dati e della trasparenza (IFPDT) è stato informato, agli abbonati di rete fissa e ai clienti commerciali è stata inviata una comunicazione scritta ed è stato istituito un servizio informazioni gratuito via SMS per dare modo ai clienti di telefonia mobile di verificare se la fuga di dati li riguardava.

4.5.2 L'utilizzo di dati rubati

Il 26 aprile 2018 l'azienda svizzera Epsitec, produttrice di un software gestionale per PMI, ha segnalato sul proprio sito web di aver subito un furto di dati. Sono stati sottratti indirizzi di posta elettronica, numeri di telefono e circa 35 000 indirizzi postali di clienti. Stando a quanto comunicato da Epsitec, non sono stati rubati numeri di carte di credito o password.[18] È particolarmente interessante l'uso che in alcune circostanze viene fatto di simili dati: poiché gli utenti sono sempre più diffidenti nei confronti delle e-mail inaspettate e impersonali, i criminali creano attraverso le informazioni raccolte delle e-mail personalizzate, per diffondere il malware Retefe. Un messaggio personalizzato o il riferimento a un contatto aziendale esistente possono indurre la vittima ad aprire un file allegato. Nella fattispecie, per conferire maggiore credibilità all'e-mail sono stati utilizzati non soltanto nome e cognome, ma anche i dati sottratti a Epsitec. L'e-mail inviata alle vittime designate avvisava di una presunta consegna da parte del corriere DHL oppure simulava una richiesta dell'Amministrazione federale delle contribuzioni (AFC).

4.5.3 Password per estorsioni a sfondo sessuale

Nel periodo in rassegna è stato constatato un ulteriore impiego di dati rubati. La particolarità consiste nel fatto che, nonostante fossero coinvolti dati sensibili come le password, essi risalivano per lo più a diversi anni fa e, di conseguenza, nel caso delle password, non venivano più utilizzate da buona parte degli utenti rivoltisi a MELANI. A prima vista quindi questi dati sembrerebbero avere poco valore, non essendo, in molti casi, più validi, non potendo cioè essere sfruttati per accedere ad un account. I criminali hanno però trovato il modo di farli fruttare. Nell'estate del 2018 MELANI ha rilevato infatti una serie di ondate di e-mail con tentativi di ricatto. I criminali minacciavano i destinatari di pubblicare materiale compromettente precedentemente acquisito infettando il computer con un malware.[19] I ricattatori affermavano di avere anche il controllo della webcam della persona presa di mira. Come prova essi menzionavano una password o un numero di cellulare realmente utilizzati, quantomeno precedentemente, dalla vittima. La menzione di dati tanto personali serve a conferire maggiore credibilità alla richiesta e a disorientare i destinatari. Proprio qui entrano in gioco le informazioni acquisite con furti di dati di vecchia data, come è accaduto per tutti i casi segnalati.

---

17 https://www.swisscom.ch/it/about/medien/press-releases/2018/02/20180207-mm-swisscom-verschaerft-sicherheitsmassnahmen-fuer-kundenangaben.html (stato: 31 luglio 2018)

18 https://www.watson.ch/digital/schweiz/581594688-hacker-klauen-35-000-kundendaten-bei-schweizer-software-firma-epsitec (stato: 31 luglio 2018)

19 https://www.skppsc.ch/it/temi/internet/sextortion/?noredirect=it_IT (stato: 31 luglio 2018)

Valutazione

I ricattatori hanno inviato le e-mail alla cieca sperando che tra i destinatari vi fossero persone che negli ultimi tempi avevano visitato siti pornografici e che fossero quindi più inclini a cedere al ricatto. A MELANI non è stato segnalato un solo caso di questo genere in cui gli autori fossero effettivamente in possesso di materiale, fotografico o video, compromettente e tanto meno che lo avessero diffuso o pubblicato.

4.5.4 «Credential stuffing» con vecchie password

Molti utenti cambiano regolarmente le loro password, ma se un criminale riesce a procurarsi molti record di dati, tra di essi vi sono sempre delle password valide. Molti utenti utilizzano la stessa password per diversi servizi e a lungo. Ciò semplifica di molto il compito ai criminali consentendo loro di testare sistematicamente, con differenti fornitori di servizi Internet, i dati di accesso raccolti attraverso le varie fughe di dati. In questi casi si parla del cosiddetto «credential stuffing». Utilizzando le stesse credenziali per servizi diversi si consente ai criminali, con un po' di fortuna o di perseveranza, di accedere e fare un uso indebito dei servizi. In un caso segnalato a MELANI nel 2018, quasi un milione di credenziali rubate sono state utilizzate per tentare di accedere a un portale online. I dati utilizzati abusivamente provenivano da furti, in parte molto vecchi, subiti da altri fornitori.

Valutazione / Raccomandazione

I siti di e-commerce e altri servizi Internet vengono regolarmente hackerati per rubare i dati clienti. Se le password non sono criptate o lo sono soltanto in misura insufficiente, i criminali possono acquisire i dati d'accesso con cui tentano poi di accedere a molte altre piattaforme Internet, sperando che gli utenti utilizzino le stesse credenziali per vari servizi.

I servizi che constatano simili tentativi di accesso possono annunciarsi a MELANI. I dati verranno inseriti nel check tool (www.checktool.ch), che permette agli internauti di verificare se i loro dati sono stati rubati.

Le password utilizzate online devono essere sufficientemente lunghe in modo da essere difficili da indovinare. Per ogni sito di e-commerce e/o servizio bisognerebbe scegliere una password differente e, se possibile, attivare un'autenticazione a due fattori.

4.6 Crimeware

Anche nel primo semestre del 2018 vi sono state molte infezioni con crimeware. La statistica nella figura 7 mostra la ripartizione dei principali software nocivi in Svizzera. Esistono anche malware che, pur essendo rilevanti, non appaiono nelle statistiche, come ad esempio Retefe, il malware per l'e-banking che non è un software dannoso in senso stretto del termine, poiché si limita a modificare le impostazioni del browser.

Come già negli anni passati, la maggior parte delle infezioni è da imputare a Downadup (noto anche come «Conficker»). Questo worm esiste già da oltre dieci anni e si propaga attraverso una falla di sicurezza nei sistemi operativi Windows scoperta nel 2008. Anche il relativo patch è disponibile dal 2008. Al secondo posto segue Gamut – un malware spam (o «malspam») che nell'ultimo trimestre del 2017 sarebbe responsabile del 37 per cento dei messaggi spam a livello internazionale. La botnet Gamut invia innanzitutto spam inerenti a offerte di lavoro ai

fini di reclutamento come «money mule».[20] Al terzo posto si trova Gamarue[21], noto anche come «Andromeda». Si tratta di un downloader in grado di scaricare altri malware. Al quarto e quinto posto vi sono, rispettivamente, Spambot e Stealrat, anch'essi responsabili dell'invio di spam. Stealrat lo fa attraverso domini o indirizzi IP infetti, tra i quali troviamo WordPress, Joomla! e Drupal. I messaggi spam sono così inviati attraverso server di posta elettronica legittimi e quindi più difficili da filtrare. Il sesto posto è occupato da Monerominer, il primo cryptominer in classifica, mentre per trovare il primo trojan bancario, Gozi, occorre andare alla nona posizione. La botnet Mirai, nota per aver attaccato il fornitore di servizi Internet Dyn, è uscita dalla top eleven.

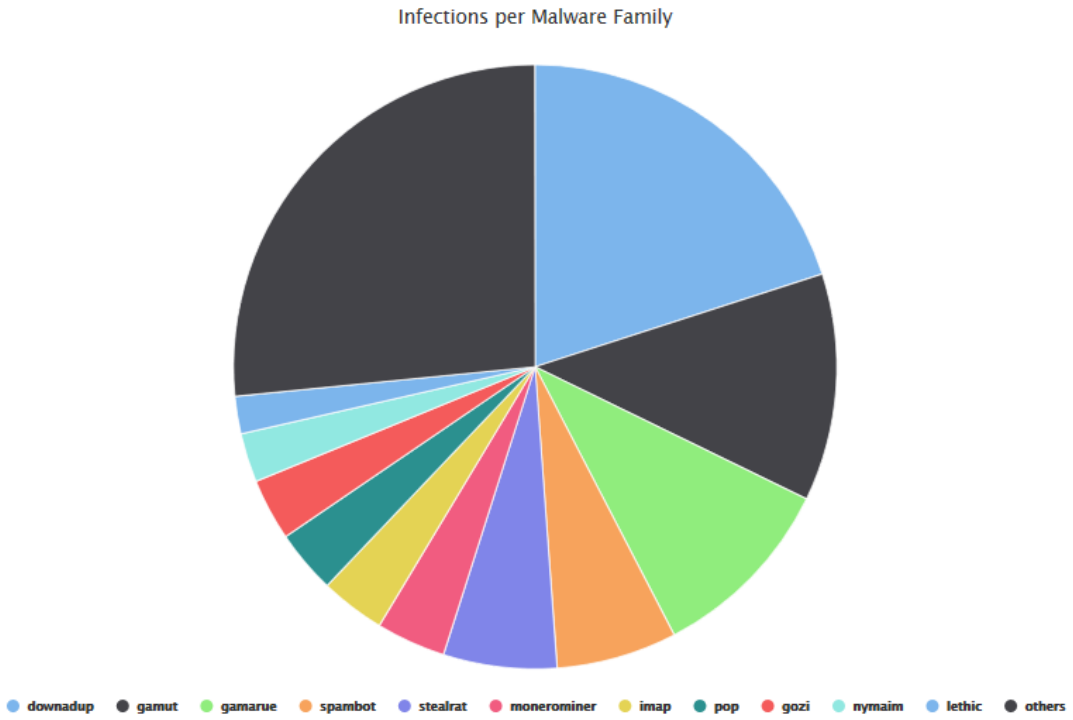


Figura 7: Ripartizione dei malware noti a MELANI in Svizzera (giorno di riferimento: 30 giugno 2018). I dati aggiornati sono pubblicati all'indirizzo: https://www.govcert.ch/statistics/malware/.

4.7 Trojan bancari in Svizzera

I sistemi di pagamento online sono obiettivi allettanti per i criminali informatici, poiché permettono di conseguire utili elevati con un rischio relativamente basso. La maggior parte delle campagne informatiche attuali combinano metodi di social engineering e l'utilizzo di malware. Vengono inoltre usati diversi trucchi per aggirare i programmi antivirus, per proteggere la propria infrastruttura da tentativi di take down e per sfuggire ai provvedimenti

[20] https://sensorstechforum.com/de/necurs-gamut-botnets-spam/ (stato: 31 luglio 2018)

[21] https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/BotNetze/Avalanche/Schadsoftware/Andromeda_Gamarue.html (stato: 31 luglio 2018)

delle autorità di perseguimento penale. Anche nel periodo in esame sono stati impiegati diversi trojan bancari.

4.7.1 Retefe e social engineering

Attualmente Retefe è tra i trojan più diffusi in Svizzera. Una volta la propagazione del malware avveniva in primo luogo attraverso l'invio di false fatture a nome di negozi online come Zalando o Ricardo, ma recentemente Retefe ha aumentato il numero dei propri mittenti aggiungendo molte aziende conosciute. Nel primo semestre del 2018 MELANI ha registrato diverse ondate di spam a nome di DHL, delle FFS, e delle forze di polizia di vari Cantoni, dell'AFC e della compagnia aerea Swiss. Inoltre, Retefe è passato dall'invio capillare di spam a quello mirato con contenuto personalizzato: le e-mail contenevano nome e numero di telefono corretti dei destinatari. Se la personalizzazione presuppone una preparazione più accurata dell'attacco, gli sforzi vengono però ripagati, poiché le vittime si lasciano ingannare più facilmente e le possibilità di infettare un dispositivo elettronico aumentano.

Il software nocivo punta a modificare le impostazioni del browser (Internet Explorer, Firefox e Chrome) in modo tale che, quando la vittima apre una pagina di e-banking, essa venga reindirizzata su una copia gestita dai cyber criminali. Al momento del login nel presunto portale di e-banking viene dapprima visualizzato un codice QR che, una volta aperto da uno smartphone, conduce a un cosiddetto trojan per furto tramite sms. Dopo l'installazione di questa applicazione per Android, tutti gli sms spediti dalla banca per l'autenticazione a due fattori vengono reindirizzati agli hacker. I truffatori possono così collegarsi all'e-banking della vittima ed inviare ordini di pagamento. In un altro caso i cyber criminali hanno tentato di ottenere i dati di attivazione per l'e-banking. Di solito i clienti delle banche ricevono questi dati attraverso lettere recapitate tramite posta, le quali possono contenere un codice QR che dev'essere scansionato mediante un'apposita applicazione per il primo accesso all'e-banking tramite smartphone. Lo smartphone è così riconosciuto dalla banca quale mezzo di comunicazione per l'autenticazione a due fattori. I truffatori hanno indotto le vittime mediante e-mail a scansionare o fotografare le suddette lettere.[22] Finora Retefe è stato diretto contro i sistemi Windows, ma nel 2017 diverse ondate hanno preso di mira gli utenti svizzeri del sistema operativo MacOS.[23]

Dal settembre 2017 anche la vulnerabilità EternalBlue è stata integrata nel repertorio della campagna d'attacco. Se un collaboratore di una ditta apre inavvertitamente un allegato infetto, grazie a questa falla il malware infetta il computer utilizzato per accedere al servizio e-banking. Naturalmente questa pratica funziona soltanto se la vulnerabilità, per la quale il 14 maggio 2017 è stata emessa una patch di sicurezza, non è ancora stata eliminata. L'implementazione di EternalBlue sembra indicare che Retefe abbia preso di mira innanzitutto le PMI.

4.7.2 Dridex e software offline per i pagamenti

Alle nostre latitudini è molto diffuso anche il trojan bancario Dridex. Si tratta di un worm comparso per la prima volta nel 2012 con il nome di Cridex. La diffusione di un worm presenta però degli inconvenienti, poiché necessita di falle di sicurezza aperte e la sua propagazione

---

22 https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/e-banking--angreifer-haben-es-auf-aktivierungsbriefe-abgesehen.html (stato: 31 luglio 2018)

23 https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/malware---si-raccomanda-prudenza-indipendentemente-dal-sistema-o.html stato: 31 luglio 2018)

può essere rilevata facilmente. Le versioni più recenti vengono perciò diffuse quasi esclusivamente tramite invii di spam massicci. A tale scopo si impiegano documenti di Word infetti camuffati da fatture, conferme di ordini online, solleciti di pagamento o simili. I mittenti sembrano essere vere aziende che spesso hanno sede nello stesso Paese delle vittime. Le e-mail preparate per la Svizzera sono principalmente in tedesco. Nel primo semestre del 2018 nel nostro Paese è stata registrata una sola ondata finalizzata a propagare Dridex: le e-mail inviate a nome di Swisscom contenevano una fattura elettronica molto simile a quelle legittime. Il campo su cui cliccare per visionare la fattura celava un collegamento a un JavaScript dannoso che tentava poi di installare Dridex.

Una volta installato, Dridex applica il cosiddetto metodo «man in the middle» (MITM). Con questa tecnica, senza farsi notare l'hacker si inserisce in un canale di comunicazione tra due partner – in questo caso la banca e il cliente di e-banking – per potere seguire e manipolare lo scambio di dati. Dridex ha un'organizzazione decentralizzata e la sua architettura di rete è suddivisa su più livelli e in reti subordinate gestite da differenti operatori, il che rende difficile alle autorità adottare contromisure. Per tale motivo Dridex continua a rappresentare un serio pericolo, sebbene nell'ottobre 2015 il Ministero delle giustizia statunitense e l'FBI abbiano arrestato il presunto capo della botnet e altri membri in un secondo tempo.[24]

Nel luglio 2016 Dridex ha esteso il proprio modus operandi ai sistemi offline per i pagamenti.[25] Dopo aver infettato il computer, il malware cerca nel computer software offline per i pagamenti. Questo tipo di software è utilizzato da molte imprese per trasmettere via Internet a una o più banche grandi quantità di pagamenti. Se Dridex trova sul computer i suddetti software, scarica da Internet dei malware specifici che permettendo al truffatore di effettuare pagamenti fraudolenti. In alcuni casi è stato ad esempio utilizzato il codice nocivo Cobalt Strike, in altri Carbanak. Se sul computer infetto non trovava software offline per i pagamenti, Dridex attaccava le sessioni di e-banking conformemente alle sue possibilità.

Dal 2016 anche i portafogli digitali di criptovaluta (cryptocurrency wallet) sono nel mirino di Dridex. E nell'anno in corso gli obiettivi inseriti nel file di configurazione sono aumentati.

Al momento si osserva solo un'attività moderata sia in Svizzera che all'estero. Ciò non significa però che il pericolo sia in diminuzione. Questo periodo di calma apparente, potrebbe essere interpretato come fase di aggiornamento per prepararsi a nuovi attacchi. Inoltre, altre organizzazioni che probabilmente hanno un rapporto di collaborazione con Dridex, come il gruppo Cobalt Gang, continuano a palesarsi con una certa regolarità.

4.7.3 Gozi ISFB e la diffusione drive-by

Gozi, malware sviluppato per attaccare il settore bancario, è stato osservano per la prima volta in Svizzera nel gennaio del 2009. Si presume che sia stato creato dal russo Nikita Kuzmin, arrestato dall'FBI nell'agosto del 2011.[26] Ciononostante, vari cyber criminali continuano a impiegarlo grazie alla sua diffusione sui mercati illegali. La nuova versione, Gozi ISFB, ha

---

24 https://www.fbi.gov/contact-us/field-offices/pittsburgh/news/press-releases/bugat-botnet-administrator-arrested-and-malware-disabled (stato: 31 luglio 2018).

25 https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/offline-payment-software.html (stato: 31 luglio 2018)

26 https://www.justice.gov/usao-sdny/pr/nikita-kuzmin-creator-gozi-virus-sentenced-manhattan-federal-court (stato: 31 luglio 2018)

preso di mira i clienti di banche svizzere per la prima volta nel maggio del 2015. Anche Gozi utilizza il metodo «man in the middle» (MITM).

La nuova variante di Gozi viene propagata innanzitutto attraverso l'infezione di pagine web. Le versioni online dei quotidiani, visitate ogni giorno da numerosi lettori, sono obiettivi d'attacco ideali per questo genere di malware, poiché consentono di raggiungere un gran numero di vittime. Per propagare il trojan bancario, nel marzo del 2017 è stata ad esempio attaccato il sito web di 20min.ch.[27] Si osservano, parimenti, ondate di e-mail con allegati zip infetti, come all'inizio dello scorso mese di marzo, quando è stato allegato il presunto annuncio dell'arrivo di un pacco da parte di Fedex. Nel 2018 Gozi ha utilizzato per la prima volta anche «malvertising»; questa tecnica consiste nell'indurre l'utente a scaricare un software manipolato attirandolo con annunci pubblicitari. Spesso nei motori di ricerca gli annunci vengono visualizzati sopra i risultati della ricerca, confondendo gli utenti. Nel caso concreto, i criminali hanno pubblicizzato su google.ch il software Java e Firefox, che oltre al programma desiderato comprendeva anche il malware.

Attualmente anche Gozi sembra prendere di mira, oltre ai sistemi di e-banking, anche software offline per i pagamenti e wallet di criptovalute. L'interesse per questi obiettivi moderni pare essere una tendenza generale del prossimo futuro.

Valutazione / Raccomandazione

Le tre campagne evidenziano alcune tendenze nel settore degli attacchi ai sistemi di pagamento. Oltre ai tradizionali vettori d'attacco quali e-mail e pagine Web infette, anche l'abuso di pubblicità a scopi criminali si rivela un metodo efficace per diffondere malware bancari. Per gli utenti diventa sempre più difficile riconoscere simili attacchi. Sono quindi in primo luogo i gestori delle pagine Web a dover svolgere una verifica sistematica degli annunci pubblicitari e di altri contenuti dinamici – proprio di ditte terze esterne. Gli utenti devono continuare a essere prudenti quando ricevono le e-mail, anche se apparentemente serie e personalizzate. Si raccomanda perciò di cliccare piuttosto una volta in meno che una volta in più su un link o un allegato. Un altro trend evidente è che le PMI sono sempre più spesso bersagli di attacchi ai sistemi e-banking perché, tendenzialmente, sono meno protette delle grandi aziende, ma operano comunque un volume di transazioni bancarie superiore rispetto a un privato. Nell'ambito della sicurezza informatica le PMI svizzere sono perciò confrontate a sfide crescenti. Quanto alle misure da adottare internamente, di recente MELANI ha pubblicato un aggiornamento del «Promemoria sulla sicurezza delle informazioni per le PMI», che contiene consigli e suggerimenti su come le imprese possano migliorare la sicurezza informatica della loro rete aziendale:

DOCU

Promemoria sulla sicurezza informatiche per le PMI

https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/promemoria-sulla-sicurezza-informatica-per-le-pmi.html

[27] https://www.srf.ch/news/schweiz/nach-malware-attacke-auf-20-minuten-was-sie-jetzt-tun-koennen (stato: 31 luglio 2018)

5 La situazione a livello internazionale

5.1 Spionaggio

5.1.1 Sofacy chiamato in causa in relazione a diversi incidenti

Sofacy, noto anche come «APT28», «Fancy Bear» e «Tsar Team», si conferma uno dei gruppi di spionaggio più attivi e conosciuti a livello mondiale. Utilizza ogni vettore di infezione possibile: spear phishing perpetrato tramite e-mail ben preparate e mirate con allegati o link appositamente predisposti, oppure attacchi compiuti tramite i cosiddetti «watering holes». In queste campagne viene utilizzato un vasto arsenale di server del tipo «command and control». Gli sviluppatori che si celano dietro a Sofacy non si limitano ad adeguare il malware alle singole vittime, ma svolgono anche un notevole lavoro per sferrare attacchi ad hoc di social engineering[28]. Oltre agli attacchi molto mirati a cui la campagna ci ha abituati, sono state osservate ultimamente azioni ad ampio spettro per raggiungere il massimo numero possibile di potenziali vittime. Negli attacchi compiuti con il programma nocivo Zebrocy, un downloader per backdoor, gli obiettivi (indirizzi di posta elettronica) non sono stati selezionati in modo specifico, bensì piuttosto casualmente ed erano facilmente reperibili, ad esempio mediante motori di ricerca. Questo modus operandi è abbastanza atipico per una campagna di spionaggio informatico APT, mentre è più diffuso tra i criminali informatici. Una simile strategia aumenta la probabilità di successo di un'infezione, ma accresce pure il rischio di essere scoperti[29]. Merita di essere sottolineata anche la diffusione degli attacchi sferrati in Estremo Oriente con un forte interesse per le organizzazioni militari, di difesa e diplomatiche[30]. La scelta di obiettivi e tattiche differenti rende più difficile l'attribuzione e questo potrebbe essere anche il motivo dell'attuale sviluppo di Sofacy.

Nel 2018 è salito alla ribalta delle cronache il malware Olympic Destroyer in relazione con i Giochi olimpici di PyeongChang (Corea del Sud). Questo worm ha attaccato l'infrastruttura TIC delle Olimpiadi invernali e quella di alcuni partner. Sebbene non sia possibile una chiara attribuzione, la società di sicurezza informatica Kaspersky Lab ha individuato alcune analogie con Sofacy (v. anche cap. 4.1.1).

Il 10 gennaio 2018 il gruppo Fancy Bears Hack Team ha pubblicato dati che sarebbero stati sottratti al Comitato olimpico internazionale e al Comitato olimpico nazionale statunitense tra la fine del 2016 e l'inizio del 2017. Anche in questo caso si sospettano legami con il gruppo Sofacy[31].

---

28 https://securelist.com/a-slice-of-2017-sofacy-activity/83930/ (stato: 31 luglio 2018)

29 https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/ (stato: 31 luglio 2018)

30 https://www.kaspersky.it/about/press-releases/2018_sofacy (stato: 31 luglio 2018)

31 https://www.wired.com/story/russian-fancy-bears-hackers-release-apparent-ioc-emails/ https://www.mid-day.com/articles/russia-apparently-hacking-winter-olympics-emails-report/18923160 https://www.eclecticiq.com/resources/russian-hacking-group-fancy-bear-prepares-to-attack-winter-olympics-u-s-senate (stato: 31 luglio 2018)

5.1.2 VPN Filter – Colpiti almeno 500 000 apparecchi

Il 23 maggio 2018 Talos, il centro di ricerca per la sicurezza informatica di Cisco, ha pubblicato dati riguardanti una rete bot chiamata «VPN Filter», che si presume comprenda almeno mezzo milione di router e NAS[32]. Se l'hacker impartisce un determinato ordine, il malware sovrascrive i primi 5000 byte del primo blocco di memoria, dopo di che il dispositivo non può più avviarsi. È facile immaginare quali possano essere le ripercussioni se venisse messo fuori funzione contemporaneamente mezzo milione di apparecchi, localizzati in 54 Paesi, prevalentemente in Ucraina. Torna alla mente il malware NotPetya. Anche in quel caso l'attacco aveva preso di mira l'Ucraina, ma vi furono ripercussioni in tutto il mondo.

Tutti i computer infettati erano collegati a Internet e presentavano note falle nella sicurezza oppure erano protetti soltanto con password standard. VPNfilter è stato scoperto su diversi apparecchi, tra l'altro dai produttori di router MikroTik, Linksys, Netgear, TP-Link, ma sono stati colpiti anche i dispositivi NAS prodotti da QNAP. Il malware opera in tre fasi distinte: solo la prima si installa in permanenza sull'apparecchio, per poi scaricare il vero e proprio malware e le relative funzioni nelle due fasi successive.

All'inizio il malware poteva essere eliminato soltanto ripristinando le impostazioni di default. Quasi contemporaneamente alla divulgazione della rete bot, l'FBI è riuscita a prendere il controllo del server che, dopo il riavvio, fornisce nella seconda fase le informazioni su dove e come il malware debba essere reinstallato. In concreto, il software malevolo legge le informazioni necessarie a una nuova installazione dai metadati di un'immagine memorizzata su Photobucket.com, una piattaforma di condivisione online di foto e video. Il riavvio non elimina il malware, che tuttavia non riesce più a scaricare le vere e proprie funzioni della fase due e tre. Le misure adottate dall'FBI consentono di neutralizzare quasi completamente il software maligno e di identificare gli apparecchi infettati. Nella sua analisi, Cisco Talos ha individuato un caratteristico errore nell'attuazione della crittografia utilizzata RC4, già emerso in rapporto con il malware BlackEnergy.

5.1.3 Attaccata la rete del Governo tedesco

Alla fine di febbraio 2018 è stata diffusa la notizia che il Ministero degli affari esteri tedesco è rimasto vittima di un cyber attacco, probabilmente avvenuto già tra la fine del 2016 e l'inizio del 2017[33]. Gli autori avrebbero avuto accesso per circa un anno alla rete centrale di dati dell'Amministrazione federale tedesca, la cosiddetta rete telematica Berlin-Bonn (IVBB). La IVBB è una sorta di Intranet per il Bundesrat, la Cancelleria, i ministeri e la Corte dei conti nonché diverse autorità preposte alla sicurezza. Dopo quello che ha colpito la rete del Bundestag nel 2015, questo è il secondo attacco di vasta portata sferrato all'infrastruttura TIC del Governo tedesco[34].

---

32 https://blog.talosintelligence.com/2018/05/VPNFilter.html (stato: 31 luglio 2018)

33 https://www.zeit.de/politik/2018-04/hackerangriff-bundesregierung-russland-verfassungsschutz-hans-georg-maassen (stato: 31 luglio 2018)

34 https://www.zeit.de/digital/datenschutz/2018-03/hackerangriff-bundesregierung-outlook-auswaertiges-amt (stato: 31 luglio 2018)

Si presume che gli hacker si siano serviti di una piattaforma di apprendimento utilizzata per la formazione continua alla Scuola federale superiore dell'amministrazione pubblica.[35] Tuttavia non sono state diramate informazioni più precise sulle vulnerabilità probabilmente utilizzate[36].

Diversi media avevano ipotizzato che dietro all'attacco potesse esserci il gruppo Sofacy. Solo in un secondo momento il sospetto è caduto sul gruppo Snake/Turla, considerato responsabile pure di alcuni attacchi in Svizzera. Anche l'azienda di armamenti Ruag ha subito un attacco attribuito a Snake/Turla.

5.1.4 Attacchi contro le aziende fornitrici di energia elettrica

Il 15 maggio 2018 la Süddeutsche Zeitung ha pubblicato la notizia di un attacco contro Netcom BW, fornitrice di telecomunicazioni, filiale di EnBW, compiuto già nel corso dell'estate del 2017[37]. Sebbene sia stato sventato già nella fase iniziale, secondo il quotidiano è stato comunque possibile, per breve tempo, intercettare il traffico Internet. Servendosi dell'account dei dipendenti di un fornitore esterno di servizi, gli hacker sono riusciti ad accedere al router. Si presume che, tra l'altro, siano state sfruttate anche le falle del software Cisco per i router, tuttavia non sono stati resi noti dettagli riguardanti la vulnerabilità. Una volta preso il controllo, i criminali informatici potevano avviare programmi e scaricare dati. Sembra comunque che non sia stato corso il rischio di sabotaggio, poiché l'energia non verrebbe distribuita tramite la rete di Netcom. Inoltre, l'attacco sarebbe stato scoperto nello stadio iniziale. Non è stato possibile individuare con sicurezza gli autori, ma è sospettato il gruppo Sandworm, a cui sono stati attribuiti gli attacchi sferrati contro la rete elettrica ucraina nell'inverno 2015/2016, e il gruppo Dragonfly, che già lo scorso anno aveva richiamato l'attenzione per aver preso di mira aziende elettriche occidentali[38].

Il 7 giugno 2018 l'Ufficio federale della Protezione della costituzione (BfV) si è rivolto alle aziende elettriche tedesche tramite una pubblicazione in cui rivelava che erano in corso attacchi da parte del gruppo APT Dragonfly, diretti contro l'approvvigionamento di energia elettrica ed idrico, lo smaltimento di acque reflue nonché la tecnica dell'informazione e le telecomunicazioni. Sarebbe emerso che gli attacchi degli ultimi mesi erano rivolti soprattutto a componenti delle infrastrutture come i router[39]. Per le loro offensive i cyber criminali utilizzano spesso strumenti di pubblico dominio e cercano di assumere il controllo di sistemi non sufficientemente protetti. In generale, per ottenere l'accesso, cominciano analizzando la rete di una potenziale vittima con un port scanner per mappare le porte presenti nel computer. Il 13 giugno 2018 anche l'agenzia governativa tedesca responsabile della sicurezza informatica

---

35 http://m.faz.net/aktuell/politik/inland/hacker-angriff-war-gezielter-angriff-auf-das-auswaertige-amt-15476826.html (stato: 31 luglio 2018)

36 https://www.tagesschau.de/inland/hackerangriff-bundesregierung-101.html (stato: 31 luglio 2018)

37 https://www.sueddeutsche.de/digital/enbw-tochter-hacker-haben-deutschen-energieversorger-angegriffen-1.3980625 (stato: 31 luglio 2018)

38 Rapporto semestrale MELANI II/2017 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2-2017.html (stato: 31 luglio 2018)

39 https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/pb-spionage-und-proliferationsabwehr/broschuere-2018-06-bfv-cyber-brief-2018-01 (stato: 31 luglio 2018)

ha messo in guardia contro attacchi rivolti non solo al settore dell'energia, ma anche ad altri settori[40].

Nel mese di luglio del 2018, il Dipartimento della sicurezza interna degli Stati Uniti ha reso noto a sua volta che negli ultimi anni erano stati attaccati centinaia di obiettivi nel settore della fornitura di energia del Paese. Apparentemente gli hacker erano riusciti ad accedere fino ai centri di controllo ed erano quindi penetrati così profondamente negli impianti da poter «azionare gli interruttori», compromettendo o sospendendo l'erogazione di energia[41]. Nella maggior parte dei casi gli hacker hanno cercato di accedere mediante società terze dotate di una rete protetta in modo inadeguato. Ad esempio, hanno inviato e-mail di phishing per carpire le credenziali di login. Una volta entrati in questa rete, si concentravano sul loro vero e proprio obiettivo, i fornitori di energia elettrica[42].

5.1.5 Gli hacker prendono di mira Smart Install di Cisco

Già dal 2016 sono regolarmente riportate notizie di attacchi contro gli switch di Cisco mediante Smart Install (SMI), una funzione che consente la configurazione e la gestione in remoto. Sono vulnerabili i dispositivi collegati a Internet direttamente e senza protezione, poiché il software non richiede l'autenticazione. La protezione deve essere installata appositamente dal gestore[43]. Cisco aveva reso noto il problema già nel mese di febbraio del 2017[44], tuttavia, dal momento che il funzionamento degli apparecchi non è compromesso, Cisco non vi intravedeva una vulnerabilità ma faceva piuttosto appello alla responsabilità degli utenti, i quali hanno il compito di proteggere i propri dispositivi. Il problema dipende dagli utenti che omettono di configurare o disattivare il protocollo. Il client attende allora costantemente sullo sfondo dei comandi per la configurazione o le installazioni. Un hacker riesce così a modificare le impostazioni del server, selezionare e modificare i dati della configurazione, sostituire il sistema operativo, creare account ed eseguire i comandi che gli interessano.

Nel frattempo oltre 200 000 dispositivi a rischio erano raggiungibili da Internet e sarebbe stato teoricamente possibile riconfigurarli o acquisirne il controllo. In Svizzera erano noti circa 1500 indirizzi IP di sistemi potenzialmente esposti[45]. Dalla fine del 2017 Cisco ha ricevuto segnalazioni che gli hacker scandagliano sistematicamente i dispositivi alla ricerca di questa falla. Come mostra un grafico elaborato da Cisco, da allora il traffico sulla porta 4786 in questione si è notevolmente intensificato.

---

40 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Cyber_Angriffe_auf_deutsche_Energieversorger_13062018.html (stato: 31 luglio 2018)

41 https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110 (stato: 31 luglio 2018)

42 https://www.nzz.ch/international/russische-hacker-sitzen-schon-an-den-hebeln-der-amerikanischen-stromversorgung-ld.1406263 (stato: 31 luglio 2018)

43 https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k17-0274_update_1.html (stato: 31 luglio 2018)

44 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi (stato: 31 luglio 2018)

45 Stato: maggio 2018

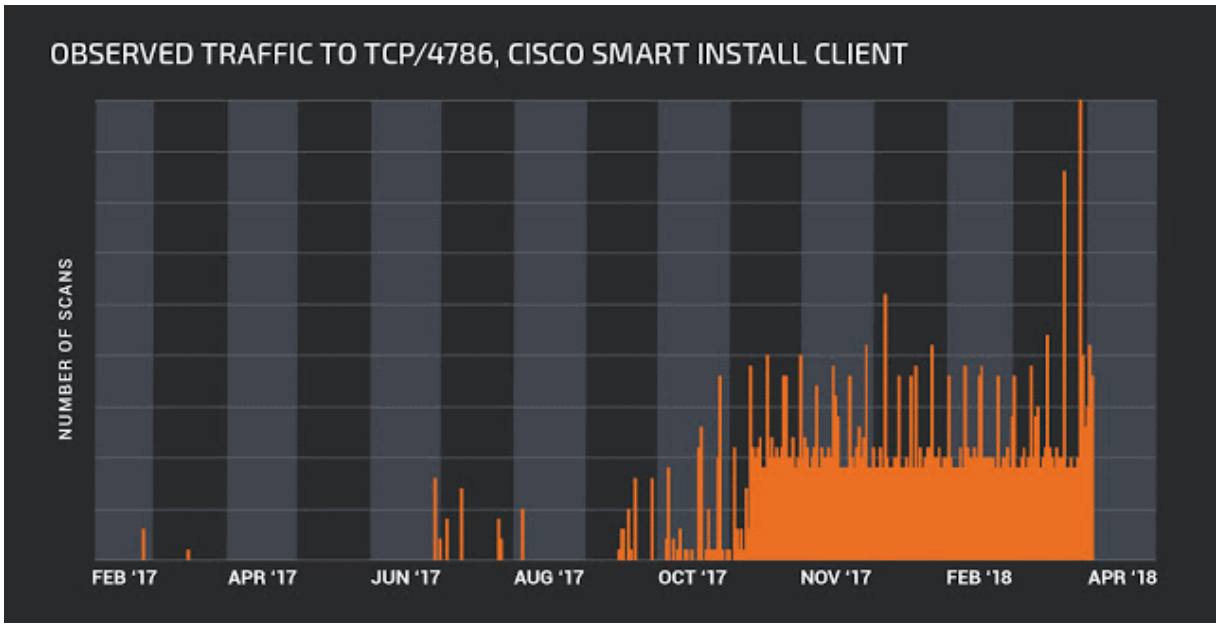


Figura 8: Numero di scansioni eseguite sui client Cisco Smart Install tra febbraio 2017 e aprile 2018 (fonte: Talos, https://www.talosintelligence.com/)

In un'altra pubblicazione di inizio aprile 2018, Cisco Talos ha segnalato la presenza di indizi di ripetuti attacchi, compiuti contro infrastrutture critiche utilizzando il protocollo SMI[46]. In concreto si sospettava un collegamento con il gruppo di spionaggio informatico Dragonfly. In precedenza, dal Computer Emergency Response Team (CERT) statunitense era stato diramato un allarme riguardante «soggetti russi» che avevano attaccato e penetrato le reti di aziende operanti nel settore dell'energia ma anche in altri settori critici.[47]

Sempre in aprile gli esperti di Kaspersky, una società che produce software per la sicurezza informatica, hanno scoperto un'offensiva commessa da cyber criminali, con la quale sono stati presi di mira soprattutto dispositivi Cisco ubicati in Iran e in Russia. Questa vasta offensiva sembra riconducibile a una rete bot che cerca porte 4786 aperte e non protette per abusare del protocollo Smart Install, sovrascrivere la configurazione e rendere inutilizzabile lo switch. Alla fine veniva lasciato un messaggio con la bandiera statunitense e il testo «Don't mess with our elections»[48].

La pubblicazione, a fine marzo, di due falle che consentono a un hacker di bloccare i dispositivi Cisco o di assumerne il controllo ha accresciuto ulteriormente all'attenzione dei media. La coincidenza degli attacchi in Russia e in Iran e della notizia delle due falle ha dato adito a numerose speculazioni sull'esistenza di un possibile nesso, inducendo Cisco a chiarire che gli attacchi sino ad allora constatati non avevano sfruttato alcuna vulnerabilità, ma erano stati causati esclusivamente da dispositivi non configurati correttamente o del tutto privi di configurazione[49].

---

46 https://blog.talosintelligence.com/2018/04/critical-infrastructure-at-risk.html (stato: 31 luglio 2018)

47 https://www.us-cert.gov/ncas/alerts/TA18-106A (as at 31 July 2018).

48 https://www.kaspersky.it/blog/cisco-apocalypse/15357/ (stato: 31 luglio 2018)

49 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180409-smi (stato: 31 luglio 2018)

Valutazione / Raccomandazione

I router sono presi sempre più di mira dai pirati informatici per due ragioni fondamentali: prima di tutto rappresentano spesso l'anello più debole della catena, poiché gli aggiornamenti non vengono sempre prontamente installati. In secondo luogo, i router sono essenziali dispositivi di rete che consentono la comunicazione all'interno di un'azienda. Inoltre, sono spesso collegati direttamente a Internet, da cui gli hacker possono attaccarli direttamente.

Il protocollo Smart Install di Cisco non richiede un'autenticazione, pertanto un hacker può prendere di mira ogni dispositivo accessibile da Internet e non dotato di un'ulteriore protezione. Si raccomanda fortemente di proteggere questi dispositivi da accessi abusivi. Inoltre, gli aggiornamenti devono essere tempestivamente eseguiti.

5.2 Sistemi industriali di controllo

5.2.1 Violazione del sistema Infotainment di Volkswagen e Audi

Nel mese di aprile del 2018 alcuni ricercatori olandesi specializzati in sicurezza hanno pubblicato uno studio in cui evidenziavano in particolare la vulnerabilità del sistema informatico di alcuni modelli di Volkswagen e Audi. La connessione Wi-Fi delle auto si è infatti dimostrata un ottimo vettore d'attacco per compromettere il sistema IVI («In-Vehicle Infotainment»). Il sistema IVI comprende diversi servizi audio e video interattivi che permettono ad esempio di ascoltare musica, ricevere informazioni o telefonare direttamente dall'auto. I ricercatori hanno rivelato che la violazione ha permesso loro di ascoltare conversazioni effettuate col vivavoce, accedere alla rubrica del telefono e seguire gli spostamenti del veicolo. Teoricamente avrebbero potuto accedere anche ad altri sistemi che controllano parti più sensibili del veicolo, come i freni e l'acceleratore, ma hanno deciso di non spingersi oltre.[50]

Non è la prima volta che la sicurezza delle auto è fonte di preoccupazioni, e dal 2015, anno in cui è stata piratata la celebre Jeep Cherokee, quest'ambito è diventato soggetto di molte ricerche.[51] La separazione tra il sistema IVI, spesso bersaglio degli attacchi, e i sistemi più sensibili del veicolo è fondamentale. I ricercatori non sono infatti riusciti a dimostrare una permeabilità tra i due sistemi. Quando viene pubblicata una vulnerabilità è sempre consigliato aggiornare l'intera flotta automobilistica, o anche a distanza, i rispettivi software, ma non sempre è fattibile. Spesso vengono aggiornati solo i sistemi dei veicoli nuovi, ma il cliente ha sempre la possibilità di far installare la patch presso il suo concessionario.

5.2.2 Cryptominer infiltrati in un impianto di trattamento delle acque

Il successo delle criptovalute offre opportunità molto allettanti ai criminali informatici. Oltre a casi di furti di Bitcoin su larga scala, i criminali hanno attaccato il mercato delle criptovalute anche in un altro modo, approfittando di uno specifico processo per questo tipo di valuta: il

50 https://www.bleepingcomputer.com/news/security/volkswagen-and-audi-cars-vulnerable-to-remote-hacking/ (stato: 31 luglio 2018)

51 https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (stato: 31 luglio 2018)

cosiddetto processo di mining, con il quale le transazioni in una criptovaluta vengono convalidate dai membri della rete e vengono create nuove unità monetarie. Questo processo richiede la risoluzione di complessi calcoli matematici che necessitano di notevoli capacità computazionali e viene compensato con una determinata somma di valuta «estratta», proporzionale al lavoro di calcolo svolto. Alla fine il mining contribuisce a creare valuta.

Poiché questo processo produce valuta, alcuni attori da qualche tempo hanno cercato di sfruttarlo a proprio vantaggio (questo tipo di casi è già stato menzionato nel nostro rapporto semestrale 2013/2[52]). Nel frattempo si sono moltiplicati gli attacchi volti a sfruttare la potenza di calcolo dei computer a scopo di mining. La ditta di sicurezza informatica Palo Alto Networks ha scoperto più di 470 000 versioni di malware che permettono di approfittare della potenza di calcolo della vittima.[53] Inoltre, non vengono prese di mira unicamente i dispositivi personali, i sistemi di burotica o server web. Secondo un articolo di portale d'informazione Security Week, un operatore di infrastrutture critiche attivo nell'ambito del trattamento delle acque in un Paese europeo, ad esempio, ha scoperto un cryptominer sulla sua rete di produzione («Operational Technology Network»)[54]. In questo caso, il malware ha rallentato la rete utilizzando la potenza di calcolo e la larghezza di banda.[55] L'infezione non ha avuto nessun impatto negativo sul funzionamento della rete, ma ha generato costi per l'impresa in termini di consumo di elettricità e di banda larga Internet. L'infezione avrebbe però potuto avere ripercussioni a lungo termine sul funzionamento dell'infrastruttura e causare conseguenze per i clienti.

5.2.3 Hide'n Seek – una botnet IoT con la funzione peer-to-peer

Con il malware Mirai l'opinione pubblica ha fatto la conoscenza delle botnet, che sfruttano i dispositivi dell'Internet delle cose per perseguire i propri scopi. All'inizio di gennaio del 2018 i ricercatori di sicurezza informatica hanno scoperto una nuova botnet IoT battezzata «Hide'n Seek», che si diffonde utilizzando il meccanismo del worm. Questo software malevolo, che ha la capacità di autoreplicarsi, crea un elenco casuale di indirizzi IP di potenziali vittime che sono poi prese di mira. Se alcune porte del dispositivo sono aperte, il malware cerca di accedere al sistema con password standard o termini del dizionario; vengono inoltre messe alla prova diverse falle di sicurezza. La rete bot si basa su una struttura periferica peer-to-peer atipica per l'Internet delle cose. Alcuni dispositivi si scambiano informazioni sui tentativi riusciti di login e apprendono l'uno dall'altro. Contrariamente a Mirai, il malware Hide'n Seek non è tanto focalizzato sulla funzione DDoS, quanto sullo spionaggio e sui successivi tentativi di estorsione. Tra le funzioni si annoverano l'esfiltrazione di dati, l'esecuzione di codici, la messa fuori funzione delle apparecchiature. Dal momento che sinora il codice malevolo non riesce ad annidarsi in modo duraturo, i dispositivi infettati possono essere ripuliti mediante la procedura di riavvio.

---

[52] MELANI rapporto semestrale 2013/2 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2013-2.html stato: 31 luglio 2018)

[53] https://researchcenter.paloaltonetworks.com/2018/06/unit42-rise-cryptocurrency-miners/ (stato: 31 luglio 2018)

[54] https://www.securityweek.com/cryptocurrency-mining-malware-hits-monitoring-systems-european-water-utility (stato: 31 luglio 2018)

[55] https://radiflow.com/case-studies/detection-of-a-crypto-mining-malware-attack-at-a-water-utility/ (stato: 31 luglio 2018)

Conclusione / Raccomandazione

La crescente tendenza alla computerizzazione e al collegamento in rete di ogni tipo di oggetto di uso comune (Internet delle cose) offre molte comodità con funzioni nuove e utili. Ne fanno parte l'elettronica d'intrattenimento e l'accesso a Internet nei mezzi di trasporto, tra cui la macchina e l'aereo. Tuttavia, gli aspetti positivi non devono indurre a trascurare i rischi collegati. Nuove opportunità celano sempre anche nuovi pericoli, da considerare già nella fase di sviluppo («security by design»).

Misure di protezione per i sistemi di controllo industriali

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

5.3 Attacchi (DDoS, Defacement, Drive-By)

5.3.1 Attacco Memcached DDoS

L'attacco sferrato il 28 febbraio 2018 a Github, fornitore di servizi online, ha rappresentato uno dei più potenti attacchi DDoS sinora registrati, con una larghezza di banda di circa 1,35 Tbps. Tuttavia, l'intervento del provider «Akamai» ha consentito di interromperlo molto in fretta[56,57]. In questo caso l'attacco DDoS si è servito della cosiddetta funzione Memcached, utilizzata nei server. Si tratta di un software open source impiegato per il salvataggio intermedio («caching») di dati che sono archiviati nella memoria di lavoro, pertanto sono facilmente accessibili e consentono generalmente una migliore efficienza, ad esempio, delle applicazioni Internet (v. anche il capitolo 3). Di norma il server si mette in ascolto sulla porta 11211 utilizzando i protocolli TCP e/o UDP, quindi è raggiungibile da tutti gli utenti di Internet. Oltre al protocollo TCP, viene utilizzato anche il trasporto senza connessione UDP, con il quale gli hacker riescono ad usufruire dei servizi Memcached non protetti con le misure necessarie, ad esempio un firewall, per lanciare attacchi DDoS contro altri utenti di Internet. In questo caso si parla di attacchi di amplificazione DDoS. Il problema maggiore consiste nel fatto che gli autori dell'attacco DDoS possono ottenere, con un unico pacchetto UDP, un fattore di amplificazione fino a 51 000, quindi raggiungere senza problemi un volume di 1 Tbps e oltre.

Al momento dell'aggressione si registravano in tutto il mondo circa 95 000 sistemi vulnerabili[58]. Successivamente, numerosi gestori di questi sistemi vulnerabili sono stati contattati per scritto con la richiesta di implementare una protezione. Lo sforzo ha senz'altro prodotto i suoi frutti,

---

56 https://githubengineering.com/ddos-incident-report/ (stato: 31 luglio 2018)

57 https://blog.apnic.net/2018/03/26/understanding-the-facts-of-memcached-amplification-attacks/ (stato: 31 luglio 2018)

58 https://blog.apnic.net/2018/03/26/understanding-the-facts-of-memcached-amplification-attacks/ (stato: 31 luglio 2018)

poiché da allora il numero di attacchi è fortemente diminuito. Anche MELANI ha informato più volte i gestori in Svizzera riguardo a sistemi vulnerabili e anche qui il loro numero si è ridotto.

Raccomandazione

Solitamente la porta UDP di Memcached (11211 UDP) non necessaria per il traffico regolare. Nel caso in cui utilizziate Memcached, consigliamo pertanto di disabilitare completamente il supporto UDP, semplicemente aggiungendo al file di configurazione di Memcached (/etc/memcached.conf) la stringa seguente:

-U 0

Limitate l'accesso al server Memcached con un firewall. Dovrebbero avere accesso a questo server solo i sistemi per i quali è necessario.

Oltre a ciò, raccomandiamo le misure note al grande pubblico per proteggere i servizi online, ad esempio:

- assicuratevi di eseguire subito gli aggiornamenti in modo da utilizzare sempre la versione più aggiornata di Memcached;
- configurate Memcached in modo che il corrispondente servizio si metta in ascolto su una porta diversa dalla 11211 con i protocolli TCP/UDP. Considerate tuttavia che questa misura da sola non è sufficiente, poiché si limita a nascondere il problema invece di risolverlo;
- controllate il server per accorgervi in fretta di un eventuale abuso.

Maggiori informazioni sulla protezione di Memcached sono pubblicate agli indirizzi seguenti:

https://www.digitalocean.com/community/tutorials/how-to-secure-memcached-by-reducing-exposure

https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/CERT-Bund/CERT-Reports/HOWTOs/Offene-Memcached-Server/Offene-Memcached-Server_node.html

5.3.2 I sistemi interni delle banche restano un bersaglio

Nel periodo in rassegna i sistemi interni delle banche sono di nuovo stati presi di mira dai criminali. A febbraio 2018, la Banca centrale di Russia ha comunicato che un anno prima un attacco contro un istituto russo aveva portato a una perdita totale di 339,5 milioni di rubli (in quel momento circa 6 mio. USD). I criminali erano riusciti a prendere il controllo di un apparecchio dal quale erano stati effettuati dei trasferimenti di denaro con il sistema interbancario SWIFT. I dettagli concernenti la vittima e l'esatto modus operandi non sono stati resi noti.

Nell'agosto del 2018 è stato comunicato un attacco ancora più spettacolare: i criminali sono riusciti a rubare 13,5 milioni di dollari alla banca indiana Cosmos. Le informazioni rilasciate indicano che l'attacco ha compromesso contemporaneamente le infrastrutture che controllavano i dispositivi per il prelievo automatico di denaro contante della banca e la sua infrastruttura SWIFT della banca. I criminali hanno così potuto prelevare contanti da distributori automatici sparsi in 28 Paesi, per un totale di 11,5 milioni di dollari, ed effettuare transazioni

con il sistema SWIFT per 2 milioni di dollari. Dopo aver inizialmente compromesso il sistema, i pirati hanno bucato i sistemi critici della banca attraverso movimenti laterali. Il livello di complessità e di coordinazione dell'attacco (avvenuto in più Paesi) è probabilmente opera di professionisti. L'impresa Securonix ha indagato sull'incidente e attribuito l'attacco al gruppo Lazarus, conosciuto per aver già preso di mira in passato i sistemi di diverse banche.[59]

5.4 Fughe di dati

5.4.1 Furto di dati personali al DHS

Nel mese di gennaio del 2018 il Dipartimento della sicurezza interna degli Stati Uniti («United States Department of Homeland Security», DHS) ha reso noto di essere rimasto vittima di un furto di dati interno. L'attacco ha riguardato i dati personali di oltre 240 000 dipendenti del DHS, in particolare risalenti al 2014. Sono stati inoltre colpiti i dati di persone che, tra il 2002 e il 2014, erano coinvolte in un'indagine da parte dell'ufficio dell'ispettorato generale del DHS. Sono stati trafugati anche i dati di testimoni e accusatori, tra cui nome, numero di previdenza sociale, indirizzo di domicilio e di posta elettronica, numero di telefono e data di nascita.

In questo caso la fuga di dati non è dovuta a un cyber attacco esterno ma a un incidente interno. Nel mese di maggio del 2017 è emerso infatti da un'inchiesta penale in corso che un ex-dipendente del DHS aveva creato una copia non autorizzata del sistema di gestione dei casi investigativi del Dipartimento.

Il DHS ha informato i suoi collaboratori per posta e ha messo a disposizione una hotline di assistenza telefonica per le persone colpite, alle quali ha offerto anche un servizio della durata di 18 mesi che monitorava l'utilizzo abusivo dei dati personali e i loro crediti. Il DHS ha inoltre implementato misure di sicurezza per limitare l'accesso ai sistemi contenenti dati personali[60].

5.4.2 Dati trafugati da Exactis

Per lungo tempo è stato possibile accedere dall'esterno a una banca dati senza protezione della società statunitense Exactis contenente dati personali di diversi milioni di persone. Exactis è una società di marketing con sede in Florida che raccoglie dati sulle preferenze e sul comportamento di milioni di persone. Non è chiara la portata esatta della fuoriuscita di dati. Si stima che siano stati colpiti 200 milioni di dati personali e 110 milioni di dati di aziende. Tra i dati si trovano informazioni commerciali, numeri di telefono, indirizzi postali e e-mail. Fortunatamente sembra che la banca dati non contenesse informazioni finanziarie, numeri di previdenza sociale e altri dati sensibili. Pur non prevedendo che le persone colpite vengano danneggiate direttamente, i dati potrebbero essere utilizzati in futuro per compiere attacchi mirati e personali contro di loro (v. cap. 6.1).

La peculiarità di questo incidente è che non si tratta di un vero e proprio atto di pirateria informatica. Il ricercatore di sicurezza informatica Vinny Troia si era servito dello strumento di

---

59 https://www.securonix.com/securonix-threat-research-cosmos-bank-swift-atm-us13-5-million-cyber-attack-detection-using-security-analytics/ (stato: 31 luglio 2018)

60 https://www.dhs.gov/news/2018/01/18/privacy-incident-involving-dhs-oig-case-management-system-update (stato: 31 luglio 2018)

ricerca Shodan per individuare in Internet le banche dati del tipo ElasticSearch[61]. Tra le altre ha scoperto così quella di Exactis, non protetta da firewall o altre misure di sicurezza, quindi accessibile a chiunque. Non è noto se Troia sia stato il primo a intercettare la banca dati oppure se i dati fossero stati già scoperti prima e copiati da altri attori. Dopo essere stata informata da Troia, Exactis ha messo in sicurezza i suoi dati.

5.5 Misure preventive

5.5.1 Arrestato un membro del gruppo Carbanak/Cobalt

Il 26 marzo 2018, in collaborazione con l'Europol e altre polizie nazionali, la polizia spagnola ha arrestato un membro del gruppo dietro al malware Carbanak (o Cobalt).[62] Il gruppo si è fatto conoscere nel 2013, attaccando le banche ed in particolare manipolando i sistemi controllanti i distributori automatici di contanti per prelevare denaro (v. rapporto semestrale MELANI 2016/I[63]). Secondo una procedura simile a quella utilizzata nel phishing, le vittime ricevevano un'e-mail contenente un documento infetto, che, una volta scaricato e aperto, permetteva ai membri del gruppo di infettare tramite spostamento laterale il sistema bancario. Si pensa che il gruppo abbia attaccato più di 100 istituti finanziari nel mondo e causato perdite per oltre un miliardo di euro.

5.5.2 Cyber Europe 2018 – preparazione alla prossima crisi informatica

Immaginatevi questa situazione: all'aeroporto è una giornata come tutte le altre. Improvvisamente gli sportelli automatici per il check-in segnalano un errore di sistema. Le app di viaggio sugli smartphone non funzionano più. Gli operatori ai banchi del check-in non riescono più a utilizzare i loro computer. I viaggiatori non possono più consegnare i bagagli né passare i controlli di sicurezza. Ovunque si formano lunghe code. Sui cartelloni dell'aeroporto tutti i voli sono annunciati come cancellati. Per motivi sconosciuti il ritiro bagagli non funziona più e oltre la metà degli aerei deve rimanere a terra. Da quanto riferito, un gruppo radicale ha assunto il comando dei sistemi critici dell'aeroporto con attacchi digitali e ibridi. Ha già rivendicato l'attacco e sfrutta i suoi canali di propaganda per diffondere un appello alla mobilitazione e reclutare nuovi proseliti della sua ideologia radicale.

Il 6 e 7 giugno 2018 oltre 900 esperti europei di sicurezza delle reti e delle informazioni provenienti da 30 Paesi diversi hanno affrontato questo scenario estremo in occasione dell'edizione di quest'anno di Cyber Europe 2018 (CE2018), sinora la più vasta esercitazione in materia condotta dai Paesi dell'UE/AELS. Cyber Europe 2018 è stata organizzata dall'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) in collaborazione con le autorità e gli uffici preposti alla sicurezza informatica di tutta Europa. Anche la Svizzera ha partecipato all'esercitazione con diversi esponenti dell'Amministrazione pubblica e dell'economia privata. L'obiettivo principale era aiutare le organizzazioni a testare i

---

61 http://www.vinnytroia.com/ (stato: 31 luglio 2018)

62 https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain (stato: 31 luglio 2018)

63 Rapporto semestrale MELANI 2016/1 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2016-1.html (stato: 31 luglio 2018)

propri piani d'emergenza interni per il mantenimento dell'operatività e i rispettivi piani di gestione delle crisi, incentivando nel contempo la collaborazione tra enti pubblici e privati. Cyber Europe rafforza questa collaborazione e rappresenta la risposta alle minacce transfrontaliere. Presuppone la piena cooperazione fra le nazioni e le organizzazioni europee.

Dati di riferimento dell'esercitazione Cyber Europe 2018:

- Paesi partecipanti: 30
  (Austria, Belgio, Bulgaria, Cipro, Croazia, Danimarca, Estonia, Finlandia, Francia, Germania, Grecia, Irlanda, Italia, Lettonia, Lituania, Lussemburgo, Malta, Norvegia, Paesi Bassi, Polonia, Portogallo, Repubblica Ceca, Romania, Slovacchia, Slovenia, Spagna, Svezia, Svizzera, Regno Unito, Ungheria)
- organizzazioni partecipanti: 300
- numero di intervenuti: oltre 900 esperti di cyber sicurezza
- numero di attacchi: 23 222

Cyber Europe è stata istituita otto anni fa ed è diventata un'importante esercitazione in materia di sicurezza delle reti e dell'informazione alla quale collaborano centinaia di esperti di sicurezza informatica di tutta Europa. Consente un'esperienza di apprendimento flessibile, poiché i partecipanti possono sintonizzare l'esercitazione sulle loro esigenze, che si tratti di singoli analisti o intere organizzazioni. La cooperazione internazionale di tutte le organizzazioni partecipanti è una delle priorità. La Svizzera ha condiviso il progetto sin dall'inizio e dal 2010 partecipa all'esercitazione Cyber Europe, che si tiene ogni due anni.

5.5.3 Presa di controllo di un server di comando e di controllo del gruppo Lazarus

Il 25 aprile l'istituto ThaiCERT ha annunciato di aver scoperto e preso in consegna un server di comando e controllo in un'università tailandese.[64] Il server sarebbe stato utilizzato dal gruppo Hidden Cobra (anche conosciuto come Lazarus Group), sospettato di aver condotto un attacco contro Sony Pictures nel 2014 e alla Banca nazionale del Bangladesh nel 2016[65] (v. rapporto semestrale MELANI 2016/I[66]). Quest'ultimo attacco avrebbe permesso al gruppo di rubare 81 milioni di dollari.

McAfee ritiene che l'operazione (battezzata «Operation GhostSecret») mirasse alle infrastrutture critiche, agli istituti finanziari, sanitari e di intrattenimento di oltre 17 Paesi, compresa la Svizzera. McAfee crede che il server faccia parte di una campagna che nel febbraio 2018 aveva preso di mira gli istituti finanziari in Turchia.[67]

---

64 https://www.thaicert.or.th/alerts/admin/2018/al2018ad001.html (stato: 31 luglio 2018)

65 https://threatpost.com/thaicert-seizes-hidden-cobra-server-linked-to-ghostsecret-sony-attacks/131498/ (stato: 31 luglio 2018).

66 Rapporto semestrale MELANI 2016/1 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-1.html (stato: 31 luglio 2018)

67 https://securingtomorrow.mcafee.com/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/ (stato: 31 luglio 2018)

Per raggiungere il loro obiettivo i criminali hanno a disposizione molti malware. US-CERT ha pubblicato diverse analisi a questo proposito e ritiene che queste attività siano riconducibili a hacker nordcoreani.[68] Secondo McAfee, al momento della scoperta del server la campagna era ancora finalizzata all'ottenimento di informazioni per progettare gli attacchi futuri.

6 Tendenze e prospettive

6.1 L'impiego dei dati negli attacchi perpetrati

Così come esposto nell'ultimo rapporto semestrale MELANI[69], le fughe involontarie di dati sono sempre più frequenti. Questa tendenza non risparmia neppure la Svizzera, come dimostrano gli incidenti accaduti a Swisscom, DVD-Shop e Epsitec.

In merito all'impiego di questi dati, i cyber criminali si dimostrano poliedrici e innovativi. Un metodo immediato per trasformare in moneta sonante i dati trafugati è ricattare direttamente la società dalla quale essi sono stati sottratti. Qui non conta tanto la criticità dei dati. Nell'epoca del Regolamento generale dell'Unione europea sulla protezione dei dati (GDPR), il solo fatto che i dati siano sfuggiti al controllo di una società la espone a ulteriori pressioni. Essa è solo una delle tante possibilità a disposizione dei criminali e l'esempio più noto in Svizzera di questo modus operandi è il gruppo di hacker Rex Mundi. In generale è constatabile la tendenza secondo cui i criminali diventano sempre più abili nel riconoscere il valore dei dati e nel trarre profitto da informazioni apparentemente prive di valore[70].

Per i malviventi è utile il fatto che le risorse di dati rubati sono quasi inesauribili sul mercato nero. Il solo portale https://haveibeenpwned.com/, sul quale chiunque può controllare se i suoi dati di accesso sono stati oggetto di un furto, contiene oltre cinque miliardi di combinazioni di nomi utente e password. A ciò si aggiunge una miriade di altri dati trafugati, attinti da account di posta elettronica o computer violati. Clandestinamente è così sorto un settore di attività che vaglia i dati, estrae quelli importanti e li raggruppa in nuove banche dati, che vengono quindi rivendute ad altri criminali. Al capitolo 4.5 sono illustrati diversi esempi di possibili utilizzi di questi dati. Tutti i differenti metodi utilizzati sono accumunati da un'attuale tendenza alla personalizzazione.

Ne sono esempio eloquente gli attacchi fasulli di sextortion: alla vittima viene fatto credere che i criminali siano in possesso di sue immagini pornografiche. Per rendere questo bluff più convincente, i ricattatori utilizzano dati personali della vittima provenienti da una fuga di dati (ad es. nome e cognome, indirizzo IP o provider utilizzato, password o numeri di cellulare).

Anche la diffusione di software malevoli è sempre più spesso personalizzata. È addirittura possibile che talvolta i dati rubati abbiano ripercussioni dirette sulle attività di un gruppo di

---

68 https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity (stato: 31 luglio 2018)

69 Rapporto semestrale MELANI 2017/2 hthttps://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2-2017.html (stato: 31 luglio 2018)

70 Rapporto semestrale MELANI 2015/1 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2015-1.html (stato: 31 luglio 2018)

malware. Un'ipotesi è che la fuga di dati della società Epsitec, un'azienda nella Svizzera romanda, abbia agevolato, un'espansione del trojan e-banking Retefe, che per anni aveva focalizzato i suoi attacchi in Svizzera contro utenti germanofoni, alla Svizzera romanda.

Un altro tipo di truffa, per la quale la base di dati riguardanti la vittima ha un ruolo cruciale, è la cosiddetta «truffa del CEO» o «President Scam». Ancora attualmente, buona parte dei criminali che mettono in atto simili truffe, concentrano la propria ricerca d'informazioni per elaborare uno scenario adeguato, sui siti delle società o sugli account dei social media. Ma anche in quest'ambito è presumibile che le fughe di dati acquisteranno un'importanza sempre maggiore. A poter essere utilizzate per questo tipo di attacchi in futuro, sono proprio fughe di informazioni analoghe a quella a cui si è esposta la società Exactis, dove un terzo dei dati proveniva da aziende.

In generale le informazioni attinte dalle fughe di dati aiutano i criminali a compiere attacchi più mirati. Sembra che la personalizzazione aumenti notevolmente la percentuale di successo rispetto agli spam di massa. C'è dunque da attendersi che in futuro molti più criminali ricorreranno a questo metodo.

6.2 Dispositivi medici, dati sanitari e cartelle dei pazienti in rete

Il processo di digitalizzazione non si ferma neppure davanti al sistema sanitario. Con il termine «eHealth» vengono indicati tutti i servizi sanitari elettronici. Gli strumenti elettronici migliorano i processi nel sistema sanitario e creano una rete dei partecipanti. L'elemento centrale è il documento sanitario digitale, la cosiddetta «cartella informatizzata del paziente» (CIP), nella quale sono memorizzati tutti i dati clinici di un individuo. In questo modo dovrebbe aumentare la qualità delle cure mediche, migliorare i processi terapeutici, la sicurezza dei pazienti dovrebbe accrescere e il sistema sanitario diventerebbe più efficiente, infine attraverso la digitalizzazione viene promossa la competenza dei pazienti in materia di salute. Mediante un collegamento sicuro a Internet, i dati sanitari possono essere consultati in qualunque momento dagli utenti e dai professionisti della salute. Sono gli utenti stessi a decidere chi è ammesso a consultare questi documenti. Ogni elaborazione della CIP è registrata. Nel protocollo di accesso viene iscritto segnatamente chi ha consultato i documenti, chi ne ha memorizzati di nuovi e quando è avvenuto. Questa registrazione completa degli accessi dà vita una "catena di fiducia" che consente di verificare in modo affidabile e su più fasi di lavoro che le informazioni siano trasmesse correttamente e fedelmente.

Confidenzialità, integrità e disponibilità dei dati nonché la tracciabilità del loro trattamento devono essere imperativamente garantite. I dati sanitari rappresentano una categoria di dati personali che meritano di essere particolarmente protetti non solo in virtù della loro natura privata, ma anche perché tendenzialmente conservano la loro validità. I dati riguardanti il nostro organismo e la cartella clinica esistono e non possono essere cambiati.

Quando un fascicolo sanitario finisce in mani sbagliate, i dati (ad esempio una particolare patologia oppure i farmaci prescritti) diventano noti e non hanno limite di durata. Questo aspetto può essere sfruttato da diversi attori. Oltre all'ovvio impiego per ricattare immediatamente le vittime, i dati dei pazienti possono essere anche conservati per essere eventualmente utilizzati in seguito, poiché non possono cambiare. In futuro una persona potrebbe rappresentare un target più redditizio, assumendo ad esempio una posizione di spicco in politica o in economia o diventando maggiormente vulnerabile al ricatto per altri motivi (o per ricavarne una somma maggiore). Tuttavia, i dati sanitari non sono interessanti soltanto per i criminali che li utilizzano direttamente, ma possono essere venduti anche ad attori

economici e statali. Ad esempio, sarebbe possibile lanciare una pubblicità personalizzata dei farmaci contro l'impotenza oppure divulgare pubblicamente informazioni sensibili.

Dal momento che neppure il sistema meglio protetto è infallibile, in ambito sanitario occorrerebbe fare in modo che i dati non possano essere automaticamente attribuiti a una persona concreta. Nella pseudonimizzazione è necessario trovare il giusto equilibrio, per la sicurezza dei pazienti, tra il pericolo di attribuzione errata dei dati da parte dei professionisti della salute legittimati e il rischio di un'attribuzione corretta da parte di terzi non autorizzati.

In Svizzera la CIP verrà attuata sotto forma di sistema decentralizzato. Questo approccio offre vantaggi nell'ottica della sicurezza dell'informazione, poiché non esiste un unico luogo nel quale sono archiviati tutti i documenti CIP della popolazione svizzera. In tal modo viene evitato il rischio di una concentrazione. L'introduzione della CIP è prevista nella primavera del 2020. Sino ad allora saranno svolti ancora numerosi test, per garantire la sicurezza del sistema e la riservatezza dei dati al momento della sua introduzione.

6.3 La velocità prima della sicurezza? Prudenza con la telefonia mobile

6.3.1 I noti problemi con il protocollo SS7 per le reti 2G e 3G

Ormai la maggior parte degli utenti conosce bene i rischi connessi all'utilizzo di reti WLAN[71] aperte. Le reti di telefonia mobile, invece, riscuotono una maggiore fiducia in termini di sicurezza da gran parte dei possessori di dispositivi mobili. Come riferito a più riprese in passato[72,73], devono essere considerati alcuni rischi anche nelle reti mobili, soprattutto se sono utilizzate come secondo canale fidato, ad esempio per ricevere codici sms utilizzati come secondo fattore di autenticazione. Il vettore tecnico che gli hacker utilizzano per violare le reti mobili di seconda e terza generazione contiene il protocollo SS7 che regola il coordinamento tra i fornitori di reti mobili, ad esempio nel roaming. Nel frattempo offerenti di dubbia reputazione[74] propongono nella Darknet l'utilizzo di queste vulnerabilità come servizio ad altri criminali. Anche società legittime[75] offrono servizi simili alle autorità[76]. Grazie all'impiego di un'opportuna tecnologia firewall da parte degli operatori di reti mobili, è possibile impedire simili abusi nella propria rete. Tuttavia, non appena qualcuno è in roaming in una rete estera, è vulnerabile a questo tipo di attacchi, se l'operatore straniero non ha attuato le misure di protezione.

---

71 https://www.melani.admin.ch/melani/it/home/schuetzen/sekundaere-grundschutz.html (stato: 31 luglio 2018)

72 Rapporto semestrale MELANI 2017/1, capitolo 5.4.5, https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2017-1.html (stato: 31 luglio 2018)

73 Rapporto semestrale MELANI 2016/2, capitolo 6.2 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/halbjahresbericht-2016-2.html (stato: 31 luglio 2018)

74 https://www.theverge.com/2017/6/13/15794292/ss7-hack-dark-web-tap-phone-texts-cyber-crime (stato: 31 luglio 2018)

75 https://www.forbes.com/sites/thomasbrewster/2017/09/27/ability-inc-ss7-hackers-fail-to-sell-surveillance/#13d65f0d734c (stato: 31 luglio 2018)

76 https://www.techrepublic.com/article/ss7-flaws-used-by-surveillance-firms-highlight-need-for-better-vendor-due-diligence/#ftag=RSS56d97e7 (stato: 31 luglio 2018)

Le speranze di aumentare la sicurezza dei clienti di telefonia mobile sono dunque riposte nelle moderne reti della quarta e, soprattutto, della quinta generazione. Per il momento i terminali dotati della tecnologia 5G non sono ancora disponibili, tuttavia le discussioni sulla messa all'asta delle frequenze necessarie e i risultati dei primi test di larghezza di banda continuano ad alimentare il dibattito sui vantaggi dell'ultima generazione di telefonia mobile. Grazie alle elevate ampiezze di banda e ai rapidi tempi di reazione, si crede che lo standard 5G abbia le potenzialità per spianare la strada all'Internet delle cose («Internet of Things», IoT) e all'industria 4.0 (IIoT). I primi test pilota[77] mostrano già i successi della tecnologia di prossima generazione.

6.3.2 LTE è molto migliorato ma è ben lungi dalla perfezione

Attualmente la tecnologia Long Term Evolution (LTE), lo standard di telefonia mobile di quarta generazione, mette a disposizione dei terminali la modalità di collegamento più rapida e spesso utilizzata. Invece del protocollo SS7, LTE punta sul protocollo Diameter. Tuttavia, è sufficiente un po' più di impegno per compiere tuttora molti degli attacchi noti a causa della configurazione non sufficientemente sicura e della retrocompatibilità con i vecchi standard. Il Dott. Silke Holtmanns di Nokia Bell Labs ha presentato le sue scoperte[78] in proposito al 34° Chaos Computer Congress. Così come nel caso degli attacchi perpetrati contro gli standard precedenti, esistono senz'altro misure[79] per colmare le lacune da parte dei gestori di reti mobili, ma non tutti le attuano con la stessa coerenza.

Nell'ultimo semestre sono state rese note ulteriori varianti di aggressione[80] contro LTE. Grazie ai cosiddetti attacchi «Authentication Relay», i ricercatori di sicurezza della Purdue University e dell'Università dello Iowa sono riusciti a intercettare messaggi di testo o dati sull'ubicazione di utenti di grossi gestori di rete statunitensi. Con l'aiuto di apparecchiature acquistate a un prezzo inferiore a 4000 dollari statunitensi potrebbero essere inviate, in questo modo, addirittura finte allerte di catastrofi a tutti gli utenti di rete di una regione.

Un team di ricerca dell'Università della Ruhr a Bochum e della New York University di Abu Dhabi ha illustrato tre nuovi scenari di attacco[81] sulle reti LTE con un dispendio leggermente superiore. Due varianti passive, che consentono di identificare gli utenti nella rete e tracciare i siti web che hanno visitato. E una variante attiva, che sfrutta una falla del metodo di codifica utilizzato per reindirizzare gli utenti su siti web falsificati mediante risposte del DNS manipolate. Anche in questo caso gli operatori di rete hanno reagito, dimostrando[82] quali siano le possibilità di sventare simili attacchi.

---

77 https://www.inside-it.ch/articles/50396 (stato: 31 luglio 2018)

78 https://www.heise.de/newsticker/meldung/34C3-Auch-4G-Mobilfunk-ist-einfach-abzuhoeren-und-zu-ueberwachen-3928496.html (stato: 31 luglio 2018)

79 https://researchcenter.paloaltonetworks.com/2018/02/sp-prevent-bad-signals-harming-network-availability/, (stato: 31 luglio 2018)

80 https://www.zdnet.com/article/new-lte-attacks-eavesdrop-on-messages-track-locations-spoof-alerts/ (stato: 31 luglio 2018)

81 https://alter-attack.net/media/breaking_lte_on_layer_two.pdf (stato: 31 luglio 2018)

82 https://blogs.cisco.com/security/protecting-against-the-latest-lte-network-attacks (stato: 31 luglio 2018)

6.3.3 La tecnologia 5G colma finalmente le lacune?

Oltre ai tanto osannati progressi ottenibili nel trasferimento dei dati, la telefonia mobile di quinta generazione promette anche una maggiore sicurezza per i gestori e gli utenti della rete. I miglioramenti sono previsti, ma purtroppo saranno riprese anche alcune lacune dagli standard precedenti. Ad esempio, l'architettura Evolved Packet Core (EPC), che fa convergere flussi vocali e di dati nella rete, entra nel nuovo standard. La mancanza di meccanismi di codifica integrati nel protocollo GTPv2 contenuto consente di monitorare i flussi di dati mobili e di lanciare attacchi DoS alle componenti di rete[83].

Come dispositivi alternativi nella tecnologia 5G vengono utilizzati anche i satelliti di comunicazione. Ciò che è da accogliere favorevolmente ai fini della resilienza della rete in caso di guasti a terra apre la strada a nuovi vettori di attacco[84] alla comunicazione mobile. Se i satelliti sono parte dello scenario d'impiego, nelle considerazioni riguardanti la sicurezza dovrebbe essere prestata attenzione ai rischi a essi collegati.

Neppure lo standard più recente riuscirà a eliminare tutti i rischi riguardanti la sicurezza delle telecomunicazioni. Una grossa responsabilità incombe tuttora sui gestori di rete mobile che devono decidere quale priorità intendono attribuire alla sicurezza nell'attuazione dello standard. Esistono già gli strumenti, tra cui la modellizzazione della minaccia[85] della propria rete e le esperienze attinte dalla sicurezza delle classiche reti TIC, ma il loro impiego comporta un costo che i gestori devono essere disposti a sostenere.

6.3.4 La sicurezza della rete da sola non basta

In conclusione, neppure con l'ultimissima generazione di telefonia mobile gli utenti possono presupporre che lo standard o il gestore elimini i rischi riguardanti la sicurezza delle informazioni. Anche nel caso della telefonia mobile è necessario attuare le misure preventive adeguate ai rischi della propria infrastruttura e delle applicazioni.

Il passato lo dimostra: gli utenti cercano di penetrare i sistemi non solo tramite la rete, ma anche mediante i processi commerciali e i collaboratori coinvolti. Spesso l'autenticazione a più fattori o i processi per reimpostare la password sono abbinati al numero di cellulare del titolare dell'account. Gli hacker sono così riusciti già più volte a trasferire il numero sul proprio dispositivo oppure a farsi inviare schede SIM sostitutive telefonando al servizio clienti del gestore della rete mobile[86].

I gestori europei di reti mobili si sono trovati di fronte a una sfida imprevista per la disponibilità della rete con le nuove regole dell'Unione europea sulle tariffe di roaming negli Stati membri. Grazie a questa novità, gli utenti hanno potuto beneficiare delle stesse condizioni della loro

---

83 https://www.darkreading.com/perimeter/new-4g-5g-network-flaw-worrisome-/d/d-id/1330062 (stato: 31 luglio 2018)

84 https://blog.trendmicro.com/trendlabs-security-intelligence/attack-vectors-in-orbit-need-for-satellite-security-in-5g-iot/ (stato: 31 luglio 2018)

85 https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2018/march/tackling-5g-security-with-threat-modelling/ (stato: 31 luglio 2018)

86 https://krebsonsecurity.com/2018/02/how-to-fight-mobile-number-port-out-scams/ (stato: 31 luglio 2018)

rete locale anche negli altri Paesi europei. Ciò ha indotto chi viaggia a non cercare più hotspot WLAN, ma a utilizzare la rete mobile per la trasmissione dei dati anche all'estero, il che ha comportato un traffico dati in roaming da sei a otto volte più elevato[87]. Questo improvviso aumento ha spinto alcuni degli operatori nelle mete turistiche ai limiti delle loro capacità.

7 Politica, ricerca, policy

7.1 Svizzera: interventi parlamentari

Affare	Numero	Titolo	Depositato da	Depositato il	CN/ CS	Dip.	Stato delle deliberazioni e link
Po.	18.3003	Una ciberstrategia globale chiara per la Confederazione	Commissione della politica di sicurezza CN	22.01.2018	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183003
Mo.	18.3249	Servizio centralizzato per lottare contro gli atti persecutori in rete (cyberstalking)	Marchand-Balet Géraldine	15.03.2018	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183249
Ip.	18.3335	Come disciplina il diritto internazionale il cyberspazio?	Dobler Marcel	16.03.2018	CN	DFAE	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183335
Ip.	18.3511	Sfruttare i vantaggi strategici della Svizzera per sviluppare un mercato digitale sicuro per l'hardware	Vonlanthen Beat	13.06.2018	CS	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183511
Ip.	18.434	Rendere finalmente perseguibile l'adescamento in rete di minorenni	Amherd Viola	14.06.2018	CN	Parlamento	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20180434
Ip.	18.3556	Ridurre i cyber-rischi attraverso la sensibilizzazione della popolazione e degli ambienti economici	Glanzmann-Hunkeler Ida	14.06.2018	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183556
Ip.	18.3562	Cyber criminalità. Prevedere l'obbligo di notifica a Melani	Gruppo PPD	14.06.2018	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183562
Po.	18.3565	Copertura del danno. Limite per evento in caso di cyber attacchi	Gruppo PPD	14.06.2018	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183565
Mo.	18.3006	Evitare il collasso delle reti di telefonia mobile e garantire il futuro della digitalizzazione del Paese	Commissione dei trasporti e delle telecomunicazioni CS	29.01.2018	CS	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183006
Ip.	18.3013	La Posta rispetta il pari trattamento tra Amazon e le altre piattaforme di commercio elettronico?	Feller Olivier	26.02.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183013

[87] https://www.lightreading.com/regulation/roam-like-at-home-the-impact-after-one-year/a/d-id/744836 (stato: 31 luglio 2018)

Dom.	18.5111	Una rete WLAN nei centri federali d'asilo?	Keller Peter	28.02.2018	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185111
IP	18.407	Iscrivere la neutralità della rete nella Costituzione	Reynard Mathias	01.03.2018	CN	Parlamento	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20180407
Ip.	18.3057	Il voto elettronico distrugge la democrazia diretta	Zanetti Claudio	01.03.2018	CN	CAF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183057
Mo.	18.3062	Rafforzamento dei diritti popolari. Raccolta delle firme elettroniche per le iniziative e i referendum in Internet	Grüter Franz	05.03.2018	CN	CAF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183062
Ip.	18.3197	Entità legale in Svizzera per i fornitori di servizi	Marchand-Balet Géraldine	14.03.2018	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183197
Ip.	18.3222	Distorsioni del mercato a scapito della Svizzera	Amherd Viola	15.03.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183222
Mo.	18.3306	Rafforzare l'applicazione del diritto in Internet introducendo un recapito obbligatorio per le grandi piattaforme commerciali in rete	Glättli Balthasar	15.03.2018	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183306
Mo.	18.3349	Garantire la neutralità della rete	Flach Beat	16.01.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183349
Ip.	18.3367	La scienza, importante risorsa della diplomazia della Svizzera	Béglé Claude	16.03.2018	CN	DFAE	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183367
Mo.	18.3379	Accesso delle autorità di perseguimento penale ai dati conservati all'estero	Commissione degli affari giuridici CS	23.03.2018	CS	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183379
Dom.	18.5258	Quando la velocità minima di Internet sarà aumentata a 10 megabit al secondo?	Candinas Martin	30.05.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185258
Oggetto CF	18.049	Legge federale sui servizi d'identificazione elettronica	Rapporto del Consiglio federale	01.06.2018		DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20180049
Ip.	18.3443	La formazione digitale degli anziani	Marchand-Balet Géraldine	04.06.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183443
Ip.	18.3448	Le fake news nella democrazia elvetica	Marchand-Balet Géraldine	04.06.2018	CN	CAF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183448
Dom.	18.5321	Accesso gratuito a Internet presso le FFS	Derder Fathi	04.06.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185321
Mo.	18.3507	Attuazione della LSCPT conformemente al dispositivo di votazione	Molina Fabian	13.06.2018	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183507
Po.	18.3590	Web 3.0 – Quale posto per la Svizzera in un web decentralizzato?	Béglé Claude	14.06.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183590

Ip.	18.3591	Sito ch.ch. Qual è il suo utilizzo e quali eventuali sviluppi sono previsti?	Wehrli Laurent	14.06.2018	CN	CAF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183591
Mo.	18.3617	Creare un'identità digitale 3.0. Per una Svizzera leader del settore blokchain e un'inedita sicurezza dei dati personali	Béglé Claude	14.06.2018	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183617
Ip.	18.3670	Connessioni WLAN nei treni FFS	Ammann Thomas	15.06.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183670
Mo.	18.3701	Contrassegno digitale a titolo volontario	Candinas Martin	15.06.2018	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183701
Mo.	18.3702	Smart data. Come far primeggiare la Svizzera nella digitalizzazione sostenibile ad elevato valore aggiunto	Béglé Claude	15.06.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183702
I	18.1044	Droni	Leutenegger Oberholzer Susanne	15.06.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20181044
Po.	18.3601	Adattare la legislazione ai droni	Marchand-Balet Géraldine	14.06.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183601
Po.	18.3478	Rapporto del Consiglio federale sulle misure da adottare per i droni	Brélaz Daniel	11.06.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183478
Ip.	18.3397	Disciplinare l'uso privato di droni	Jositsch Daniel	28.05.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183397
Dom.	18.5399	Droni in Svizzera	Leutenegger Oberholzer Susanne	06.06.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185399
Mo.	18.3371	Disciplinare l'utilizzazione dei droni per garantire ordine e sicurezza	Candinas Martin	16.03.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183371
Po.	18.3245	Identificazione di droni e di apparecchi volanti analoghi	Guhl Bernhard	15.03.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183245
Ip.	18.3463	Da Smart Cities a Smart Villages	Egger Thomas	07.06.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183463
Ip.	18.3445	Veicoli autonomi e responsabilità. A quando un adeguamento della legislazione svizzera?	Marchand-Balet Géraldine	04.06.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183445
Dom.	18.5220	Il gigante Internet Amazon è trattato come gli altri clienti della Posta nell'ambito delle tariffe di distribuzione dei pacchi?	Feller Olivier	28.05.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185220
I	18.1021	Perché la Confederazione, in qualità di proprietaria di Swisscom, non attribuisce maggiore importanza a un'ampia	Glättli Balthasar	16.03.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20181021

		politica di protezione dei dati orientata al cliente?					
Dom.	18.5209	Diffusione della rete 5G in Svizzera. Il Consiglio federale può legiferare mediante l'ordinanza	Derder Fathi	07.03.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185209
Dom.	18.5167	Implementazione della rete 5G nel settore della telefonia mobile senza aumentare i valori limite	Leutenegger Oberholzer Susanne	07.03.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185167
Ip.	18.3044	Partenariato tra la Posta Svizzera e Amazon	Reynard Mathias	28.02.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183044
Ip.	18.3575	Per apparecchiature informatiche dell'amministrazione federale che non siano frutto di lavoro infantile	Masshardt Nadine	14.06.2018	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183575
Ip.	18.3374	Discutibile assegnazione all'UFIT dello sviluppo di un nuovo software per la registrazione delle malattie tumorali. Uno spreco di denaro pubblico?	Weibel Thomas	16.03.2018	CN	DFI	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183374
Mo.	18.3219	Digitalizzazione. Promuovere la formazione continua dei lavoratori senior	Kälin Irène	15.03.2018	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183219
Mo.	18.3008	Firma elettronica quale procedura standard per i documenti interni all'Amministrazione federale	Dobler Marcel	26.02.2018	CN	CAF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183008
Mo.	18.3517	Programma di incentivazione. Digitalizzazione nelle scuole	Gruppo PPD	13.06.2018	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183517
Mo.	18.3664	Digitalizzazione anche nel sistema sanitario. Invio elettronico di tutte le fatture agli assicuratori malattie	Grossen Jürg	15.06.2018	CN	DFI	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183664
Mo.	18.365o	Una maggiore sicurezza dei pazienti grazie alla documentazione elettronica e allo scambio elettronico di dati medici	Humbel Ruth	15.06.2018	CN	DFI	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183650
Po.	18.3502	Firma digitale per i documenti interni all'amministrazione federale	Dobler Marcel	12.06.2018	CN	CAF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183502

7.2 Sviluppi politici nel settore cyber: la situazione attuale

Con le mozioni Eder (CS PLR-17.3508)[88], Dittli (CS PLR-17.3507)[89] e Grüter (CN UDC-17.3199)[90], lo scorso anno il Parlamento ha presentato tre affari di vasta portata nel settore cyber. Nel frattempo la mozione Eder è stata approvata a larga maggioranza dalle due Camere, la mozione Dittli è stata accolta dal Consiglio nazionale e dal Consiglio degli Stati con modifiche di piccola entità, mentre la mozione Grüter, approvata dal Consiglio nazionale con 134 voti a favore, 47 contrari e 9 astenuti, è stata recentemente respinta dal Consiglio degli Stati. Al Consiglio federale è stato quindi dato il mandato di creare un centro di competenza per la cyber-sicurezza e di costituire, in seno all'esercito svizzero, un comando Cyber Defence militare formato da 100 specialisti informatici/cyber professionisti. La prima scuola reclute cyber ha preso avvio nel mese di agosto del 2018, mentre per l'attuazione dei mandati in ambito civile occorre più tempo.

Con la nuova «Strategia nazionale per la protezione della Svizzera contro i cyber-rischi per gli anni 2018–2022» (SNPC II)[91], il Consiglio federale intende affrontare attivamente i rischi informatici e adottare le misure necessarie per salvaguardare la sicurezza del Paese di fronte alle minacce provenienti dal cyber-spazio. La SNPC II è stata adottata dal Consiglio federale il 18 aprile 2018. L'attuazione e l'attribuzione delle misure della SNPC II sono svolte insieme ai Cantoni, all'economia e alle scuole universitarie professionali. Anche il mandato sulla creazione di un centro di competenza per la cyber-sicurezza sarà pianificato e sviluppato nell'ambito dell'attuazione della SNPC II.

Prima della pausa estiva, il Consiglio federale ha adottato le principali decisioni in vista della creazione di un centro di competenza per la cyber-sicurezza, per intensificare i suoi sforzi nella prevenzione e nella lotta ai cyber-rischi. Secondo queste decisioni iniziali, il centro di competenza per la cyber-sicurezza dovrà essere aggregato al Dipartimento federale delle finanze (DFF) e assumere il coordinamento interno all'amministrazione federale nella lotta contro i cyber-rischi, promuovere le misure di prevenzione e fungere da interlocutore centrale per rispondere alle esigenze dell'economia e dei Cantoni. Al contempo, deve essere rafforzata la collaborazione con il mondo scientifico e la ricerca. Infine, la guida del centro di competenza sarà affidata a una persona di elevato livello gerarchico («un signor o signora "cyber"»), tuttavia senza la facoltà di impartire istruzioni, com'era invece richiesto nella mozione Eder. Il grado di centralizzazione di tutti gli uffici che operano nel settore della sicurezza informatica non è ancora chiaro allo stato attuale.

La decisione di dotare il centro di un «signor o signora cyber» con funzioni di coordinamento ma senza la facoltà di impartire istruzioni, ha sollevato ampie critiche e, in una lettera aperta delle associazioni economiche[92] e in un'altra della Commissione della politica di sicurezza del Consiglio nazionale[93], il Consiglio federale è stato esortato a dotare la funzione del «signor o signora cyber» della facoltà di impartire istruzioni. Infine, la Commissione della politica di

---

88 https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173508 (stato: 31 luglio 2018)

89 https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173507 (stato: 31 luglio 2018)

90 https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173199 (stato: 31 luglio 2018)

91 https://www.isb.admin.ch/isb/it/home/themen/cyber_risiken_ncs/ncs_strategie.html (stato: 31 luglio 2018)

92 https://www.satw.ch/cybersecurity/detail/publication/zu-den-grundsatzentscheiden-des-bundesrates-zur-cybersecurity/ (stato: 31 luglio 2018)

93 https://www.parlament.ch/press-releases/Pages/mm-sik-n-2018-08-21.aspx (stato: 31 luglio 2018)

sicurezza del Consiglio nazionale chiede l'attribuzione immediata di risorse di personale e finanziarie per il periodo transitorio, tra l'altro per sviluppare la Centrale d'annuncio e d'analisi per la sicurezza (MELANI) e per migliorare la resilienza cibernetica delle infrastrutture critiche.

Le decisioni definitive del Consiglio federale in merito alla creazione del centro di competenza non sono attese prima della fine del 2018[94].

7.3 GDPR e legge sulla protezione dei dati

Il nuovo Regolamento generale dell'Unione europea sulla protezione dei dati (GDPR) è entrato in vigore il 25 maggio 2018. Da quel momento sono applicabili le principali modifiche, tra cui il diritto all'oblio, il trattamento basato esclusivamente sul consenso dell'interessato, il diritto alla portabilità dei dati a un altro fornitore di servizi, il diritto degli interessati di essere informati in caso di violazioni della protezione dei propri dati nonché la comminatoria di multe in caso di violazioni fino al 4 per cento del fatturato annuo mondiale dell'esercizio precedente. Tuttavia permangono incertezze in merito all'attuazione legalmente conforme del GDPR caso per caso. Sebbene non si sia verificata la temuta ondata di ammonizioni tra le imprese nello spazio europeo, per molte società l'attuazione concreta del regolamento ha rappresentato una sfida, non da ultimo perché non esiste una prassi corrente in materia. Di conseguenza, dopo l'entrata in vigore del GDPR non pochi siti europei sono andati offline, ma persino i quotidiani americani sono stati temporaneamente non consultabili dagli utenti europei. Un clima di incertezza si è diffuso in particolare tra le imprese di piccole dimensioni, le associazioni, i lavoratori indipendenti e le piccole imprese del settore digitale, tra cui gli shop online e i blogger. Molti hanno ritenuto di non essere in grado di adempiere i requisiti del GDPR per motivi finanziari e organizzativi e hanno temuto per la propria esistenza a causa delle multe comminate, di conseguenza hanno per il momento limitato o disattivato i propri siti.

Raccomandazione

In linea di principio il GDPR europeo non riguarda la Svizzera, tuttavia è possibile verificare in quali casi le imprese svizzere sono interessate dall'applicazione diretta del GDPR ai seguenti indirizzi:

https://www.edoeb.admin.ch/edoeb/it/home/attualita/rgpd-last-minute.html

https://www.kmu.admin.ch/kmu/it/home/consigli-pratici/gestire-una-pmi/e-commerce/regolamento-ue-sulla-protezione-dei-dati-personali.html

https://www.economiesuisse.ch/it/datenschutz-online-check

La Svizzera continua a basarsi sulla vigente legge sulla protezione dei dati che risale al 1993. La revisione totale di questa legge non è stata ancora presa in mano dal Parlamento. Sono anteposte modifiche urgenti, resesi necessarie nell'ambito dell'Accordo di Schengen, ma per la revisione totale il Parlamento vuole prendersi più tempo. Ne consegue inevitabilmente una fase transitoria non esente da problemi per l'economia e la realtà online del Paese, che devono basarsi sulla nuova normativa e non possono prescindere dalla certezza del diritto. Tuttavia,

94 https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-71458.html (stato: 31 luglio 2018)

fino a quando non sarà conclusa la seconda fase con la revisione totale della legge sulla protezione dei dati, il quadro giuridico rimarrà piuttosto confuso.

8 Prodotti MELANI pubblicati

8.1 GovCERT.ch Blog

Nel primo semestre del 2018 MELANI non ha pubblicato alcun nuovo articolo sul blog.

8.2 Bollettino d'informazione MELANI

Nel primo semestre del 2018 MELANI ha pubblicato i seguenti bollettini d'informazione:

8.2.1 Rapporto semestrale MELANI: fughe di dati, crimeware e attacchi contro i sistemi di controllo industriali

26.04.18 - Il 26° rapporto della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), pubblicato il 26 aprile 2018, rende conto degli incidenti informatici più importanti accaduti in Svizzera e all'estero nel secondo semestre del 2017. L'accento è posto sull'impiego diffuso di crimeware e sugli attacchi contro sistemi di controllo industriali nel campo dei dispositivi medici. L'intensificazione delle fughe di dati e le loro ripercussioni sono oggetto di attento esame nel capitolo dedicato al tema principale del rapporto.

https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/rapporto-semestrale-2-2017.html

8.2.2 Telefonate fraudolente alle imprese di nuovo in aumento

05.07.2018 - Negli ultimi giorni sono di nuovo in aumento le telefonate verso aziende, in cui i criminali si fanno passare per collaboratori di una banca. I truffatori incitano la ditta ad effettuare un pagamento oppure sostengono di dover svolgere un update dell'e-banking e, in seguito a ciò, condurre una sessione di prova.

https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/truffe-via-e-mail-e-telefono-in-aumento.html

8.3 Liste di controllo e guide

Nel primo semestre del 2018 MELANI non ha pubblicato né nuove liste di controllo né nuove guide.

9 Glossario

Termine	Descrizione
Advanced Persistent Threats (APT)	Questa minaccia provoca un danno ingente, che si ripercuote sulla singola organizzazione o su un Paese. L'aggressore è disposto a investire molto tempo, denaro e conoscenze nell'attacco e dispone generalmente di notevoli risorse.
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.
Attacchi Supply Chain	Attacco con cui si cerca di infettare l'obiettivo finale infettando precedentemente un'azienda nella catena di fornitura.
Attacchi Watering Hole	Infezione mirata per mezzo di software maligno tramite siti che di preferenza vengono visitati solamente da un gruppo specifico di utenti.
Attacco DDoS	Attacco di Distributed-Denial-of-Service. Un attacco DoS in cui la vittima è attaccata simultaneamente da numerosi sistemi diversi.
Autenticazione a due fattori	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 protezione di accesso oppure un'altra funzione altrimenti protetta di un programma per computer.
Bitcoin	Sistema di pagamento decentrato che può essere utilizzato in tutto il mondo e nome di un'unità di moneta digitale.
Bot	Trae origine dalla parola slava per lavoro (robota). Designa un programma che esegue autonomamente una determinata azione alla ricezione di un comando. I cosiddetti malicious bot possono pilotare a distanza i

	computer compromessi e indurli a eseguire qualsiasi azione.
Brute Force	Metodo di risoluzione di problemi nei settori dell'informatica, della crittologia e della teoria dei giochi, fondato sulla sperimentazione di tutti i casi possibili.
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.
Codifica RC4	RC4 («Ron's Code 4») è stato sviluppato nel 1987 da Ronald L. Rivest, è un marchio registrato di RSA Security e l'algoritmo è ufficialmente segreto (Security by Obscurity).
Command & Control Server	La maggior parte dei bot possono essere sorvegliati da un botmaster e ricevere comandi attraverso un canale di comunicazione. Tale canale di comunicazione è denominato Command and Control Server.
CPU / Processore	«Central Processing Unit»/processore: unità centrale di un computer, contiene i circuiti logici necessari al funzionamento di un programma per computer.
Cryptomining	Con il mining vengono creati nuovi blocchi che si aggiungono alla blockchain. Il procedimento richiede calcoli molto complessi, pertanto viene retribuito.
Defacement	Deturpamento di pagine web.
Dispositivi NAS	Network Attached Storage (NAS): server di dati facili da configurare e gestire. In generale, un NAS è utilizzato per fornire capacità di archiviazione indipendente in una rete di computer senza grande dispendio.
Domain Name System	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).
Downloader	Programma che scarica e installa una o più istanze di malware.
ElasticSearch	Motore di ricerca sviluppato in Java sulla base di Apache Lucene.

Exploit-Kit	Kit che consente a criminali di generare programmi, script o righe di codice mediante i quali è possibile sfruttare le vulnerabilità dei sistemi di computer.
Global Positioning System (GPS)	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.
HTA di Microsoft	Applicazione HTML (acronimo: HTA): termine di Microsoft per designare i software eseguiti utilizzando Internet Explorer.
Infezione da «drive-by-download»	Infezione del computer mediante malware unicamente attraverso la consultazione di una pagina web. Le pagine web interessate contengono nella maggior parte dei casi offerte serie, ma sono state dapprima compresse allo scopo di diffondere il malware. L'infezione avviene perlopiù per il tramite dell'utilizzo di exploit che sfruttano le lacune nel sistema di sicurezza lasciate scoperte dal visitatore.
Internet delle cose	L'espressione «Internet delle cose» indica che nel mondo digitale il computer è integrato in misura crescente da «oggetti intelligenti», ossia dall'applicazione dell'intelligenza digitale agli oggetti reali.
Javascript	Un linguaggio di script orientato sugli oggetti per lo sviluppo di applicazioni. Gli JavaScripts sono elementi di programma integrati nel codice HTML, che consentono determinate funzioni nel browser di Internet. Né 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 Controls, gli JavaScripts sono eseguiti sul computer del visitatore di pagine Internet. Oltre a funzioni utili, è però anche possibile programmare funzioni nocive. Diversamente dagli ActiveX Controls, gli JavaScripts sono supportati da tutti i browser.
LTE	«Long Term Evolution» (anche «3.9G»): standard di telefonia mobile di terza generazione. Una sua estensione si chiama LTE-Advanced o 4G ed è compatibile verso il basso.
Malware	Termine generico per software che esegue funzioni nocive su un computer. Rientrano tra l'altro in questo

	gruppo i virus, vermi informatici, cavalli di Troia, nonché le Logic Bombs.
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.
mobileTAN	mobileTAN (mTAN, Mobile Transaction Number) è la procedura che include il canale di trasmissione SMS. Dopo l'invio di un ordine di bonifico compilato, il cliente dell'online banking riceve dalla banca per SMS, sul proprio cellulare, un TAN unico da utilizzare esclusivamente per la transazione in questione.
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.
PKI	Public Key Infrastructure Infrastruttura per la gestione e l'utilizzazione di certificati digitali.
Port	Una porta è la parte di un indirizzo che assegna segmenti di dati a un protocollo di rete. Questo concetto è utilizzato ad esempio in TCP, UDP e SCTP per indirizzare i protocolli ai livelli superiori del modello OSI.
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.

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.
Servizi di e-currency	Valore monetario sotto forma di credito nei confronti dell'ente emittente, salvato su un supporto dati e rilasciato dietro riscossione di una somma di denaro, il cui valore non è inferiore al valore monetario emesso e che viene accettato come mezzo di pagamento da aziende diverse dall'ente emittente.
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.
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.
SS7	Il Signaling System #7 (SS7) è un insieme di protocolli e procedure di segnalazione usati per le reti di telecomunicazione. SS7 è utilizzato nella rete telefonica pubblica in correlazione con l'ISDN, la rete fissa e la rete mobile, e all'incirca dal 2000 impiegato in misura crescente anche nelle reti VoIP.
SSH	Secure Shell Protocollo che grazie alla cifratura dei dati consente tra l'altro l'accesso sicuro (Login) a un sistema di computer accessibile per il tramite di una rete pubblica (ad es. Internet).
Take down	Take down (rimozione) è un'espressione utilizzata quando un provider ritira un sito dalla rete a causa della presenza di contenuti fraudolenti.
Top-Level-Domains	Ogni nome di dominio in Internet consta di una successione di serie di caratteri separati da un punto. La designazione 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.
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.
UDP	«User Datagram Protocol»: protocollo di rete molto semplice, senza connessione, che trasporta datagrammi della famiglia di protocolli Internet.
USB	Universal Serial Bus, Bus seriale che (per il tramite di corrispondenti interfacce) consente il raccordo di periferiche come tastiera, mouse, supporti esterni di dati, stampante ecc. Al momento del raccordo o della disgiunzione di un dispositivo USB il computer non deve essere riavviato. I nuovi dispositivi sono per lo più riconosciuti e configurati automaticamente (a dipendenza però del sistema operativo).
Verme informatico	Diversamente dai virus, i vermi informatici non necessitano di un programma ospite per diffondersi. Essi sfruttano piuttosto le lacune di sicurezza o gli errori di

	configurazione del sistema operativo o delle applicazioni per diffondersi autonomamente da un computer all'altro.
WLAN	L'abbreviazione WLAN (o Wireless Local Area Network) significa rete locale senza fili.
Zero-Day	Exploit che appare il giorno stesso in cui la lacuna di sicurezza è resa nota al pubblico.
ZIP-Datei	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.