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
www.melani.admin.ch/

SICUREZZA DELLE INFORMA-ZIONI

LA SITUAZIONE IN SVIZZERA E A LIVELLO INTERNAZIONALE

Rapporto semestrale 2017/I (gennaio – giugno)

2 NOVEMBRE 2017

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

1 Panoramica / Contenuti

2 Editoriale

Michel Buri
Vice-capo servizio informatico
Responsabile della sicurezza informatica
Ospedale del Vallese

Care lettrici, cari lettori,

il contagio a livello planetario del malware «WannaCry» il 12 maggio 2017, non sarà dimenticato tanto presto. Molte imprese, private e pubbliche, hanno subito gravi danni. Persino il servizio della sanità pubblica britannico (NHS) è stato pesantemente danneggiato.

Tutti noi ci siamo probabilmente chiesti: «*E se…?*». Siamo infatti consapevoli che è solo grazie alla fortuna se gli effetti non sono stati molto più devastanti. A livello più basilare, ognuno di noi si è sicuramente domandato se la ricerca di un equilibrio tra rischi e benefici sia sempre stata condotta nel modo giusto e se il rischio residuo sia accettabile.

Questo interrogativo rappresenta tuttora una grossa preoccupazione per gli ospedali. Infatti, la medicina del XXI secolo, maggiormente incentrata sulla partecipazione attiva del paziente nel processo di cura, fa ampiamente leva su queste tecnologie, ricorrendo a un utilizzo sempre maggiore di dispositivi e di oggetti medici connessi tra loro e alla rete. Parallelamente, un attacco del tipo «WannaCry» ci mette a confronto con sfide istituzionali importanti, basti citare l'integrità fisica del paziente o l'incapacità di garantire la continuità delle attività.

La conclusione cui sono giunti i medici autori dell'articolo pubblicato il 7 giugno 2017 nella rivista «*The New England Journal of Medicine*» offre una prima risposta alla domanda dell'accettabilità del rischio: «*We wouldn't accept being told to use outdated equipment on our patients, and our now-critical IT should be no different*»[1] (*Non accetteremmo di dover utilizzare un'apparecchiatura superata sui nostri pazienti e lo stesso vale per la nostra infrastruttura IT, attualmente critica*). Se è vero che una siringa o un farmaco scaduti non devono essere più utilizzati, neppure un'apparecchiatura sanitaria allacciata alla rete con un sistema operativo superato o privo degli ultimi aggiornamenti di sicurezza, dovrebbe essere più impiegata. Ma oggi non è così!

Questa è una delle principali sfide per il settore sanitario. Per garantire una ragionevole certezza del funzionamento di un dispositivo o di un'apparecchiatura medica allacciata alla rete durante l'intero ciclo di vita, occorre concepirne in modo diverso la sicurezza, sin dalla sua progettazione. La sicurezza informatica esige un approccio dinamico e olistico.

Per dare una risposta appropriata a una simile sfida, è necessaria una stretta collaborazione tra i diversi attori coinvolti, i responsabili: i fabbricanti, gli ospedali e l'autorità di sorveglianza Swissmedic. In questo ecosistema dedicato alla sicurezza dei dispositivi e degli oggetti connessi in campo sanitario, MELANI ha un ruolo centrale di supporto.

Vi auguro una piacevole lettura del nuovo rapporto semestrale.

Michel Buri

---

[1] R. Clarke, T. Youngstein, *Cyberattack on Britain's National Health Service – A wake-up Call for Modern Medicine*, In NEJM, giugno 2017 (stato: 31.7.2017)

3 Tema principale: WannaCry e NotPetya – software di cifratura o qualcosa di più?

Nel primo semestre del 2017 due eventi avvenuti nel settore cyber sono saliti alla ribalta delle cronache mondiali: il 12 maggio 2017 il trojan di crittografia «WannaCry» ha colpito almeno 200 000 computer in 150 Paesi diversi secondo le informazioni di Europol. Tra le vittime si citano la società spagnola di telecomunicazioni Telefonica, gli ospedali in Gran Bretagna e le ferrovie tedesche (Deutsche Bahn). In Svizzera MELANI ha identificato 204 vittime potenziali, ma rispetto all'estero non sono stati colpiti gestori di infrastrutture critiche. Il 27 giugno 2017 il malware «NotPetya» ha provocato gravi danni soprattutto in Ucraina, dove sono rimasti coinvolti, tra gli altri, l'aeroporto di Kiev, la banca centrale ucraina e la stazione di misurazione della radioattività di Chernobyl. Ma tra i bersagli si annoverano anche altri Paesi: ad esempio la Danimarca con Maersk, la più grande compagnia al mondo di trasporto marittimo di container, nonché gli Stati Uniti con il colosso farmaceutico Merck. In Svizzera è rimasta vittima di «NotPetya», tra gli altri, la società pubblicitaria Admeira. Nei prossimi capitoli sono trattate le peculiarità di questi due attacchi e le domande che sollevano.

Nel caso di attacchi dei cosiddetti «ransomware», malware che cifrano file a scopo di estorsione, i dati contenuti nel computer della vittima vengono crittografati, dopo di che è richiesto il pagamento di un riscatto per poterli ripristinare. Simili software di cifratura sono utilizzati già da anni, ma da qualche tempo sembra che sempre più criminali ricorrano a questo tipo di malware. MELANI osserva attentamente lo sviluppo in tale ambito e nei suoi precedenti rapporti semestrali ha più volte segnalato i diversi tipi e i metodi utilizzati[2]. Il 19 maggio 2016, inoltre, MELANI ha svolto una giornata di sensibilizzazione dedicata all'argomento «ransomware» con diversi partner[3]. Questi fatti dimostrano una volta di più quanto sia vulnerabile la società moderna con i suoi sistemi informatici connessi.

Raccomandazione

INFO

Pagina informativa di MELANI sui ransomware
https://www.melani.admin.ch/melani/it/home/themen/Ransomware.html

3.1 Dinamica degli eventi

In entrambi i casi il malware si è diffuso sfruttando una lacuna del protocollo SMB per la condivisione in rete di file, stampanti e server su cui sono incentrati i servizi di rete di Microsoft. Il protocollo SMB è inoltre utilizzato dai software della suite «Samba» per rendere interattivi i sistemi basati su Unix con quelli di Microsoft Windows.

Gli attacchi erano stati preceduti dalla pubblicazione di un pacchetto di strumenti di hacking chiamato «DoublePulsar» da parte del gruppo «Shadow Broker» nell'aprile del 2017. Questi

[2] https://www.melani.admin.ch/melani/it/home/themen/Ransomware.html (stato: 31.7.2017)

[3] https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/ransomwareday.html (stato: 31.7.2017)

strumenti sfruttano, tra l'altro, una vulnerabilità del suddetto protocollo SMB chiamata «Eternal Blue». Una delle risorse di «DoublePulsar» è un software che serve per installare backdoor presumibilmente sviluppato e utilizzato dalla National Security Agency (NSA). Si ritiene che «DoublePulsar» sia stato trafugato alle autorità statunitensi già nel 2016.

Nel caso di «WannaCry» è molto probabile che l'infezione si sia diffusa solo tramite dispositivi visibili in Internet con un software superato del protocollo SMB, perché sino a oggi non si hanno indicazioni di altre fonti di contaminazione, ad esempio la posta elettronica. Per «NotPetya», invece, l'aggiornamento manipolato di un programma di contabilità chiamato «MeDoc» è stato trasformato in un vettore iniziale. Le imprese attive in Ucraina devono utilizzare questo software per versare le imposte. Una volta contagiato un computer di una rete aziendale, la vulnerabilità del protocollo SMB serviva per diffondere «NotPetya» orizzontalmente nella rete. Inoltre, gli hacker hanno inserito possibilità alternative alla propagazione orizzontale. I casi esposti si distinguono dunque nel senso che con «WannaCry» i criminali hanno cercato di piazzare il loro software in modo fortuito, mentre per «NotPetya» si presume l'intenzione di prendere di mira società ucraine.

In considerazione del potenziale dei due attacchi, il pagamento dei riscatti è stato gestito con scarsa professionalità: per «NotPetya» gli hacker hanno puntato sulla comunicazione via mail. Tuttavia, il rispettivo indirizzo di posta elettronica è stato rapidamente bloccato, rendendo impossibile la comunicazione con le vittime e impedendo anche l'invio alle vittime di un codice di decodificazione. I media hanno diffuso in fretta l'informazione, pertanto il numero di coloro che hanno pagato è basso. Inoltre, in entrambi i casi, la somma di poco superiore ai 300 dollari chiesta come riscatto era relativamente modesta.

3.2 Matrice criminale o sabotaggio mirato?

Nei due casi esposti in precedenza gli esperti in materia di sicurezza hanno messo in discussione l'esistenza di una matrice puramente criminale. L' attuazione poco professionale della componente del pagamento induce a dubitare che gli interessi finanziari abbiano realmente avuto la priorità. Nell'ambito dei ransomware, l'intento di attori motivati soltanto dal denaro è quello di estorcere alle loro vittime una somma elevata nel modo più rapido ed efficiente possibile. Ecco perché proprio questa parte dell'attacco è solitamente la più sviluppata, mentre non si può dire altrettanto di «WannaCry» e «NotPetya».

Secondo gli esperti, il codice dannoso di «WannaCry» presentava analogie con il malware «Lazarus», utilizzato nell'attacco alla Banca nazionale del Bangladesh compiuto nel mese di marzo del 2016. Nel caso di «NotPetya», il vettore di diffusione mirato tramite il programma ucraino di contabilità «MeDoc» induce a ritenere che la motivazione principale degli autori dell'attacco sia stato il sabotaggio. Il fatto che operino in Ucraina e, di conseguenza, debbano utilizzare il suddetto software di contabilità spiegherebbe perché siano state colpite anche imprese al di fuori dell'Ucraina. Probabilmente non sarà mai del tutto chiarito chi si cela dietro questi due attacchi. Quanto accaduto è un esempio lampante dei vantaggi di un cyber attacco: così come spesso avviene in simili casi, anche qui non rimangono che indizi. Una prova sicura non esiste. Mentre il mondo si arrovella sulla motivazione e sull'origine dell'attacco, chi l'ha commesso può nascondersi dietro l'anonimato di Internet.

3.3 Il problema dei sistemi non aggiornati

In entrambi i casi il malware si è propagato a macchia d'olio poiché la vulnerabilità del protocollo SMB ne ha consentito la diffusione senza l'interazione degli utenti. Tuttavia, la falla di sicurezza era già conosciuta da molto tempo. Microsoft aveva pubblicato un aggiornamento sin dall'inizio di marzo del 2017. Di conseguenza, quanto accaduto con «WannaCry» o «NotPetya» non avrebbe mai dovuto infettare computer. Ma allora perché aziende rinomate sono rimaste vittime di questi attacchi? Per gli utenti privati gli aggiornamenti sono spesso installati con una funzione automatica. Ad esempio, gli aggiornamenti pubblicati di martedì dal produttore figurano su gran parte dei computer privati già il mercoledì. Nei sistemi professionali, invece, la situazione è diversa. Qui gli aggiornamenti non possono essere installati semplicemente di notte. Un aggiornamento errato può comportare il mancato funzionamento di un'applicazione critica per l'attività che si traduce in una perdita per l'azienda. Da qui deriva la necessità di svolgere test preliminari al fine di garantire che gli aggiornamenti messi a disposizione dalle società di software non abbiano ripercussioni negative sulle applicazioni cruciali. Per questo motivo, prima di ogni aggiornamento occorre valutare se il rischio di una mancata installazione supera quello di un'applicazione non funzionante. Naturalmente è anche possibile adottare soluzioni che limitino i rischi, tra l'altro l'isolamento dei sistemi in pericolo.

In determinati settori, ad esempio in quello sanitario, un aggiornamento è, spesso, pressoché impossibile. Con ogni intervento, tra cui l'installazione di un aggiornamento, le apparecchiature mediche perderebbero la certificazione, quindi anche l'omologazione. Il rischio passerebbe così dal produttore al gestore. Un aggiornamento errato su un dispositivo medico può mettere a repentaglio la vita di un paziente. È, dunque, comprensibile che gli ospedali, gli ambulatori medici, i laboratori ecc. non intendano incorrere in questo rischio. Una nuova certificazione risolverebbe il problema, tuttavia comporta costi elevati, richiede tempo e non è sempre possibile. Nel caso di «WannaCry», con la sua diffusione indiscriminata e globale, non sorprende che sia caduto nella trappola anche il settore sanitario britannico.

3.4 La responsabilità degli organi di sicurezza

Per fronteggiare adeguatamente le crescenti sfide nell'ambito della sicurezza, gli organi responsabili, come la polizia o i servizi delle attività informative, devono utilizzare sempre più spesso anche metodi elettronici, ad esempio per controllare persone d'interesse. Poiché le comunicazioni in Internet hanno luogo ormai sempre più spesso in modalità cifrata, il focus degli organi di sicurezza risiederà principalmente nel dispositivo finale utilizzati dalla persona che hanno nel mirino, così che le informazioni possano essere acquisite ancor prima di venir trasmesse in dietro cifratura. Per gli organi responsabili le lacune di sicurezza sconosciute («Zero-Day») sono perciò un mezzo insostituibile per raggiungere gli scopi prefissati. Quando i dispositivi sono aggiornati e le persone non si lasciano raggirare da metodi di Social Engineering, questa è una delle uniche possibilità, per aver accesso comunque al sistema desiderato. Tuttavia, essere a conoscenza dell'esistenza di una lacuna di sicurezza del genere e non condividere quest'informazione per trarne vantaggio, è in ogni caso in contraddizione con il processo della cosiddetta «Responsible Disclosures». Di conseguenza, l'utilizzo di questo tipo di informazioni è sempre legato a un alto grado di responsabilità e presuppone, in particolare da parte di uno Stato, una valutazione del rischio regolata, giustificabile e controllata.

Se quando uno Stato sfrutta una falla Zero-Day si può, in linea di massima, partire dal principio che persegua uno scopo o una persona precisa, ciò non è forzatamente il caso quando ad agire sono altri attori. Se simili lacune di sicurezza diventassero improvvisamente e incontrollatamente pubbliche e venissero impiegate da terzi in maniera irresponsabile, i danni provocati sarebbero superiori al valore aggiunto che un organo di sicurezza aveva originariamente atteso. È ciò che è stato dimostrato dai casi «WannaCry» e «NotPetya»: presumibilmente l'informazione inerente la vulnerabilità nel protocollo SMB, come pure gli strumenti che ne avrebbero facilitato lo sfruttamento, provengono dal portfolio dell'NSA. La falla di sicurezza e i suddetti strumenti sono stati resi pubblici dal gruppo «Shadow Broker», che già in agosto 2016 aveva reclamato la paternità del furto di informazioni, riguardanti Zero-Days, ai danni del NSA.

Se le lacune di sicurezza e il relativo exploit utilizzati da WannaCry e NotPetya dovessero effettivamente provenire dall'arsenale di un servizio d'informazione, che avrebbe perso, già nel 2016, parte delle informazioni in suo possesso a vantaggio di terzi, probabilmente, una comunicazione tempestiva a Microsoft e la conseguente messa a disposizione anticipata di un update, avrebbero potuto evitare conseguenze peggiori. A causa dell'arco di tempo incorso tra il presunto furto di dati e la pubblicazione dell'update in marzo 2017 sembra poco probabile che Microsoft sia stata avvertita tempestivamente. In questo caso, non solo, una falla di sicurezza, potenzialmente pericolosa, sarebbe stata conosciuta da tempo ma una pronta «Responsible Disclosure» nei confronti di Microsoft non avrebbe avuto luogo neanche dopo il furto di queste informazioni. In questo modo, il rischio di una pubblicazione incontrollata di una lacuna di sicurezza critica sarebbe stato messo in conto.

Esistono casi precedenti, in cui informazioni relative a vulnerabilità Zero-Day sono state rubate e successivamente sfruttate per scopi criminali: la società «Hacking Team» è rimasta vittima di un attacco da parte di hacker nel 2015. I dati sottratti sono stati pubblicati in Internet. La serie di documenti che Wikileaks ha pubblicato a partire dal 7 marzo 2017 viene invece denominata «Vault 7». Essa fa riferimento, tra le altre cose, a 24 lacune Zero-Day nel sistema operativo Android, che presumibilmente la CIA conosceva già dal 2016.

3.5 Salvaguardia dei dati: un'assicurazione sulla vita per ogni azienda

Ben pochi sanno se e quanto un'assicurazione pagherebbe in un caso simile, ma ognuno spera nell'indennizzo integrale di un eventuale danno. Ancora maggiore è dunque la frustrazione se si scopre che il danno non è coperto dalla polizza, la somma rimborsata è insufficiente oppure la polizza assicurativa non è stata pagata. Si raccomanda dunque di controllare le proprie polizze di tanto in tanto, eventualmente adeguandole al mutare della propria situazione specifica. Analogamente accade nell'ambito della messa in sicurezza dei dati.

Per un'azienda i dati memorizzati sono alla base dell'attività quotidiana, un'interruzione della quale rappresenterebbe un ostacolo alla realizzazione di un fatturato. Dei dati memorizzati fanno parte: i contatti e la corrispondenza con i clienti, gli ordini, la contabilità, il sito web con eventuali banche dati e molte altre informazioni indispensabili per l'operatività quotidiana. È dunque indubbio che questi dati debbano essere salvati regolarmente, tuttavia non è sufficiente fare affidamento esclusivamente sulla tecnica. Sarebbe opportuno testare regolarmente il funzionamento dei backup. È inoltre importante verificare periodicamente che i processi di salvataggio includano realmente tutti i dati rilevanti.

In caso di una perdita dei dati, ad esempio collegata all'attacco di trojan di crittografia, si aggiunge un altro aspetto. Di norma l'installazione dei file di backup dura diverse ore, durante le quali i dipendenti non possono lavorare. Nella migliore delle ipotesi ciò comporta una perdita in termini di guadagno ma per infrastrutture critiche come gli ospedali può avere conseguenze molto più gravi. Nel caso di «WannaCry», gli ospedali britannici hanno dovuto sospendere il servizio di pronto soccorso e dirottare i pazienti su altri ospedali.

Raccomandazione

Definite una strategia di backup!

Chiedetevi quali siano i dati da salvare, con quale frequenza e per quanto tempo i backup debbano rimanere memorizzati.

La copia di sicurezza dovrebbe essere salvata offline, ossia su un supporto esterno, ad esempio un disco rigido esterno, da scollegare dal computer subito dopo il processo di backup, in modo da impedire che un trojan di crittografia possa accedervi. In caso contrario l'attacco di un ransomware cifrerebbe probabilmente anche i dati salvati sul supporto per backup rendendoli inaccessibili.

4 La situazione a livello nazionale

4.1 Sistemi di controllo industriali (ICS)

Come esposto al capitolo 3, anche i gestori di infrastrutture critiche possono rimanere vittime di attacchi di ransomware che, tuttavia, nella maggior parte dei casi non si annidano direttamente nei sistemi di controllo industriali, bensì nei «sistemi di amministrazione». Se questi venissero danneggiati, potrebbero esserci comunque ripercussioni anche sulla produzione.

Per il momento, ransomware che prendano di mira espressamente i sistemi di controllo industriali sono emersi soltanto nei lavori di ricerca[4]. Ad esempio, l'Institute of Technology della Georgia, negli Stati Uniti, ha descritto uno scenario in cui lo sperimentale «LogicLocker» riusciva a crittografare la logica del sistema di controllo e avrebbe potuto ricattare i gestori per estorcere denaro.

In un altro caso la ditta «CRITIFENCE» ha volutamente sviluppato il prototipo di ransomware «ClearEnergy»[5] per commercializzare meglio le misure da loro sviluppate al fine di colmare la falla, precedentemente scoperta dall'azienda, nei prodotti ICS. Il malware blocca l'accesso alla logica del sistema di controllo minacciando di sovrascriverlo e rendendolo, quindi, inutilizzabile. Fortunatamente questi esempi non hanno varcato le soglie dei laboratori e non sono riusciti a penetrare negli ambienti produttivi.

Attacchi tradizionali di ransomware su dispositivi utilizzati contro il controllo remoto di sistemi ICS si sono già verificati anche in Svizzera. Ad esempio, un ransomware ha preso di mira un sistema che gestiva l'approvvigionamento di acqua. Il malware si è diffuso tramite il comando

[4] http://www.cap.gatech.edu/plcransomware.pdf (stato: 31.7.2017)

[5] http://securityaffairs.co/wordpress/57731/malware/clearenergy-ransomware-scada.html (stato: 31.7.2017)

remoto accessibile da Internet, probabilmente con un attacco di forza bruta al rispettivo server. Si è riusciti comunque a limitare i danni: grazie ai backup è stato ripristinato il sistema, che in seguito è stato ulteriormente protetto. Questo esempio dimostra bene che ogni funzione aggiuntiva (qui il comando remoto dei sistemi) richiede adeguate misure di sicurezza.

Alcune parti dei comandi centrali dei sistemi di controllo industriali sono salvate nel cloud. La ferrovia del Gornergrat[6], ad esempio, utilizza un sistema di controllo dei treni virtualizzato su cloud. In concomitanza con il progetto di mettere in circolazione treni senza conducente[7], aumenta dunque la criticità degli impianti di comando utilizzati, di conseguenza questi sistemi devono essere ben protetti.

Raccomandazione

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

Formulario d'annuncio MELANI:

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

Lista di controllo con le 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

4.2 Attacchi (DDoS, Defacements, Drive-By)

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

4.2.1 Il CERN analizza VENOM il rootkit per Linux

In data 11 gennaio il Computer Security-Team del CERN di Ginevra ha messo in guardia pubblicamente a livello mondiale dal rootkit «VENOM»[8]. Un rootkit è un software che l'hacker installa nel sistema manomesso per accedervi senza essere identificato e tenere nascosti i processi e i file che utilizza. Nel caso di VENOM, l'hacker carica il malware automaticamente sul sistema di file e le modifiche avvengono nell'arco di pochi minuti. Durante questo processo, l'orario del sistema viene alterato in modo che nei file figurino orari errati

6 https://www.siemens.com/innovation/en/home/pictures-of-the-future/mobility-and-motors/urban-mobility-gornergratbahn.html (in inglese e tedesco; stato: 31.7.2017)

7 https://www.sob.ch/medienmitteilung/news/2017/6/15/sob-treibt-automatisches-fahren-voran.html (in tedesco; stato: 31.7.2017)

8 https://security.web.cern.ch/security/venom.shtml (stato: 31.7.2017)

delle avvenute modifiche, rendendole quindi difficili da scoprire. Dove possibile, il codice dannoso viene eseguito direttamente nella memoria temporanea RAM del dispositivo infetto per non lasciare tracce nei drive. Il malware prende di mira il server di Linux e installa una backdoor sul dispositivo colpito, può eseguire comandi da remoto e modificare dati. EGI-CSIRT[9] presume che l'infezione iniziale avvenga tramite il furto dei dati d'accesso remoto per mezzo del protocollo SSH. L'attacco presenta analogie con l'intrusione nel server di chat per la rete «Freenode»[10] avvenuta nel 2014. Il rootkit puntava alla comunità degli astrofisici e non ha avuto nessun impatto sul CERN.

Raccomandazione

Dal momento che «Venom» fa sparire le sue tracce sul computer infetto, per i server è consigliabile disporre di un sistema esterno di log di memoria, in modo da rendere possibile l'analisi a posteriori anche di questi casi.

4.2.1 Messaggi di propaganda invece della temperatura dell'acqua

Le tensioni politiche si sfogano sempre più spesso attraverso i canali digitali. Se in passato le pareti degli edifici venivano tappezzate di graffiti, oggi gli attivisti infettano i siti web. Per gli hacker la deturpazione digitale ha il vantaggio di non doversi recare fisicamente sul posto bensì di poter diffondere la propria propaganda da un luogo qualunque. Questa disgiunzione dal luogo fisico comporta che eventi internazionali possano trovare risonanza anche sui siti web elvetici.

Alla fine di marzo 2017, nel corso di una dimostrazione a Berna, alcuni attivisti giravano per le strade esibendo uno striscione con la scritta «*Kill Erdogan with his own weapons*» (*Uccidete Erdogan con le sue stesse armi*). Nei giorni successivi MELANI ha registrato diversi defacement, ossia attacchi che modificano le pagine di un sito, su siti web svizzeri[11]. Ad esempio i visitatori del sito della piscina di Wülflingen non hanno trovato le informazioni relative alla temperature dell'acqua che cercavano, bensì messaggi di propaganda dei nazionalisti turchi.

9 https://wiki.egi.eu/w/images/c/ce/Report-venom.pdf (stato: 31.7.2017)

10 https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2014/october/analysis-of-the-linux-backdoor-used-in-freenode-irc-network-compromise/ (stato: 31.7.2017)

11 http://www.tagesanzeiger.ch/digital/internet/tuerkische-propaganda-auf-schweizer-badiwebsite/story/12947804 (stato: 31.7.2017)

Figura 1: Sito web della piscina di Wülflingen infettato

Il fatto che sia stata colpita proprio questa piscina e soltanto una è un puro caso. Gli hacktivisti si muovono alla ricerca di siti che presentano vulnerabilità. Piazzerebbero certamente volentieri i loro messaggi su siti molto visitati di note aziende e organizzazioni, ma nella maggior parte dei casi questi sono ben protetti, di conseguenza chi sferra l'attacco deve spesso ripiegare su siti più piccoli.

Ma la propaganda non ha mietuto vittime solo tra i siti web svizzeri. Infatti, sono stati utilizzati anche account di Twitter[12] violati per propagare messaggi. Il repertorio degli attacchi non si limitava comunque a questo: gli hacker turchi hanno rivendicato attacchi DDoS contro il sito web austriaco «oe24.at» compiuti nel mese di marzo del 2017.[13]

La propaganda politica non è l'unico motivo del defacing. Come dimostrano portali specialistici[14], spesso l'intento è cercare la notorietà o mettersi in competizione con individui che perseguono gli stessi scopi.

12 https://www.theregister.co.uk/2017/03/15/twitter_app_hack/ (stato: 31.7.2017)

13 http://www.oe24.at/oesterreich/politik/Attacke-auf-oe24-Tuerkische-Hacker-bekennen-sich/273401472 (stato: 31.7.2017)

14 http://zone-h.com/ (stato: 31.7.2017)

Raccomandazione

Gli attacchi ai sistemi di gestione dei contenuti («Content Management System», CMS) che servono per creare siti web, possono essere ridotti in misura massiccia installando subito gli aggiornamenti di sicurezza. Esiste nondimeno tutta una serie di ulteriori misure per contribuire alla sicurezza dei CMS.

DOCU

Misure per contribuire alla sicurezza dei sistemi di gestione dei contenuti (CMS)

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

4.2.2 Media online nuovamente sfruttati come canali d'infezione

Nel suo rapporto semestrale 2012/2[15] MELANI ha messo in guardia contro i rischi implicati dal sempre più frequente inserimento di contenuti di aziende terze. I portali dei media sono spesso campioni nell'includere link di filmati, pubblicità e social network. Nei suoi rapporti semestrali MELANI ha più volte[16/17] riferito di casi in cui i visitatori di questi portali sono rimasti contagiati da virus.

Nella primavera del 2017 i portali svizzeri di notizie sono stati presi ripetutamente di mira. Nel mese di marzo 20min.ch[18] ha comunicato che persone non autorizzate erano riuscite ad accedere al loro portale online per piazzare script dannosi. Un analogo incidente si è ripetuto nel mese di aprile con pctipp.ch[19]. Con uno script introdotto clandestinamente si è tentato di reindirizzare i lettori online su siti che veicolavano malware.

Per gli hacker i portali dei media sono interessanti perché contano numerosi visitatori, quindi hanno un'ampia diffusione, come ben dimostra la vasta campagna di malvertising del gruppo «AdGholas»[20]. Ricorrendo ai cosiddetti «exploit kit», venivano distribuiti malware configurati sulle vittime introducendo appositamente file malevoli.

---

15 Cfr. Rapporto semestrale MELANI 2/2012, capitolo 5.5 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2012-2.html (stato: 31.7.2017)

16 Cfr. Rapporto semestrale MELANI 2/2015, capitolo 4.3.1 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2015-2.html (stato: 31.7.2017)

17 Cfr. Rapporto semestrale MELANI 1/2016, capitolo 4.4.2 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2016-1.html (stato: 31.7.2017)

18 http://www.20min.ch/digital/news/story/Angriffsversuch-auf-20minuten-ch-vereitelt-27863282 (stato: 31.7.2017)

19 http://www.pctipp.ch/in-eigener-sache/artikel/drive-by-angriff-auf-pctipp-87549/ (stato: 31.7.2017)

20 https://www.proofpoint.com/us/threat-insight/post/massive-adgholas-malvertising-campaigns-use-steganography-and-file-whitelisting-to-hide-in-plain-sight (stato: 31.7.2017)

La guida completa e la lista di controllo possono essere scaricate dal sito www.melani.admin.ch.

DOCU

Misure per contribuire alla sicurezza dei sistemi di gestione dei contenuti (CMS)

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

Vi sono contenute anche una guida e una lista di controllo da consultare se l'attacco è già stato commesso.

DOCU

Guida alla disinfestazione dei siti web

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

4.2.3 Grazie della sua iscrizione: lo spam al momento del login

Ogni giorno sono inviati in tutto il mondo miliardi di mail indesiderate a scopo commerciale, i cosiddetti spam, ma i filtri antispam utilizzati dai provider di posta elettronica migliorano costantemente e per la maggior parte degli utenti mitigano gli effetti rendendoli quasi sempre sopportabili. All'inizio del 2017, tuttavia, MELANI ha registrato un aumento del numero di messaggi indesiderati inviati per posta elettronica che si rivolgevano a destinatari specifici. Cittadini e organizzazioni hanno dunque ricevuto molteplici messaggi indesiderati di posta elettronica contenenti la richiesta di iscriversi a diverse newsletter, forum e servizi analoghi che comportano appunto un'iscrizione. Quando, nel quadro di un attacco informatico, questo genere di servizi, viene sottoscritto in modo automatico da un apposito programma, si parla del cosiddetto «email bombing»[21].

Se i siti in questione non inviano alcuna richiesta di conferma, le vittime riceveranno automaticamente tutti i messaggi di questi innumerevoli servizi. Sebbene sia possibile disiscriversi e impostare i rispettivi filtri, in caso di diverse migliaia di registrazioni, i destinatari presi di mira possono trovarsi ad affrontare un lavoro assai gravoso.

4.3 Social engineering e phishing

Oltre a tutti gli attacchi tecnologici, hanno successo soprattutto quelli che cercano di raggirare la vittima con una storia credibile. I cosiddetti attacchi di social engineering funzionano meglio se l'utente malintenzionato riesce a raccogliere numerose informazioni concernenti la potenziale vittima. I truffatori utilizzano sia fonti accessibili a chiunque, sia informazioni pro-

---

https://www.proofpoint.com/us/threat-insight/post/adgholas-malvertising-campaign-using-astrum-ek-delivermole-ransomware (stato: 31.7.2017)

21 http://www.forbes.com/sites/leemathews/2017/05/10/secure-email-provider-attacked-with-500k-newsletter-sign-ups/ (stato: 31.7.2017)

venienti da furti di dati. I dati rubati vengono esaminati, collegati ad altri dati rubati o di pubblico dominio, preparati e rivenduti ad altri criminali. In passato chi sferrava l'attacco si accontentava, ad esempio, della lista dei contatti di un account di posta elettronica. Scriveva quindi alle potenziali vittime di trovarsi all'estero, aver perduto il cellulare e il portamonete e avere impellente bisogno di un aiuto finanziario. Oggi i criminali si prendono il tempo di esaminare meticolosamente lo scambio di e-mail di un conto manomesso alla ricerca di materiale utilizzabile, ad esempio fatture elettroniche che possono poi essere rinviate alla vittima con un numero IBAN modificato. I truffatori sono molto interessati anche alle comunicazioni con la banca. Un fatto accaduto dimostra che per le truffe sono impiegati anche dati apparentemente inutilizzabili: come base delle informazioni è stato utilizzato l'elenco dei rivenditori presenti a un'esposizione. L'attaccante contattava le aziende per iscritto ricordando loro di conoscersi da un certo evento. In quell'occasione sarebbe stato già discusso un «grosso» affare che dovrebbe essere trattato con la massima discrezione. Così poneva la necessaria base di fiducia. Infine i collaboratori venivano messi sotto pressione con la richiesta di pagare una grossa somma di denaro.

4.3.1 Phishing

Anche nel primo semestre 2017 sono stati inviati numerosi messaggi di phishing. Il contenuto delle mail non cambia molto: alcuni chiedono i dati della carta di credito per poterli «verificare», altri domandano di cliccare su un link per collegarsi a un certo sito e di inserire la password al fine di usufruire di servizi Internet. In questi messaggi di phishing sono regolarmente utilizzati, in modo illecito, loghi di aziende famose o del servizio colpito per dare alla mail una connotazione di ufficialità.

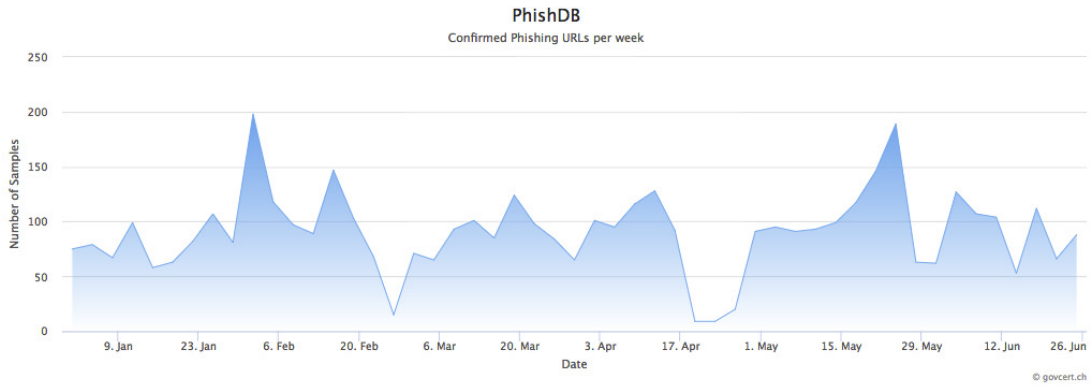


Figura 2: Siti segnalati e confermati di phishing ogni settimana su antiphishing.ch nel primo semestre 2017

Nel primo semestre del 2017 sono stati segnalati 2343 casi di inequivocabili pagine web di phishing tramite antiphishing.ch, il portale gestito da MELANI. Nella figura 2 sono raffigurate le pagine web di phishing comunicate ogni settimana il cui numero oscilla nell'arco del semestre per vari motivi: da un lato i numeri sono soggetti a fluttuazioni stagionali, poiché nei periodi delle vacanze le segnalazioni diminuiscono, dall'altro i criminali spostano periodicamente i loro attacchi da un Paese all'altro.

4.3.2 Nuovi metodi di attacco contro le aziende

Nel primo semestre del 2017 si sono moltiplicate le telefonate a potenziali aziende bersaglio nelle quali i malintenzionati si spacciavano per collaboratori di una banca. Utilizzare questo stratagemma è semplice poiché molte aziende pubblicano le proprie coordinate bancarie nel

sito web. L'informazione può essere carpita anche in anticipo da parte dei truffatori tramite una telefonata o una richiesta inviata all'azienda per e-mail.

Chi telefona finge di dover eseguire un aggiornamento nell'e-banking che dovrà poi essere testato. Per eseguire il test, tuttavia, occorrerebbe la presenza di tutti i collaboratori della divisione finanze, in particolare di quelli autorizzati alla firma nell'e-banking. Per dimostrarsi attendibili, i truffatori menzionano i nomi di alcuni collaboratori.

Durante una seconda telefonata sarà installato un tool di accesso remoto che permette ai criminali di entrare nel sistema. Essi affermano di volerne verificare il funzionamento tramite un test di pagamento e, poiché nelle aziende l'abilitazione dei pagamenti è generalmente protetta da una firma collettiva, i truffatori esortano i collaboratori autorizzati a comunicare i propri dati di accesso. In questo modo, in realtà, abilitano il pagamento. In alcuni casi, durante questo processo la vittima si trova davanti una schermata nera che le impedisce di accorgersi della truffa.

Raccomandazione

L'esempio illustra l'estrema attualità dei metodi di social engineering. Sensibilizzare i collaboratori che lavorano nelle diverse aziende è fondamentale per prevenire efficacemente questi tentativi di truffa:

- se possibile, rinunciate a pubblicare in Internet i vostri dati bancari;
- non lasciate che terzi accedano al vostro sistema;
- non installate mai i cosiddetti «remote tool» su richiesta di persone non autorizzate;
- nessuna banca vi chiederà mai di svolgere alcun tipo di test. Le banche dispongono di propri reparti che si occupano dell'IT oppure l'hanno esternalizzata. In ogni caso gli aggiornamenti di sicurezza vengono verificati prima di essere resi accessibili al pubblico.

4.3.3 La truffa del CEO – Una frode low-tech

Si parla di «CEO-Fraud» se i malviventi incaricano la contabilità o la divisione finanze di un'azienda, a nome del direttore generale, di procedere al pagamento su un loro conto (generalmente estero). Spesso la richiesta giunge da un indirizzo falsificato di posta elettronica ma sono stati constatati anche casi in cui si è operato da un account di posta elettronica autentico precedentemente manomesso. I motivi del pagamento sono diversi ma nella maggior parte dei casi si tratta di un pagamento spacciato per «urgente ed estremamente delicato» (in particolare in materia di acquisizione). Fa spesso parte di questo scenario anche un consulente o un studio legale fasullo o con un account mail manomesso. I malintenzionati sanno esattamente come esercitare pressione sui collaboratori coinvolti riferendosi a una questione dichiarata di estrema urgenza, affinché la vittima proceda al pagamento eludendo eventuali istruzioni procedurali.

Diverse statistiche, pubblicate nel primo semestre del 2017, confermano che questa forma di truffa sta vivendo una crescita esponenziale. Secondo l'Ufficio federale tedesco della polizia criminale (BKA), negli ultimi mesi la Germania ha subito danni per milioni di euro con la truffa

del CEO[22]. Nel mese di maggio di quest'anno anche l'FBI ha reso noti i dati che ne rivelano una crescita enorme. Nel caso della truffa del CEO, tra gennaio del 2015 e dicembre del 2016, è stato constatato un incremento del 2370 per cento. Secondo il rapporto, 132 Paesi hanno subito danni per miliardi[23]. Nella maggior parte dei casi il denaro rubato viene dirottato sulle banche cinesi e di Hong Kong, ma anche le banche del Regno Unito registrano somme di denaro, sempre più ingenti, estorte con questo tipo di truffa. Da molto tempo, ormai, gli attacchi di social engineering sono responsabili di una parte notevole dei danni finanziari perpetrati in Internet senza comportare un particolare dispendio a livello tecnologico.

Raccomandazione

Gli attacchi di social engineering fanno leva sulla disponibilità, sulla buona fede o sull'incertezza delle persone, ad esempio per entrare in possesso di dati confidenziali oppure indurre le vittime a svolgere determinate azioni. Tra tutte le possibilità di attacco, questa è la tecnica che ha più successo in assoluto. MELANI ha pubblicato consigli su come difendersi da simili attacchi.

Pericoli attuali: CEO-Fraud

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

Pericoli attuali: social engineering

https://www.melani.admin.ch/melani/it/home/themen/socialengineering.html

4.3.4 Falsa assistenza telefonica: perfezionamento dei metodi

Già da parecchi anni alcuni utenti svizzeri vengono contattati da truffatori, la maggior parte delle volte a nome di Microsoft, col pretesto di un problema informatico che necessita una riparazione a distanza. I truffatori cercano di spaventare le vittime facendo credere loro di avere un computer contaminato. Per esempio, chiedono loro di aprire ila visualizzazione di eventi (in inglese «Event viewer»), che elenca tutti gli eventi e le attività del computer. A seconda della tecnologia e della configurazione del computer, la lista dei messaggi di errore pubblicata nella lista degli eventi può essere molto lunga, senza che il sistema presenti il minimo problema. In seguito, i truffatori cercano di accedere al computer grazie a un software a distanza per poter procedere a delle manipolazioni e a volte chiedono un pagamento per la loro prestazione. Abbiamo già avuto l'occasione di descrivere questo fenomeno ripetutamente (la prima volta nel nostro rapporto semestrale 2011/2, cap. 3.1)[24].

Questa tecnica è ancora utilizzata ma ormai i truffatori usano anche altri metodi per contattare le vittime. In un primo esempio l'utente riceve una telefonata ma d'altra parte del filo c'è un

---

22 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/CEO_Fraud_10072017.html (stato: 31.7.2017)

23 https://www.ic3.gov/media/2017/170504.aspx#fn3 (stato: 31.7.2017)

24 Cfr. Rapporto semestrale MELANI 2/2011, capitolo 3.1 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2011-2.html (stato: 31.7.2017)

messaggio registrato che chiede di chiamare un numero per poter risolvere dei problemi informatici riscontrati sul suo computer.

Una tendenza più nociva è attiva da un po' di tempo all'estero e solo recentemente in Svizzera. L'utente che naviga in Internet vede apparire un pop-up propagato da siti Internet sospetti o da adware dannosi. Il pop-up contiene un messaggio che sembra provenire da Microsoft e che annuncia la presenza di un virus sul computer. Per evitare conseguenze dannose come il furto di dati sensibili, l'utente deve chiamare un numero di telefono. Una volta effettuata la chiamata parte il classico metodo di falsa assistenza telefonica descritto sopra. È interessante notare che i truffatori a volte ricorrono a numeri svizzeri, dai quali le chiamate sono probabilmente ridirette all'estero.

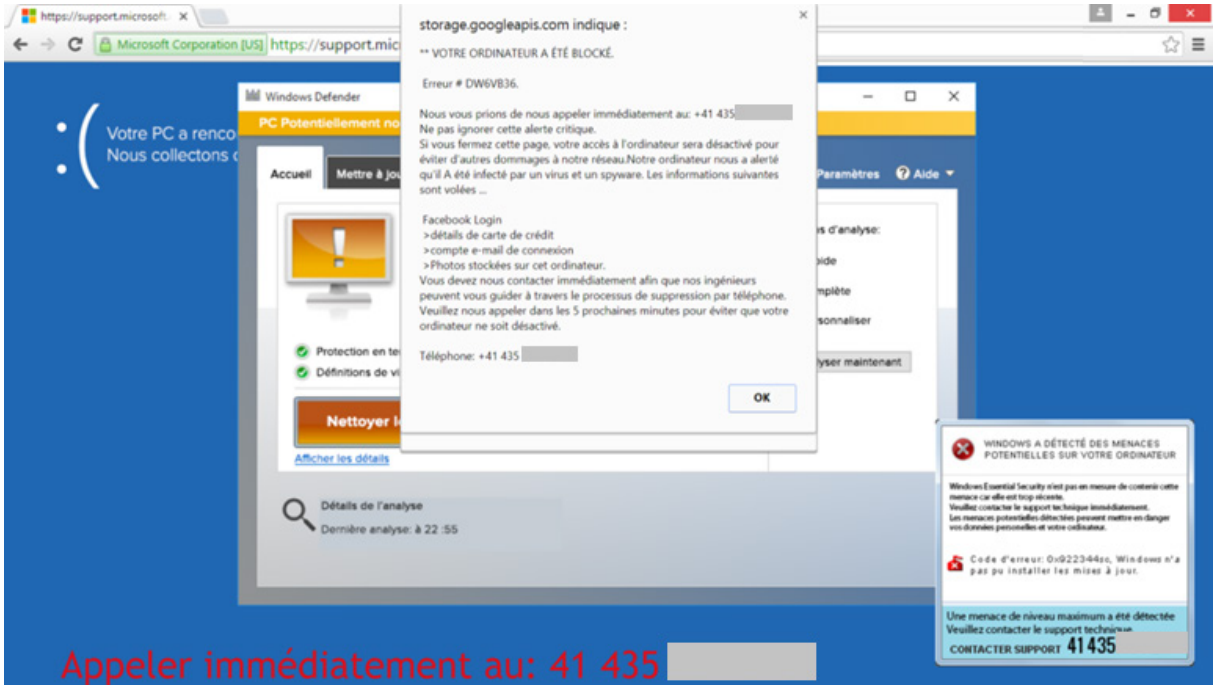


Figura 3: Esempio di pop-up. Non si tratta della barra di navigazione reale, ma di un'immagine che vuole farvi credere di essere sul sito di Microsoft.

Di fronte a questo nuovo metodo i consigli di base restano gli stessi. Occorre partire dal principio che Microsoft o altre aziende non effettuano telefonate spontaneamente per risolvere problemi informatici. Le telefonate sospette devono essere immediatamente interrotte. Nel caso in cui venga concesso un accesso a distanza ai truffatori, si raccomanda di reinstallare completamente il sistema e di cambiare la password di accesso al computer.

Se appaiono dei messaggi di allarme sotto forma di pop-up, in genere è possibile farli scomparire chiudendo la finestra del browser. Nel caso i pop-up persistano, è possibile chiudere il browser dalla finestra di gestione delle attività («task manager»). Infine, bisogna ricordare che solitamente questi pop-up sono generati da siti poco affidabili. Navigando il più possibile su siti sicuri è possibile premunirsi ampiamente.

Raccomandazione

Maggiori informazioni sul sito Microsoft:

INFO

https://blogs.technet.microsoft.com/mmpc/2017/04/03/tech-support-scams-persist-with-increasingly-crafty-techniques/

https://www.microsoft.com/en-us/safety/online-privacy/avoid-phone-scams.aspx

4.3.5 Phishing tramite la funzione «Data URL»

Da un lato i malintenzionati cercano sempre nuove strade per abbindolare gli internauti, dall'altro vogliono rendere sempre più difficile ai servizi di sicurezza la disattivazione di siti fraudolenti. Una di queste possibilità è l'abuso della cosiddetta funzione dei «Data URL» del browser per gli attacchi di phishing. In realtà il metodo non è nuovo, ma nel mese di marzo del 2017 è stato nuovamente utilizzato per questi fini. Un «Data URL» consente di inserire dati direttamente in un link come se fossero risorse esterne. Il vantaggio consiste nel fatto che così è possibile incorporare l'intero contenuto di un sito web direttamente nel link, senza doverlo scaricare da un server, come avviene di solito. La pagina non è salvata su un server, quindi non può essere disattivata neppure dai fornitori di servizi di sicurezza.

Una pagina così annidata in un link si distingue da una normale pagina web per l'URL raffigurato, che non comincia come di solito con «https://», bensì con «data:text/html» ed è molto lungo. Scegliendo abilmente la prima riga, quindi la porzione che appare nella riga dell'indirizzo del browser, un malintenzionato può comunque indurre la vittima a credere di essere indirizzato sul server di un provider di posta elettronica o di un istituto di carte di credito. A tal fine, il truffatore imposta la porzione iniziale del «Data URL», in modo che appaia soltanto il link della rispettiva azienda (cfr. figura seguente). Il resto del link molto lungo, che contiene l'intero testo sorgente della pagina, scompare nelle altre righe non visualizzate[25].

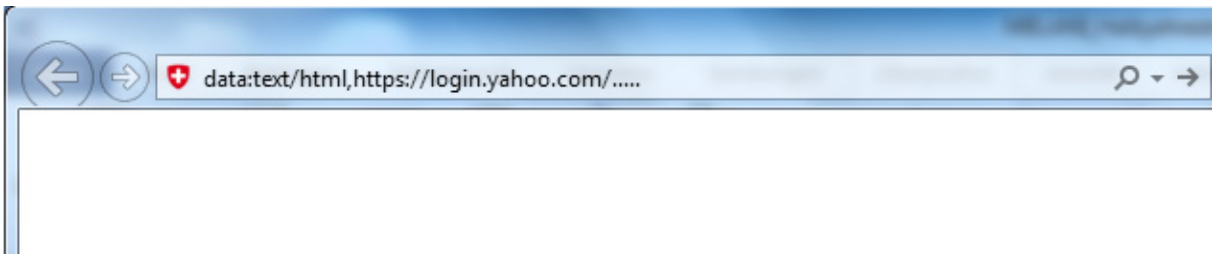


Figura 3: «Data URL» di un sito web incorporato che all'apparenza conduce alla pagina di login di Yahoo, ma in realtà è un sito creato da truffatori.

4.4 Crimeware

Il crimeware è una forma di malware che dal punto di vista criminologico rientra nel campo della criminalità informatica e giuridicamente è da collocare nell'ambito del danneggiamento

[25] https://thehackerblog.com/dataurization-of-urls-for-a-more-effective-phishing-campaign/index.html (stato: 31.7.2017)

di dati e dell'abuso di un impianto per l'elaborazione di dati. Anche nel primo semestre del 2017 sono state rilevate numerose infezioni da crimeware. Così come avvenuto negli anni passati, la maggior parte ha riguardato il malware «Downadup» (noto anche come «Conficker»), un worm che esiste già da più di otto anni e si diffonde tramite una falla di sicurezza rilevata nei sistemi operativi Windows nel 2008 e perciò riparata da lungo tempo. Al secondo e al terzo posto troviamo i malware «spambot» e «cutwail», che si sono specializzati nell'invio di spam e malware. Al quarto posto troviamo la rete bot «Mirai», resa celebre dall'attacco al fornitore di servizi Internet «Dyn» che infetta apparecchiature dell'Internet delle cose. Al nono posto si colloca il primo trojan «Dyre» che colpisce chi opera con l'e-banking.

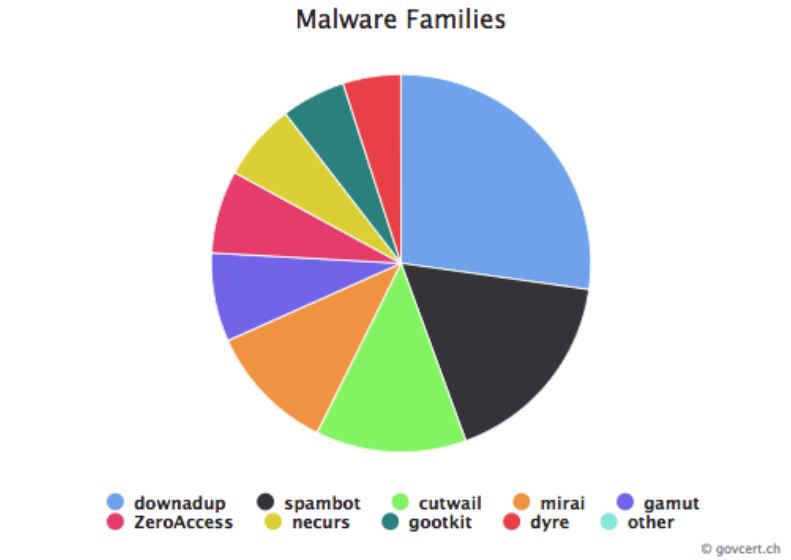
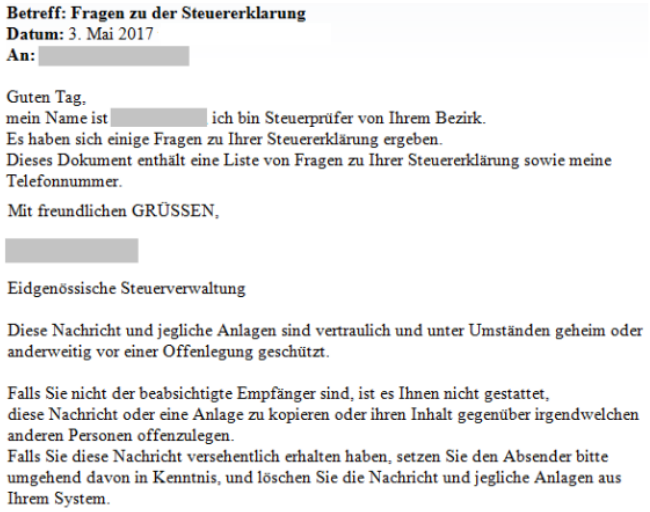


Figura 4: Distribuzione dei malware in Svizzera secondo i dati in possesso di MELANI. Il giorno di riferimento è il 30 giugno 2017. Dati aggiornati disponibili al seguente indirizzo: http://www.govcert.admin.ch/statistics/dronemap/

4.4.1 Crescente impiego abusivo di uffici federali e note aziende nell'invio di malware

I truffatori mettono vieppiù in circolazione e-mail inviandole a nome di servizi federali, per conferire ai messaggi un carattere il più possibile ufficiale e dare maggiori possibilità di successo al loro tentativo di truffa. Ad esempio, fingendo che provenissero dall'Amministrazione federale delle contribuzioni (AFC), sono state messe in circolazione e-mail che prospettavano un rimborso d'imposta, ottenibile compilando il documento allegato e contenente un software dannoso. In questi casi i mittenti delle e-mail sono falsificati.



Betreff: Fragen zu der Steuererklarung
Datum: 3. Mai 2017
An: [redacted]

Guten Tag,
mein Name ist [redacted] ich bin Steuerprüfer von Ihrem Bezirk.
Es haben sich einige Fragen zu Ihrer Steuererklärung ergeben.
Dieses Dokument enthält eine Liste von Fragen zu Ihrer Steuererklärung sowie meine Telefonnummer.

Mit freundlichen GRÜSSEN,

[redacted]

Eidgenössische Steuerverwaltung

Diese Nachricht und jegliche Anlagen sind vertraulich und unter Umständen geheim oder anderweitig vor einer Offenlegung geschützt.

Falls Sie nicht der beabsichtigte Empfänger sind, ist es Ihnen nicht gestattet, diese Nachricht oder eine Anlage zu kopieren oder ihren Inhalt gegenüber irgendwelchen anderen Personen offenzulegen.
Falls Sie diese Nachricht versehentlich erhalten haben, setzen Sie den Absender bitte umgehend davon in Kenntnis, und löschen Sie die Nachricht und jegliche Anlagen aus Ihrem System.

Figura 5: Esempio di e-mail fraudolenta inviata a nome dell'Amministrazione federale delle contribuzioni (AFC)

I truffatori utilizzano anche nomi di rinomate aziende come mittenti al fine di dare maggiore credibilità all'e-mail. Sembrano molto popolari i tentativi di consegne fittizie di pacchi da parte di DHL o della Posta Svizzera oppure di ordini di pagamento. Un altro noto esempio sono le fatture falsificate di Swisscom con le quali i truffatori hanno cercato di diffondere il malware «Dridex» nel mese di febbraio del 2017.

I truffatori utilizzano pure inviti falsificati a udienze o messaggi di posta elettronica apparentemente provenienti dalla polizia cantonale con l'intento di disorientare e indurre le vittime a cliccare un determinato link oppure ad aprire un allegato.

Conclusione

I truffatori vogliono cogliere di sorpresa gli utenti, incuriosirli o spaventarli, inducendoli ad agire in modo incauto. Nella maggior parte dei casi, però, si scopre ben presto che si tratta di una falsificazione. L'AFC, ad esempio, contatta i contribuenti solo per posta ordinaria, mai via e-mail. Le organizzazioni che hanno subito un furto d'identità sono confrontate con un numero elevato di richieste di spiegazioni in merito, quindi con un'ingente mole di lavoro.

4.4.2 Malware: la cautela è d'obbligo, indipendentemente dal sistema operativo

Anche gli utenti del sistema operativo MacOS devono prepararsi agli attacchi di malware tramite i documenti di Microsoft Office: i ricercatori attivi nel settore della sicurezza hanno scoperto documenti Word in circolazione le cui macro sono appositamente concepite per MacOS. Se l'utente apre il documento manomesso e, nonostante l'avvertenza, consente l'attivazione della funzione macro, il malware contenuto controlla se il firewall «Little Snitch» è attivo. Se non lo è, viene caricato il codice dannoso creando una backdoor sul Mac[26].

[26] https://www.digitaltrends.com/computing/macos-suffers-first-word-macro-virus/ (stato: 31.7.2017)

Altri attacchi contro MacOS distribuivano un allegato sotto forma di file .zip che avrebbe dovuto contenere la fattura dettagliata di un presunto ordine. L'obiettivo era installare il trojan bancario «Retefe» su questi computer. «Retefe» è un programma dannoso molto conosciuto in Svizzera che, tuttavia, era sinora utilizzato unicamente da chi attaccava sistemi operativi Windows.

Per scoprire il sistema operativo utilizzato da una determinata vittima e fornirgli la versione adatta del malware, i criminali inviano, in una prima fase, una e-mail non sospetta che consenta all'hacker di ottenere l'informazione automaticamente. L'e-mail contiene una piccola immagine (1x1 pixel) quasi invisibile per il destinatario. Se è scaricata (operazione che può avvenire automaticamente a dipendenza della configurazione dell'e-mail), viene instaurato un collegamento con il server dell'hacker nel quale è salvata l'immagine. Nel contempo sono automaticamente trasmesse disparate informazioni sulla configurazione del computer, tra l'altro anche quelle sul sistema operativo utilizzato. I criminali hanno così la possibilità di instaurare un collegamento tra l'indirizzo di posta elettronica e la configurazione del computer. In una fase successiva inviano una e-mail adeguata al sistema operativo corrispondente.

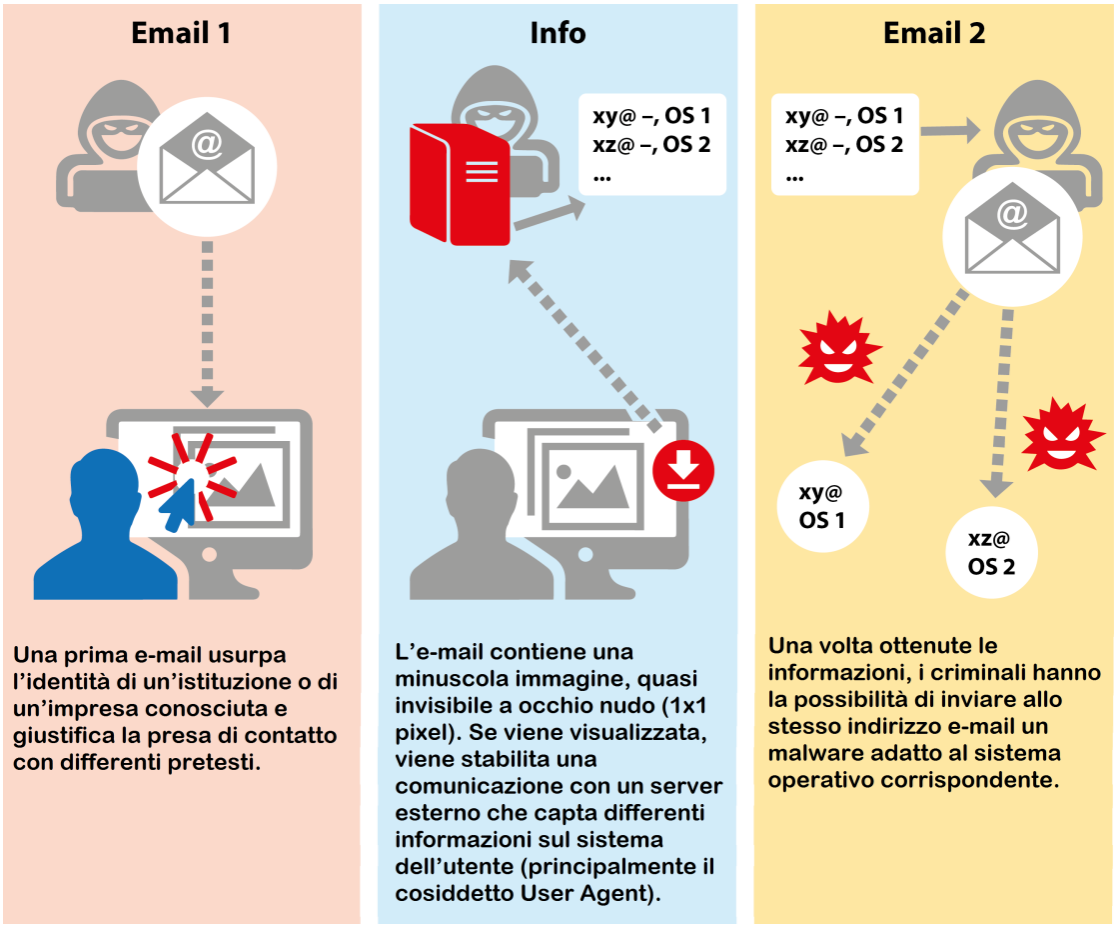


Figura 6: Rappresentazione schematica di come i truffatori risalgono al sistema operativo della vittima designata

5 La situazione a livello internazionale

5.1 Spionaggio

5.1.1 IT Managed Service Provider di nel mirino di APT10

La campagna di spionaggio informatico «APT10» di sospetta provenienza cinese, nota anche con i nomi di «menuPass», «CVNX», «StonePanda» e «POTASSIUM», prende di mira diversi settori industriali e istituzioni statali dal 2009. In particolare sembra che i criminali abbiano scelto come bersaglio le istituzioni militari di diversi Paesi e gli Stati Uniti.

Nel mese di aprile del 2017, in collaborazione con la società di revisione e consulenza PwC e il National Cyber Security Center britannico, il fornitore di servizi di sicurezza «BAE System» ha pubblicato un'indagine concernente le recenti attività di «APT10». È emerso che «APT10», all'incirca dalla seconda metà del 2016, ha condotto due campagne di attacco: la prima contro organizzazioni giapponesi; la seconda, invece, prendeva di mira alcuni importanti provider di Managed IT Service (MSP) a livello mondiale.

Nella prima campagna è stato utilizzato il nuovo trojan «ChChes» che utilizza un certificato proveniente dal grande furto di dati commesso ai danni della società «Hacking Team» nel mese di luglio del 2015[27]. Allo stato attuale delle conoscenze, «APT10» risulta l'unico gruppo di hacker che utilizzi questo specifico malware. Tramite e-mail mirate sono stati diffusi, tra l'altro, due noti tipi di malware, ossia «PlugX» e «Poison Ivy». Le mail contenevano file camuffati da documento Word con un'icona che, dopo averla cliccata, scaricava il malware. Le e-mail con finti mittenti e oggetti di attualità, ad esempio «The impact of Trump's victory to Japan», sono state inviate in modo mirato ai collaboratori di aziende farmaceutiche giapponesi e a una succursale statunitense di una società giapponese[28] due giorni dopo le presidenziali americane.

Gli MSP presi di mira nella seconda campagna supportano grandi organizzazioni nella gestione dell'infrastruttura IT. Sono dunque un obiettivo interessante, poiché possiedono i diritti d'accesso diretto ai sistemi e ai dati dei loro clienti. Presumibilmente gli MSP non erano il vero obiettivo, ma servivano unicamente a procurarsi l'accesso alle reti di numerose grandi aziende. Anche questo dimostra chiaramente l'importanza di scegliere i propri partner in modo accurato, in particolare quando la sicurezza è affidata a imprese esterne.

Gli MSP sono stati attaccati, tra l'altro, dallo strumento di cyber spionaggio «PlugX», utilizzato da diversi gruppi. Viene utilizzato pure «RedLeaves», un virus backdoor di recente creazione.

Tuttavia, «APT10» non soltanto attacca con nuovi strumenti, ma nel periodo in questione è stata notevolmente ampliata l'infrastruttura di comando e controllo, lasciando intuire che il gruppo opera con una grande professionalità e dispone di ingenti risorse finanziarie. Inoltre, anche lo spettro delle potenziali vittime è stato notevolmente ampliato: gli attacchi non si limi-

---

[27] Cfr. Rapporto semestrale 2/2015, cap. 5.1.1 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2-2015.html (stato: 31.7.2017)

[28] https://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/ (stato: 31.7.2017)

tano più al settore della difesa statunitense o a quello della tecnologia e delle telecomunicazioni, ma prendono di mira anche diversi altri comparti industriali in tutto il mondo. Sono stati colpiti sistemi in Gran Bretagna, negli Stati Uniti, in India, Giappone e altri Paesi.

5.1.2 Due fratelli spiano 16 000 persone

Il cyber spionaggio e il furto di dati sensibili di personaggi di spicco nel mondo politico sono diventati molto popolari dall'attacco sferrato al Comitato nazionale democratico negli Stati Uniti (cfr. capitolo 6.2). Anche la classe politica italiana, a suo modo, è stata vittima di un episodio simile. Dietro all'attacco in questione però, non si nascondeva un presunto governo straniero intenzionato a influenzare le sorti del Paese, bensì una coppia di fratelli, Giulio e Francesca Maria Occhionero, arrestati il 10 gennaio scorso.

Il malware utilizzato, un file Win32 eseguibile, portatile e nascosto, è stato creato da loro stessi. Per quanto sia stato sviluppato da criminali inesperti, che non si preoccupavano della loro sicurezza, è rimasto nell'ombra per quasi tre anni e ha spiato 16 000 persone. L'attacco è andato a monte quando il responsabile della sicurezza dell'ENAV (Ente nazionale di assistenza al volo) si è rivolto alla polizia postale e delle comunicazioni italiana a causa di un'e-mail sospetta che diffondeva il malware. I presunti colpevoli e sviluppatori del malware avevano lasciato tracce nella registrazione degli indirizzi IP e nel furto di dati. La polizia è così riuscita a risalire ai nomi dei responsabili. Il sospetto ha poi trovato conferma poiché i due fratelli comunicavano tramite WhatsApp, quando ancora la comunicazione non era cifrata.

La campagna era indirizzata contro rappresentanti del governo e dell'economia. Vittime famose sono state Matteo Renzi, ex presidente del Consiglio dei ministri, Mario Draghi, presidente della Banca centrale europea, nonché personaggi di spicco del Vaticano. Sono stati attaccati anche i membri di una loggia massonica. La società di sicurezza informatica Trendmicro stima che in questo modo i fratelli siano riusciti a sottrarre circa 87 gigabyte di dati sensibili. I dati, provenienti dal settore finanziario, avrebbero potuto essere utilizzati a proprio vantaggio dai due autori dell'attacco, poiché erano titolari della società di consulenza finanziaria «Westland Securities». Rimane ancora da chiarire se e a chi avrebbero dovuto essere vendute le informazioni trafugate dagli account di politici.

5.1.3 Un top manager di Kaspersky arrestato in Russia con l'accusa di alto tradimento

Le attività online possono essere pericolose. Questa affermazione piuttosto generica non vale solo per le potenziali vittime o i criminali, perché talvolta anche i ricercatori nel settore della sicurezza informatica corrono rischi se si occupano di informazioni concernenti la sicurezza di determinati Paesi. Lo può confermare Ruslan Stoyanov, responsabile della «Computer Incidents Investigation» presso la società di sicurezza informatica Kaspersky, arrestato alla fine del 2016 con l'accusa di alto tradimento. La nota azienda ha preso le distanze dall'accaduto dichiarando che «il dipendente era stato arrestato a causa di fatti precedenti al suo impiego presso Kaspersky»[29]. Le autorità russe non hanno rilasciato ulteriori commenti in merito all'arresto, ma apparentemente a Stoyanov è stato rimproverato di avere rivelato informazioni segrete ad aziende americane, tra l'altro alla società di servizi informatici «Verisign», che a sua volta avrebbe trasmesso le informazioni ai servizi segreti statunitensi. Lo

[29] http://www.forbes.com/sites/thomasbrewster/2017/01/25/russia-kaspersky-treason-arrest/#1ce5f9174a68 (stato: 31.7.2017)

stesso reato viene attribuito a Sergei Mikhailov, vicecapo della divisione cyber dei servizi segreti russi FSB, e a un altro collaboratore, Dmitry Dokuchayev. Il vicedirettore di «Verisign» ha smentito che i rapporti consegnati alle autorità governative o ad altri clienti potessero contenere segreti di Stato, ma non si è pronunciato concretamente sul caso Stoyanov.

5.1.4 APT32: spionaggio dal Vietnam?

Qualche volta le campagne di spionaggio provengono anche da regioni poco coinvolte in questi fatti. È il caso, ad esempio, del gruppo «OceanLotus», scoperto da «SkyEye Labs» nel 2014, ma salito alla ribalta delle cronache solo di recente, grazie a una ricerca condotta dalla società di sicurezza «FireEye». Da allora è chiamato «APT32». Gli hacker operano probabilmente già dal 2013 e le loro azioni sembrano essere allineate congli interessi del Vietnam. Gli attacchi hanno preso di mira non solo diverse aziende che avevano interessi commerciali in Vietnam, il settore sanitario, alcuni media vietnamiti e governi stranieri, soprattutto quello cinese, ma anche dissidenti e attivisti. «FireEye» ha constatato dodici attacchi massicci.

«APT32» lavora con pacchetti di software dannosi, che vengono associati a strumenti commercialmente reperibili. In base ai bersagli mirati si presume che fosse coinvolta un'organizzazione statale, tuttavia il governo vietnamita ha dichiarato di non essere a conoscenza delle attività condotte da «OceanLotus».

Nei recenti attacchi il gruppo «APT32» ha utilizzato documenti di Microsoft contenenti macro dannose e inviati alle vittime tramite e-mail. Gli attacchi erano rivolti a una succursale vietnamita di una società di consulenza operante su scala mondiale, contro gli aderenti alla diaspora vietnamita in Australia, contro gli impiegati del governo filippino e le succursali vietnamite di due produttori di beni di consumo nelle Filippine e negli Stati Uniti. Gli hacker hanno utilizzato semplici tecniche di social engineering per convincere le vittime ad attivare le macro.

5.1.5 Abuso di programmi di sorveglianza commerciali

«Pegasus» è un sofisticato programma di spionaggio (spyware), appositamente ideato per i telefoni cellulari e in grado di infiltrarsi nei sistemi iOS e Android. È stato sviluppato dalla NSO, azienda israeliana di sistemi di sorveglianza, ed è venduto esclusivamente a istituzioni statali per la lotta al terrorismo e alla criminalità. «Pegasus» consente di sorvegliare tutte le attività di un dispositivo mobile. Si è però consolidato il sospetto che, in alcuni casi, lo spyware della NSO, sia stato sfruttato per particolari interessi commerciali e non per gli scopi previsti. Già nel mese di agosto del 2016 le imprese di sicurezza «Citizen Lab» e «Lookout Security»[30] avevano pubblicato la storia di Ahmed Mansoor, un noto attivista per i diritti umani proveniente dagli Emirati Arabi Uniti, rimasto vittima di questo programma di spionaggio. Sembra che in Messico il software sia stato utilizzato in due diverse operazioni.

Tra luglio e agosto del 2016 «Pegasus» ha preso di mira un importante scienziato del Mexican National Institute for Public Health (INSP) e i direttori di due ONG messicane, impegnati nella lotta al sovrappeso. Le tre personalità oggetto dell'attacco erano favorevoli alla cosiddetta «Soda Tax», una misura introdotta nel 2014 e intesa a limitare il consumo di bevande zuccherate. L'imposta ha portato, come sperato, a una flessione delle vendite di questi pro-

[30] https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/ (stato: 31.7.2017)

dotti, il che ha comprensibilmente generato insoddisfazione nel settore dei generi alimentari. Nel mese di giugno del 2017 «Citizen Lab» ha pubblicato un articolo in cui si affermava che era in atto un tentativo di attaccare con malware giornalisti, avvocati e attivisti impegnati nella lotta per i diritti umani o nelle indagini contro la corruzione delle autorità governative messicane[31]. I tentativi di infezione con lo spyware sono avvenuti in gran parte nel mese di agosto del 2015 nonché tra aprile e luglio del 2016, quando si sono moltiplicate le accuse rivolte al presidente e al governo del Paese. In entrambi i casi si è trattato di attacchi mirati, diffusi tramite SMS. Ricorrendo a tecniche di social engineering, gli hacker hanno tentato di indurre i destinatari a cliccare un link dietro il quale si celava un programma di spionaggio. Se la persona presa di mira non cadeva nella trappola, le vittime predestinate diventavano i familiari. Ad esempio, la moglie di un attivista contro la corruzione ha ricevuto un sms contenente un link a presunte prove fotografiche che il marito la tradiva.

5.2 Furto di dati

Dopo le sospette fughe di dati nel corso del 2016, tra cui il mezzo miliardo di dati di utenti di «Yahoo»[32] o gli oltre cento milioni di dati di accesso alla rete di contatti professionali «LinkedIn»[33], anche all'inizio del nuovo anno sono emerse segnalazioni di dati personali sottratti. Al capitolo 6.3 sono inoltre illustrate le modifiche apportate alla legislazione europea nell'ambito della «EU general data protection regulation (GDPR)», che implicherà anche una diversa gestione di questo tipo di eventi.

5.2.1 Pubblicati per errore i profili degli elettori del Partito repubblicano americano

Durante la campagna elettorale del 2016 negli Stati Uniti, il Partito repubblicano aveva incaricato alcune società di raccogliere informazioni sui potenziali elettori. Apparentemente queste società non hanno preso troppo sul serio la messa in sicurezza dei server sui quali erano salvati i dati. I ricercatori dell'azienda «Upgard»[34] hanno trovato i dati raccolti senza alcuna protezione su un server gestito dalla società «Deep Root Analytics» di Amazon Cloud, dove erano conservati e accessibili a chiunque 1,1 terabyte di dati raccolti da questa società e da altre due aziende partner. Tra le informazioni personali si annoveravano nomi, date di nascita, indirizzi, numeri di telefono, dettagli sull'iscrizione all'albo elettorale e appartenenze a etnie e comunità religiose elaborate dalle società di marketing e riguardanti oltre 198 milioni di elettori americani, ossia praticamente l'intero elettorato degli Stati Uniti. «Deep Root Analy-

---

31 https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/ (stato: 31.7.2017)

32 Cfr. Rapporto semestrale MELANI 1/2016, capitolo 5.2.1 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2016-1.html (stato: 31.7.2017)

33 Cfr. Rapporto semestrale MELANI 2/2015, capitolo 5.2.2 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2015-2.html (stato: 31.7.2017)

34 https://www.upguard.com/breaches/the-rnc-files?utm_campaign=RNC%20Files&utm_source=upguard_home&utm_medium=breakingnewsbanner (stato: 31.7.2017)

tics» ha dichiarato al giornale «The Intercept[35]» che la fuga di dati è dovuta a un errore commesso nella configurazione dei diritti di accesso.

5.2.2 Protezione da DDoS, ma diffusione di contenuti confidenziali

La società «Cloudflare» è diventata famosa grazie alla sua protezione contro gli attacchi di DDoS. Tuttavia, a causa di una configurazione errata del software del server, sono stati distribuiti contenuti sensibili di pagine web di terzi ai visitatori di altri clienti. Tavis Ormandy, ricercatore in materia di sicurezza informatica presso «Google Project Zero», si è accorto che per diversi mesi, aprendo le pagine web, inserite nella rete «Content Delivery Network Cloudflare»[36], oltre alle pagine web consultate erano pubblicate anche informazioni segrete di altri clienti. L'errore è stato battezzato «Cloudbleed» ispirandosi al bug SSL «Heartbleed» diffusosi sui social media.

Ormandy è noto per occuparsi soprattutto di aziende che promettono di proteggere dai pericoli di Internet. Cloudflare ha dichiarato di non avere indicazioni che, oltre al ricercatore di Google, altre persone abbiano scoperto l'errore. Rimane il rischio che siano tuttora accessibili a utenti non autorizzati i dati contenuti nelle cache dei motori di ricerca e dei servizi per il web che hanno indicizzato le pagine web.

5.2.3 La fuga di dati personali mina la fiducia nell'indiana E-ID

Per rendere più trasparenti i flussi di denaro nel Paese, l'India vuole creare incentivi per ridurre i pagamenti in contanti e aumentare quelli con le carte. A questo scopo, otto anni fa è stato varato il progetto «Aadhaar» per la registrazione online dell'identità dei cittadini. Esso gestisce la base per la banca dati dei numeri di identificazione univoci (UID) utilizzati per autenticare e autorizzare i pagamenti con le carte.

L'indiano «Center for Internet and Society (CIS)»[37] ha reso noto che sono stati sottratti 135 milioni di dati relativi alle carte e collegati a 100 milioni di conti bancari. La fuga di dati non è imputabile alla banca dati di «Aadhaar». Il problema riguarda almeno quattro progetti governativi che integravano i dati di «Aadhaar» con informazioni proprie.

Quanto accaduto è un ottimo esempio per illustrare i rischi collegati all'utilizzo di codici identificativi univoci in rete che sarebbe imperativo limitare il più possibile. Una piccola negligenza compiuta da uno dei partner può causare gravi danni alla sfera privata degli utenti e minare a lungo la fiducia in questo progetto.

---

35 https://theintercept.com/2017/06/19/republican-data-mining-firm-exposed-personal-information-for-virtually-every-american-voter/ (stato: 31.7.2017)

36 Una «Content Distribution Network» è una rete di server presenti in varie regioni e collegati tramite Internet che consente di consegnare contenuti, in particolare file multimediali di grandi dimensioni.

37 http://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1 (stato: 31.7.2017)

5.3 Sistemi industriali di controllo (ICS)

Il presente capitolo si occupa di quanto emerso in riferimento al malware responsabile nel 2016, per la seconda volta, di un'interruzione nell'erogazione di energia elettrica in Ucraina[38]. Ma tra le vittime del primo semestre 2017 si annoverano anche i televisori, le sirene d'allarme, le videocamere di sorveglianza e le porte delle camere di albergo che sono da includere tra i «sistemi di controllo industriali».

Anche tra i gestori dei sistemi di controllo industriali vengono continuamente alla luce software dannosi. Uno studio del progetto «MIMICS (Malware in Modern Industrial Control Systems)»[39] della società di cybersicurezza «Dragos», attiva nell'ambito degli ICS, giunge alla conclusione che i gestori dei sistemi di controllo industriali devono lottare con gli stessi tipi di malware che colpiscono le altre aziende. Un puro trojan bancario che agisce a livello dell'e-banking può fare poco in un sistema di controllo, mentre un ransomware può rendere l'apparecchiatura o l'intero sistema inutilizzabile se sono crittografati dati necessari per il suo funzionamento. Ad esempio, recentemente sono stati colpiti da trojan di crittografia televisori smart[40] o videocamere di sorveglianza[41] a Washington DC. Ha provocato grandi danni anche il malware «Brickerbot»[42/43], che ha creato dei seri disagi nell'Internet delle cose paralizzando i dispositivi vulnerabili connessi. Tutti questi attacchi sono sicuramente gravi per gli utenti coinvolti, ma non sono miravano espressamente a perturbare il funzionamento dei sistemi di controllo.

5.3.1 Industroyer/CrashOverride – Il malware comunica autonomamente con una sottostazione

Dopo i ripetuti resoconti dei fatti[44/45] avvenuti all'inizio di quest'anno, è tornata la calma sul fronte del presunto cyber attacco sferrato nel mese di dicembre del 2016 alla rete di distribuzione dell'energia elettrica nella zona a nord di Kiev. I ricercatori attivi nell'ambito della sicurezza si sono nel frattempo impegnati assiduamente per risalire alle cause del blackout. Il 12 giugno le agenzie di servizi per la sicurezza «ESET» e «Dragos», società specializzate nella sicurezza delle informazioni per i sistemi di controllo industriali, hanno pubblicato congiuntamente i risultati dei tipi di malware esaminati, che sono stati battezzati «Industroyer»[46] e

---

38 Cfr. Rapporto semestrale MELANI 2/2016, capitolo 5.3.1 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-2.html (stato: 31.7.2017)

39 https://dragos.com/blog/mimics/ (stato: 31.7.2017)

40 https://www.heise.de/security/meldung/Erpresser-Botschaft-in-Dauerschleife-Smart-TV-von-LG-mit-Ransomware-infiziert-3584043.html (stato: 31.7.2017)

41 www.theregister.co.uk/2017/01/30/ransomware_killed_70_of_washington_dc_cctv_ahead_of_inauguration/ (stato: 31.7.2017)

42 https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-102-01A (stato: 31.7.2017)

43 http://www.zdnet.com/article/homeland-security-warns-of-brickerbot-malware-that-destroys-unsecured-internet-connected-devices/ (stato: 31.7.2017)

44 http://www.bbc.com/news/technology-38573074 (stato: 31.7.2017)

45 https://nakedsecurity.sophos.com/2017/01/16/ukraine-power-outages-the-work-of-cyberattackers-warn-experts/ (stato: 31.7.2017)

46 https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ (stato: 31.7.2017)

«CrashOverride»[47]. «CrashOverride» è una piattaforma espressamente progettata per sabotare le reti elettriche. Dopo «Stuxnet», «Havex» e «Blackenergy 2», è solo il quarto malware ideato appositamente per sabotare i sistemi industriali di controllo. Oltre a «Stuxnet», «CrashOverride» è addirittura appena il secondo malware in grado di influenzare autonomamente il processo fisico. Come illustra la Figura 7, l'applicazione «launcher» consente di eseguire quattro moduli diversi per influenzare la comunicazione tra protocolli industriali, spesso presenti nell'esercizio delle reti elettriche. La piattaforma è strutturata in modo modulare, nell'intento di integrare altri protocolli per obiettivi futuri con un dispendio ragionevole. «Dragos» denomina il responsabile del malware «ELECTRUM» e, secondo i suoi analisti, sarebbe collegato al gruppo «Sandworm». A quest'ultimo vengono imputati, da parte di diverse agenzie di servizi per la sicurezza[48], gli attacchi alla rete elettrica in Ucraina negli anni 2015 e 2016.

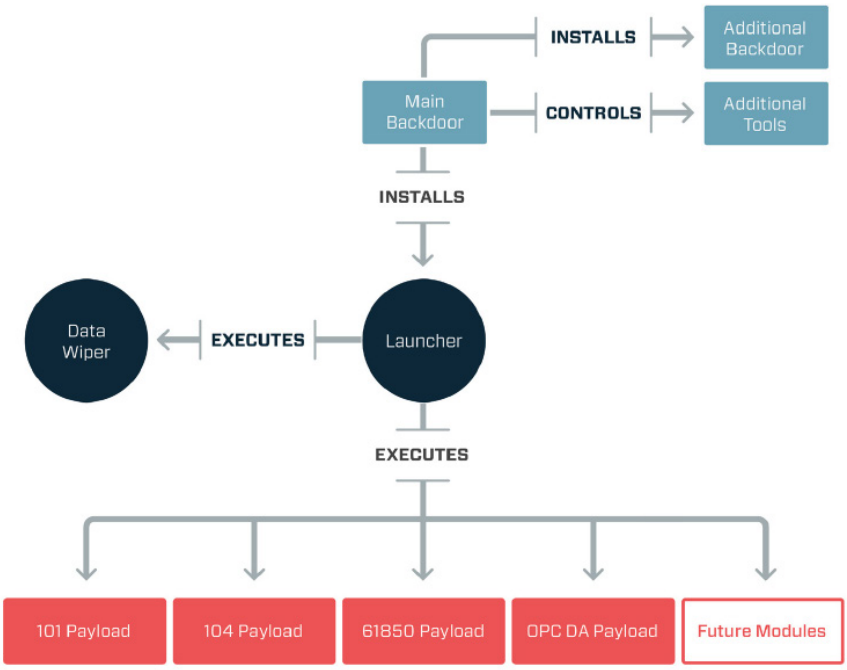


Figura 7: Struttura schematica e interazione dei moduli «Crashoverride» (*https://dragos.com/blog/crashoverride/)*

5.3.2 Gli hacker delle onde radio fanno suonare le sirene di allarme a Dallas a mezzanotte

In Svizzera, ogni primo mercoledì di febbraio a mezzogiorno, viene condotto il tradizionale test delle sirene, per accertare il funzionamento del sistema di allerta della popolazione in caso di catastrofe. Le sirene scattate a Dallas poco prima della mezzanotte del 7 aprile 2017 e che hanno suonato ininterrottamente per 95 minuti senza che ci fossero uragani in arrivo non sono in alcun modo riconducibili a un test. Inizialmente si era ipotizzato un attacco ai sistemi delle forze di pronto intervento della città texana, ma ben presto le autorità hanno comunicato che le reti non erano state violate. Il falso allarme è dovuto al fatto che le sirene sono comandate da segnali radio trasmessi dal servizio meteorologico nazionale in caso di

[47] https://dragos.com/blog/crashoverride/ (stato: 31.7.2017)
[48] https://www.wired.com/story/russian-hackers-attack-ukraine/ (stato: 31.7.2017)

calamità naturali. Tuttavia, nel caso delle sirene meno moderne questi segnali radio non sono particolarmente protetti né crittografati, bensì vengono trasmessi apertamente. Gli apparecchi che possono trasmettere queste onde radio, cosiddetti «Software Defined Radios (SDR)», diventano sempre più accessibili, in quanto sempre meno costosi. Praticamente chiunque può utilizzare simili dispositivi, dunque si trattava solo di una questione di tempo perché si verificassero degli abusi. L'hacker ha dovuto semplicemente provare tutti i possibili comandi sulla rispettiva frequenza. Il successo del metodo può essere confermato dalle martoriate orecchie degli abitanti di Dallas.

5.3.3 Castello sotto assedio

Molti alberghi hanno abolito le classiche chiavi e consegnano ai clienti una tessera sulla quale è memorizzato il codice di apertura della rispettiva camera. I vantaggi sono evidenti. Oltre alla maggiore maneggevolezza, in caso di smarrimento della tessera basta revocare il vecchio codice e attribuirne alla porta uno nuovo. Il fatto che questo vantaggio tangibile abbia anche un rovescio della medaglia lo ha constatato a proprie spese il Romantik Seehotel Jägerwirt in Austria. Proprio nel fine settimana dell'apertura, con l'albergo al completo, le porte delle camere non hanno più potuto essere aperte per colpa dell'infezione di un ransomware[49]. Oltre ai sistemi di contabilità e dei pagamenti, è stato crittografato anche il server delle carte magnetiche. In tal modo era impossibile sbloccare le porte delle camere e riprogrammare le carte. In questa situazione disperata l'hotel ha pagato quasi 1500 euro di riscatto in bitcoin. I ricattatori hanno quindi decifrato i dispositivi infetti, ma hanno cercato di lasciare aperta una backdoor nei sistemi, dopo di che l'hotel ha sostituito una parte delle apparecchiature e ha protetto meglio la rete, nella speranza di impedire una nuova infezione. Dopo la sgradevole esperienza con il sistema delle chiavi elettroniche, la struttura ha intenzione di tornare alle chiavi tradizionali al momento della prossima ristrutturazione.

Conclusione / Raccomandazione

La crescente computerizzazione e interconnessione di qualsiasi oggetto d'uso quotidiano (Internet delle cose) offre un gran numero di nuove e interessanti funzioni e comodità. Al tempo stesso, però, non si devono trascurare i rischi connessi. Le nuove opportunità celano sempre nuovi pericoli di cui è bene tenere conto già in fase di sviluppo (security by design).

DOCU

Liste di controllo e guide: misure di protezione dei sistemi di controllo industriali (ICS)

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

[49] https://www.thelocal.at/20170128/hotel-ransomed-by-hackers-as-guests-locked-in-rooms/ (stato: 31.7.2017)

5.4 Attacchi (DDoS, Defacement, Drive-By)

5.4.1 Le reti di istituti finanziari dirottate per sette minuti

Alla fine di aprile del 2017 il traffico di rete di diversi fornitori di servizi finanziari, tra cui anche quello delle società di carte di credito «Visa» e «Mastercard», è stato dirottato per quasi sette minuti sui router di una società russa di telecomunicazioni. Purtroppo non sono infrequenti le anomalie nel cosiddetto «Border Gateway Protokoll (BGP)». BGP regola il traffico tra le diverse porzioni di rete e stabilisce quale pacchetto di dati debba essere instradato sui diversi provider. In questo caso, tuttavia, colpisce che il comando errato della società russa di telecomunicazioni «Rostelecom» abbia riguardato esclusivamente blocchi di indirizzi di fornitori di servizi finanziari e aziende per la sicurezza informatica. È possibile che, nel periodo del dirottamento, il traffico di rete sia stato analizzato e, nel peggiore dei casi, addirittura modificato. Non è ancora emerso che cosa abbia causato l'errore nella configurazione. In particolare, non si è riusciti a chiarire se il problema sia dovuto a un fattore tecnico o umano oppure proprio all'attacco di hacker[50].

In un altro caso, che ha interessato gran parte della rete di una banca brasiliana, il traffico di rete è stato completamente convogliato altrove per cinque ore. Gli hacker sono riusciti a manomettere il gestore DNS della banca, quindi a spacciarsi per i gestori dell'infrastruttura della banca agli occhi della maggior parte degli aderenti alla rete. In questo modo è stato possibile spiare le operazioni, prelevare i dati di accesso e infettare i clienti con malware[51].

5.4.2 Infezione mirata tramite il sito web dell'autorità di vigilanza finanziaria polacca

All'inizio di febbraio del 2017 è stato reso noto che su diversi computer di numerose banche polacche era stato individuato un software dannoso. Si ritiene che il vettore dell'infezione sia il sito web del KNF, l'autorità di vigilanza finanziaria polacca, che gli hacker avevano contaminato con una cosiddetta infezione drive-by. A questo scopo uno dei file locali JavaScript era stato modificato in modo da scaricare un altro file JavaScript esterno che ha trasmesso il malware[52]. Era dunque sufficiente navigare nel sito per infettare i computer dei visitatori. Dal momento che diverse persone dell'ambiente finanziario si rivolgono all'autorità di vigilanza finanziaria, l'hacker potrebbe aver attuato un attacco molto mirato. Il malware ha quindi cercato di instaurare un collegamento con server stranieri. Secondo il portale «BadCyber», in alcuni casi chi ha sferrato l'attacco è riuscito a ottenere il controllo di computer nelle infrastrutture bancarie.[53].

È emerso che gli istituti finanziari polacchi erano solo una parte delle vittime predestinate. Infatti è stata individuata un'infezione dello stesso tipo anche nel sito web dell'autorità messicana di vigilanza sulle banche e sulle borse. L'exploit-kit era configurato in modo tale da in-

---

50 https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic/ (stato: 31.7.2017)

51 https://www.wired.com/2017/04/hackers-hijacked-banks-entire-online-operation/ (stato: 31.7.2017)

52 https://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/ (stato: 31.7.2017)

53 https://www.theregister.co.uk/2017/02/06/polish_banks_hit_by_malware_sent_through_hacked_financial_regulator/ (stato: 31.7.2017)

fettare solo gli utenti che visitavano la pagina con uno dei 150 indirizzi IP predefiniti. I 150 indirizzi IP potevano essere attribuiti a 104 organizzazioni situate in 31 Paesi diversi. Gran parte di queste aziende sono banche, una quota minore riguarda le società di telecomunicazioni e Internet. Allo stato attuale non risultano colpite organizzazioni svizzere. Gli attacchi risalgono almeno al mese di ottobre del 2016.

«Ratankba»[54], un malware sinora sconosciuto, dopo essersi messo in contatto con il server di controllo scaricava uno strumento di hacking associato a «Lazarus». Il gruppo «Lazarus» è messo in relazione con attacchi sferrati contro obiettivi americani e sudcoreani a partire dal 2009. A «Lazarus» è inoltre attribuito l'attacco contro la Banca nazionale del Bangladesh nel 2016[55]. Altri analisti di «Kaspersky» dimostrano che del gruppo «Lazarus» fa parte uno sottogruppo specializzato negli attacchi al sistema finanziario. Il gruppo è apparso in passato anche con il nome di «BlueNorof». L'ostinazione e la perseveranza dei responsabili faranno sì che il mercato finanziario internazionale sarà preso di mira anche in futuro.

5.4.3 La botnet mette in circolazione voci sulla manipolazione del mercato

«Necurs» è una classica botnet per l'invio di e-mail di spam ed è nota per la distribuzione su vasta scala del ransomware «Locky» e del trojan bancario «Dridex». Secondo le statistiche di MELANI, «Necurs» occupa il settimo posto nella classifica dei programmi dannosi più diffusi in Svizzera[56]. Nel periodo in rassegna è stato osservato come i truffatori abbiano utilizzato l'invio di spam per manipolare le quotazioni di borsa delle «penny stock», azioni scambiate a meno di cinque dollari e non quotate sulle Borse nazionali[57]. In un'ondata di spam inviati da «Necurs» è stata annunciata una presunta acquisizione sul mercato dei droni. I destinatari, che non sono riusciti a resistere alla tentazione di un guadagno facile, hanno quindi acquistato i titoli dell'azienda in questione facendone decollare il prezzo sul mercato. Gli hacker avevano acquistato quote di partecipazione nell'azienda già prima di inviare gli spam, poi le hanno vendute con un guadagno considerevole dopo l'impennata dei prezzi da essi indotta. L'esempio di questo attacco, cosiddetto «Pump and Dump», mostra come i criminali informatici cerchino sempre nuove strade per utilizzare in modo finanziariamente proficuo l'infrastruttura di cui dispongono e le loro capacità, comunque senza rinunciare a percorrere strade già note.

5.4.4 Banca dati dei pazienti nelle mani di ricattatori

Dopo i danni causati da «WannaCry» alle strutture ospedaliere soprattutto in Gran Bretagna, un altro fatto accaduto in una clinica lituana specializzata in chirurgia plastica dimostra quanto siano sensibili i dati dei pazienti e l'importanza di proteggerli adeguatamente. Gli hacker, che si sono battezzati «Tsar Team», hanno ricattato i clienti della clinica in oltre 60 Paesi minacciando di pubblicare loro fotografie che avevano precedentemente sottratto alla banca dati della clinica. Per provare la serietà delle loro intenzioni, hanno pubblicato in rete 25 000

---

54 https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0 (stato: 31.7.2017)

55 Cfr. il Rapporto semestrale MELANI 1/2016, capitolo 5.4.1 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2016-1.html

56 Cfr. capitolo 4

57 http://blog.talosintelligence.com/2017/03/necurs-diversifies.html (stato: 31.7.2017)

di queste foto[58]. I ricattatori, prima di contattare i clienti singolarmente pretendendo tra 50 e 2000 euro, hanno tentato di vendere alla clinica l'intera banca dati in cambio di mezzo milione di sterline in bitcoin, ma la clinica non ha ceduto alla richiesta. Non è noto il numero dei clienti che hanno pagato il riscatto ai ricattatori. Il nome «Tsar Team» emerge anche in rapporto con «Sofacy», ma sinora il legame non è stato confermato. È presumibile che gli hacker utilizzino la notorietà del gruppo di spionaggio soltanto per intimorire le vittime.

5.4.5 SS7, un vecchio standard per l'autenticazione nell'e-banking

Per poter accedere in modo sicuro a servizi Internet come l'e-banking viene utilizzato, oltre alla password, almeno un altro meccanismo di autenticazione che, idealmente, transita su un secondo canale di comunicazione indipendente. Molti offerenti ricorrono agli SMS sui telefoni cellulari. Ma oggi la maggior parte di questi apparecchi è costituita da piccoli computer che, in quanto tali, possono essere infettati da malware in grado, in particolare, di intercettare i messaggi trasmettendoli ai truffatori. Inoltre, le operazioni bancarie sono spesso effettuate direttamente tramite smartphone, pertanto il login e la seconda autenticazione avvengono sullo stesso dispositivo. Viene così a mancare la sicurezza supplementare che dovrebbe essere garantita dall'autenticazione inviata per SMS. Nel suo ultimo rapporto semestrale MELANI si è già occupata di questa problematica, causata dall'impiego di SMS come secondo fattore di autenticazione[59].

All'inizio di marzo del 2017 un gruppo di criminali ha attivamente utilizzato un'ulteriore possibilità di intercettare gli SMS inviati dalla banca per l'autenticazione. Come confermato dall'operatore tedesco di telefonia mobile «O_2» alla «Süddeutsche Zeitung», da anni era sfruttata una nota vulnerabilità nel protocollo SS7 per consentire transazioni fraudolente su conti bancari tedeschi[60]. A tal fine i criminali avevano manipolato una funzione nei protocolli SS7 che serve a consentire il roaming internazionale. Al difuori dei confini nazionali un telefono cellulare può agganciarsi a una rete estera, l'operatore della rete contattata lo segnala poi alla rete dell'abbonato nel suo Paese, che trasmette l'SMS alla rete straniera. Questo processo può essere simulato senza che il telefono cellulare si trovi all'estero: gli SMS saranno allora deviati verso operatori di rete all'estero finendo nelle mani dei truffatori. Ciò è possibile perché il protocollo SS7, alla base delle comunicazioni tra diversi operatori, è stato originariamente ideato come un sistema aperto, fondato sulla fiducia tra tutti gli operatori di telefonia mobile. Con il crescente numero di operatori in tutto il mondo non è più da escludere che alcune aziende non si attengano alle regole e, in determinate circostanze, possano tollerare attività fraudolente oppure collaborino con truffatori.

---

58 https://www.theguardian.com/technology/2017/may/31/hackers-publish-private-photos-cosmetic-surgery-clinic-bitcoin-ransom-payments?CMP=twt_gu (stato: 31.7.2017)

59 Cfr. Rapporto semestrale MELANI 2/2016, capitolo 6.2 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2016-2.html (stato: 31.7.2017)

60 https://www.theregister.co.uk/2017/05/03/hackers_fire_up_ss7_flaw/ (stato: 31.7.2017)

Conclusione

In alcuni Paesi la barriera di accesso per gli utenti di rete di dubbia serietà si è notevolmente abbassata. Nel contempo, non tutti gli operatori di telefonia mobile svolgono controlli di plausibilità. Questo problema viene tematizzato regolarmente a partire dal 2014. Tuttavia, per eliminare l'autenticazione tramite SMS a livello di rete occorrono particolari conoscenze specialistiche. I gruppi criminali organizzati e gli attori statali dispongono comunque già delle necessarie capacità. Per compiere una truffa nell'e-banking, la contemporanea infezione dei computer e degli smartphone degli utenti rimane senz'altro il metodo più diffuso e redditizio. Già solo per questo gli offerenti di servizi web passeranno relativamente presto a metodi alternativi di autenticazione.

5.5 Misure preventive

Oltre alla sensibilizzazione degli utenti, la misura preventiva più efficace contro la criminalità su Internet consiste nell'arrestare i cyber criminali. In molti pensano che sia difficile o addirittura impossibile identificare gli autori e arrestarli, ma anche in questo campo si possono conseguire vittorie.

5.5.1 «Mirai» manda in tilt Deutsche Telekom: un arresto

Nell'ultimo rapporto semestrale si è ampiamente parlato della botnet «Mirai»[61], un malware che colpisce il sistema operativo Linux, utilizzato soprattutto in apparecchiature dell'Internet delle cose. Il 27 novembre 2016 un attacco perpetrato con questo malware ha tagliato fuori dalla rete 900 000 clienti di «Deutsche Telekom». L'attacco è stato possibile grazie all'utilizzo di una nuova versione del malware che, sfruttando un errore di programmazione nei router delle reti domestiche di «Deutsche Telekom», ha provocato un crash invece di infettarla.

Nel frattempo è stato arrestato a Londra un hacker liberiano, responsabile di uno di questi attacchi. Le sue dichiarazioni dimostrano chiaramente la pluridimensionalità e la complessità che si celano dietro un simile atto. Secondo l'arrestato, una società liberiana di telecomunicazioni gli ha chiesto di sabotare i suoi concorrenti. Per attuare un attacco DDoS, ha quindi modificato il codice dannoso disponibile della botnet «Mirai» aggiungendo una nuova routine di attacco che può sfruttare la funzione di manutenzione in remoto di determinati router. Apparentemente è stata proprio questa nuova funzione a causare il crash dei router di «Deutsche Telekom». L'arrestato ha anche promosso il noleggio della sua botnet in Internet. Davanti al giudice ha tuttavia affermato che si sarebbe trattato soltanto di una manovra diversiva da parte del suo effettivo committente, da cui l'hacker sperava di essere assunto. In realtà, nel mese di gennaio del 2017 è stato attaccato il provider liberiano «Lonestar Cell», il che ha provocato una parziale interruzione della ricezione sulla rete mobile e un sovraccarico del cavo sottomarino verso l'Africa.

Il tribunale tedesco si è occupato esclusivamente dell'attacco contro «Deutsche Telekom», quindi ha condannato l'hacker ad appena un anno e otto mesi di detenzione con la condizionale. Ma l'autore dell'attacco non è rimasto a piede libero, bensì è stato incarcerato in vista

[61] Cfr. Rapporto semestrale MELANI 2/2016, cap. 3 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/halbjahresbericht-2016-2.html (stato: 31.7.2017)

dell'estradizione. Le autorità britanniche lo accusano infatti di ben altro: oltre al summenzionato attacco contro «Lonestar Cell», è sospettato anche di aver estorto somme milionarie a grandi banche britanniche.

5.5.2 Arrestati i colpevoli di contrabbando di dati dei clienti di Apple

La polizia cinese ha arrestato oltre venti collaboratori di aziende partner di Apple, accusati di avere rubato dati dei clienti della società produttrice di iPhone rivendendoli poi sul mercato nero[62]. I dipendenti, gran parte dei quali addetti alla vendita e al marketing, hanno attinto informazioni su utenti di iPhone e iPad dalle banche dati. Questi dati contenevano, tra l'altro, i nomi, i numeri di cellulare e le ID di Apple. Gli autori del furto hanno poi offerto i dati a prezzi compresi tra 1.50 e 26.50 dollari per ogni serie di dati ad acquirenti interessati che operavano nella clandestinità digitale. Sino al momento dell'arresto sono riusciti a guadagnare oltre sette milioni di dollari dalla vendita. Questi attacchi commessi da insider mettono in chiara luce la necessità di attuare non solo misure preventive di protezione contro i criminali al di fuori della propria organizzazione, ma anche processi e sistemi interni in grado di individuare gli attacchi in corso al fine di proteggere i propri dati.

Un buon primo passo per non rimanere vittime di questi attacchi o di altri simili è consultare il promemoria MELANI sulla sicurezza informatica per le PMI.

DOCU

Promemoria sulla sicurezza informatica 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

INFO

Portale della Confederazione per le piccole e medie imprese

https://www.kmu.admin.ch/kmu/it/home.html

6 Tendenze e prospettive

6.1 Il ruolo delle assicurazioni nel settore della cyber sicurezza

Secondo l'Ordinanza concernente le esigenze tecniche per i veicoli stradali (OETV) un dispositivo deve impedire che le porte «si aprano involontariamente», ma un dispositivo di chiusura a chiave non è un requisito espressamente richiesto per un veicolo stradale. In linea di massima non sono necessari neppure i sistemi di allarme per veicoli ma, se vengono utilizzati, l'OETV descrive piuttosto dettagliatamente quali esigenze debbano soddisfare.

62 https://www.tripwire.com/state-of-security/latest-security-news/apple-employees-detained-selling-user-data-chinese-black-market/ (stato: 31.7.2017)

Anche se un'auto senza serratura potesse essere omologata come veicolo stradale, a nessuno verrebbe in mente di togliere la serratura di serie montata sulla macchina, da un lato perché ben pochi sono interessati a facilitare il lavoro dei ladri e, dall'altro, perché in caso di furto l'assicurazione non pagherebbe.

Esistono numerosi altri esempi, in cui le assicurazioni esigono di fatto l'osservanza di standard di sicurezza mediante le condizioni applicate o i premi calcolati. Per le opere d'arte, ad esempio, alcune assicurazioni non calcolano il premio semplicemente sulla base del valore del quadro, ma vi fanno confluire altri fattori, tra cui le misure adottate per proteggerlo. Se rispondono alle miglior prassi («best practices») attualmente in uso in questo settore, il cliente paga un premio inferiore.

Il settore della cyber sicurezza è molto dinamico e ciò che ieri era considerato ancora all'avanguardia oggi è già superato. La formulazione di standard minimi di sicurezza diventa così un compito continuo e in evoluzione. In vista del diffuso impiego delle tecnologie dell'informazione e della telecomunicazione, gli standard di sicurezza nel settore cyber devono essere flessibili e adeguarsi all'autentica finalità. Il processo di regolamentazione governativo necessita però normalmente di un lasso di tempo piuttosto lungo.

Nel loro settore le assicurazioni sono relativamente libere di adeguarsi in fretta agli sviluppi e ai cambiamenti e di esigere dai loro clienti misure di sicurezza basate sulle miglior prassi attualmente in uso. Gli assicuratori coprono dunque anche le misure che non sono tipicamente assoggettate a norme. Di conseguenza, l'espansione dell'attività delle assicurazioni cyber offre non solo un'opportunità economica ma, a livello più generale, anche la possibilità di migliorare la cultura della sicurezza e, quindi, la sicurezza di fondo nel cyberspazio.

In ogni caso non si può puntare tutto sul fatto che, prima o poi, il comparto assicurativo risolverà il problema degli standard di sicurezza nel settore. Le autorità specializzate possono fungere da supporto, ad esempio elaborando prescrizioni basate su principi nel loro campo d'applicazione che il comparto assicurativo può utilizzare come filo conduttore. Ai fini del vero e proprio calcolo dei rischi, i servizi statali possono contribuire con le loro conoscenze in materia di minacce e sviluppi nel settore cyber. E, non da ultimo, anche qui esiste l'eventualità di un «terremoto del secolo» che, considerando le perdite teoricamente esorbitanti, farebbe precipitare nel baratro ogni assicurazione, quindi rende di fatto impossibile assicurare alcuni cyber-rischi. Trovare una soluzione al problema, ad esempio ispirandosi alla garanzia statale per i danni causati da un terremoto a partire da una determinata somma, è una sfida per lo Stato e per il comparto assicurativo. Ma, in caso di successo, le assicurazioni riusciranno a elaborare previsioni certe, quindi avranno anche la possibilità di impostare in modo proattivo la loro attività con polizze contro i cyber-rischi. In ultima istanza, grazie all'assunzione dei rischi e alle regole per ridurli, risulteranno vincenti non solo il comparto assicurativo, ma anche l'economia, la società e lo Stato.

6.2 I politici, un obiettivo amato dai manipolatori informatici

Il cyber attacco sferrato contro il Comitato nazionale democratico (DNC) negli Stati Uniti, attribuito dall'agenzia di sicurezza «Crowdstrike» alle operazioni di spionaggio «Cozy Bear» e «Fancy Bear»[63], è stato il primo di una lunga serie di attacchi informatici ai danni di espo-

[63] Cfr. Rapporto semestrale MELANI 2/2016

nenti del mondo politico. Gli attacchi hanno dimostrato che la pubblicazione di notizie riservate riesce sicuramente a influenzare l'opinione pubblica. Secondo un blog curato da «The Intercept»[64], si rafforza l'ipotesi che l'intenzione reale dei criminali informatici fosse di manovrare l'esito presidenziali americane. La volontà di favorire il proprio candidato danneggiando la concorrenza emerge anche nel fenomeno delle cosiddette «fake news» (notizie false), messe sempre più spesso in circolazione durante le campagne elettorali.

Per proteggere lo Stato, la società e le istituzioni democratiche, limitarsi ad adottare misure tecniche presso le reti governative e aziendali non è sufficiente. Si constata, infatti, che sempre più account privati di importanti personalità, persone politicamente attive e, in particolare, rappresentanti eletti dal popolo diventano bersagli di attacchi, sia per cercare materiale compromettente sia per diffondere affermazioni diffamatorie o manipolatrici.

Seguendo l'esempio di altri Paesi, tra cui la Germania e la Gran Bretagna, MELANI ha dunque approntato un elenco di misure di sicurezza sotto forma di infocard per aiutare i parlamentari elvetici a tutelarsi. Naturalmente le raccomandazioni sono adatte anche a chi non è un esponente politico.

6.2.1 Attacchi ai programmi elettorali

I cyber attacchi messi a segno in occasione delle elezioni presidenziali negli Stati Uniti non hanno preso di mira soltanto gli account di posta elettronica dei rappresentanti del Comitato nazionale democratico. Secondo il sito web «The Intercept», anche un'azienda che produce apparecchiature per verificare le schede elettorali è stata hackerata[65]

Inoltre, si sospetta che siano state inviate mail a oltre 100 funzionari addetti all'osservazione dei risultati elettorali. Le mail, che contenevano un malware, erano furbescamente congeniate perché si rivolgevano a collaboratori ignari di organizzazioni governative locali e sembravano provenire da un dipendente di una società che fornisce servizi nell'ambito del voto elettronico e dei software elettorali. A tale scopo, l'account della società era stato manomesso in precedenza. Tra il 31 ottobre e il 1° novembre 2016 è stata inviata un'e-mail a 122 destinatari con un documento Word contenente un trojan. La NSA, l'Agenzia di sicurezza nazionale statunitense, è rimasta tuttavia vaga sul risultato di questi attacchi, sull'eventuale successo delle mail malevoli e sui possibili dati carpiti o, addirittura, manipolati.

È dunque legittimo chiedersi fino a che punto i programmi di voto elettronico siano realmente sicuri. Gli Stati che li utilizzano dovrebbero essere consapevoli della criticità di queste infrastrutture e riflettere sui processi che ne garantiscano la migliore salvaguardia possibile. Se il rischio è ritenuto eccessivo, deve essere valutata la possibilità di adottare soluzioni estreme, ad esempio rinunciando a questi programmi, come hanno fatto la Germania e la Gran Bretagna.

---

https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/halbjahresbericht-2016-2.html (stato: 31.7.2017)

64 https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/ (stato: 31.7.2017)

65 https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/ (stato: 31.7.2017)

6.2.2 Honeypot: una strategia contro le infiltrazioni

Nel mese di dicembre del 2016 le e-mail dei collaboratori del candidato allo presidenziali francesi e leader di «En Marche!» sono diventate il bersaglio di una campagna di spear-phishing. La NSA ha inoltre scoperto un tentativo di penetrare l'infrastruttura francese e il 5 maggio 2017 ha messo in guardia le autorità competenti. Non è stata una sorpresa che gli attacchi si siano intensificati verso la fine della campagna elettorale. I fatti avvenuti durante la campagna per le elezioni presidenziali negli Stati Uniti e la consapevolezza di non poter offrire una protezione a tutto campo ha indotto il team di cyber security di «En Marche!» a prevenire. Con una strategia di «cyber blurring» sono stati creati falsi account di posta elettronica che fungessero da «honeypot» o esca per gli hacker. Ogni account falso è stato riempito di documenti ad hoc per disturbare il lavoro degli hacker che, se volevano estrarre i dati, dovevano prima verificare l'autenticità dei documenti. Ma gli hacker non hanno svolto questa cernita e hanno pubblicato circa 9 gigabyte di dati, quindi anche i documenti realizzati ad hoc. Inizialmente i dati sono stati diffusi dal sito web statunitense «Pastebin», poi da «4Chan» e «WikiLeaks». Nonostante il tentativo di screditare il candidato alla presidenza Macron con notizie come quella relativa a un suo conto corrente segreto alle Bahamas, la strategia ha avuto successo. Il fatto che i dati pubblicati risultassero in parte falsi e neppure particolarmente scabrosi ha impedito che la campagna di Macron fosse eccessivamente compromessa.

La qualità delle e-mail, utilizzate per l'attacco è stato giudicato generalmente buono. Poco prima della fine della campagna, ad esempio, sono emerse e-mail che sembravano provenire dal «Digital Director» di Emmanuel Macron. Nei messaggi veniva chiesto ai destinatari di scaricare un file allegato per proteggersi contro gli attacchi informatici. Tuttavia l'attacco non è stato molto professionale, inoltre gli hacker hanno lasciato tracce. Ad esempio, i documenti creati o modificati contenevano nomi di utenti russi, oppure erano elaborati con una versione di Microsoft ottenibile solo in Russia. Anche nell'infrastruttura di comando e controllo (C&C) sono emersi indizi che all'origine degli attacchi vi fosse il gruppo di hacker «Sofacy»[66], considerato responsabile anche degli attacchi contro la campagna di Hillary Clinton.

6.2.3 Prese di mira anche Germania e Gran Bretagna

Come dichiarato dall'Ufficio federale tedesco per la sicurezza informatica (BSI), alla fine di giugno del 2017 gli account privati di posta elettronica di esponenti del mondo economico e di dipendenti delle amministrazioni pubbliche sono stati quasi sommersi di ondate di phishing.[67] I tentativi di attacco si sono concentrati sugli account Yahoo e Gmail. L'esame dell'infrastruttura degli hacker ha rivelato analogie con le campagne descritte ai capitoli 6.2.1 e 6.2.2 condotte negli Stati Uniti contro il Comitato nazionale democratico e in Francia.

Venerdì 23 giugno 2017 anche il Parlamento britannico è stato bersaglio di un cyber attacco. Si sospetta che siano stati hackerati gli account di circa 90 parlamentari. Alla base potrebbero esservi password troppo banali, non conformi alle prescrizioni. Dopo aver manomesso gli account di posta elettronica, i cyber criminali hanno bloccato gli accessi remoti per impedire ai legittimi titolari dell'account di impostare password più sicure.

---

66 https://www.nytimes.com/2017/04/24/world/europe/macron-russian-hacking.html?mcubz=0 (stato: 31.7.2017)

67 http://www.zdnet.de/88302365/bsi-warnt-vor-phishing-angriffen-auf-funktionstraeger/?inf_by=59a97d93681db8d9688b45bf (stato: 31.7.2017)

Raccomandazione

Le amministrazioni e le aziende possono proteggere solo le proprie reti e infrastrutture. I dispositivi mobili, gli indirizzi di posta elettronica e altre infrastrutture IT utilizzate privatamente dai collaboratori esulano dalla loro sfera di influenza. Gli attacchi sferrati alle reti private hanno dunque maggiori opportunità di successo e non è possibile escludere che, di conseguenza, siano indirettamente infettate anche reti governative. Il BSI ha pubblicato una serie di linee guida destinate alla prevenzione che si rivolgono ai funzionari delle amministrazioni pubbliche o ai manager di società finanziarie, ma possono rivelarsi utili anche per i privati. MELANI raccomanda in particolare le seguenti misure, fondate sulle linee guida del BSI:

- non inviare e-mail di lavoro dagli account privati di posta elettronica;
- crittografare i messaggi classificati come confidenziali;
- creare un processo di autenticazione a due fattori;
- la password dovrebbe essere immediatamente cambiata al minimo sospetto che l'account di posta elettronica possa essere stato violato.

MELANI ha sviluppato un elenco di misure di sicurezza sotto forma di infocard a disposizione dei membri del Parlamento svizzero.

L'Infocard per i parlamentari può essere scaricata dal sito web di MELANI:

https://www.melani.admin.ch/melani/it/home/dokumentation/Infokarten.html

6.3 Il nuovo regolamento generale sulla protezione dei dati dell'UE e le ripercussioni sulla Svizzera

Il regolamento generale sulla protezione dei dati dell'Unione europea (EU-RGDP/EU GDPR) consente di uniformare il trattamento dei dati personali nell'Unione europea da parte di imprese private e organismi pubblici. Il regolamento, che sostituisce la direttiva 95/46/CE del 1995, è entrato in vigore il 24 maggio 2016 e dovrà essere applicato da tutti gli Stati membri dopo un periodo transitorio di due anni a decorrere dal 25 maggio 2018.

Nella convinzione che il futuro digitale dell'Europa possa essere fondato solo sulla fiducia, con il suo regolamento generale sulla protezione dei dati l'Unione europea persegue tre obiettivi: armonizzare la legislazione in materia di protezione dei dati a livello europeo, rafforzare il mercato interno garantendo le stesse condizioni economiche in tutta l'Unione e modernizzare la protezione dei dati sulla scia dell'evoluzione tecnologica, ma salvaguardando la tutela dei diritti fondamentali.

In sintesi, le principali modifiche apportate con le nuove disposizioni sono: diritto all'oblio; trattamento dei dati solo previo consenso esplicito dell'interessato; diritto alla portabilità dei dati (a un altro fornitore di servizi); diritto dell'interessato di essere informato in caso di violazione della protezione dei propri dati e, infine, un intervento più duro in caso di violazioni del regolamento. Quest'ultimo significa che a un'azienda possono essere inflitte sanzioni amministrative pecuniarie fino al 4 per cento del fatturato annuo totale mondiale dell'esercizio precedente.

A differenza della direttiva 95/46/CE, che gli Stati membri dovevano trasporre nelle rispettive legislazioni nazionali, il regolamento generale sulla protezione dei dati si applica direttamente in tutti gli Stati membri dal mese di maggio del 2018. Ciò implica che, in linea di principio, gli Stati membri non hanno la facoltà di indebolire o rafforzare la protezione dei dati sancita dal regolamento con normative a carattere nazionale. Tuttavia, il regolamento contiene oltre 70 clausole di apertura che consentono agli Stati membri di disciplinare a livello nazionale alcuni aspetti della protezione dei dati.

Le numerose deroghe e la conseguente incertezza del diritto sollevano dunque critiche in diversi ambiti nei confronti del regolamento generale sulla protezione dei dati. Secondo queste voci critiche, il regolamento mancherebbe l'obiettivo originario dell'armonizzazione, sarebbe troppo astratto, ammetterebbe troppe deroghe e porterebbe dunque inevitabilmente a difficoltà di interpretazione e contraddizioni rispetto al diritto tuttora vigente a livello nazionale. In particolare la Germania mette in guardia contro il rischio di un alleggerimento del diritto tedesco in materia di protezione dei dati. Infine, le norme sarebbero troppo neutre rispetto alla tecnologia esistente, pertanto non rilevano sufficientemente i rischi della tecnologia dell'informazione.

Il regolamento generale sulla protezione dei dati è applicabile non solo nell'Unione europea, ma anche in Paesi terzi, tra cui la Svizzera. Di conseguenza riguarda pure tutte le imprese elvetiche con o senza una succursale nell'Unione europea che offrono beni o servizi a persone che si trovano nell'UE (questa condizione dovrebbe essere soddisfatta già con le offerte su un sito web o un e-shop), o che trattano dati personali appartenenti a cittadini di Paesi membri dell'UE, oppure che analizzano il comportamento di persone che si trovano nell'UE.

Raccomandazione

MELANI consiglia di adeguare tempestivamente i processi di elaborazione delle informazioni, la tenuta dei dati e la salvaguardia delle informazioni ai nuovi requisiti di legge. Si prevede inoltre che l'introduzione dell'ordinanza e l'emanazione di elevate sanzioni pecuniarie in caso di violazione della protezione dei dati non solo riguarderà le imprese, ma indurrà pure i criminali a ideare nuovi metodi estorsivi.

La revisione totale della legge federale sulla protezione dei dati è in corso, pertanto è ipotizzabile che la legge riveduta riprenderà diverse novità introdotte dal regolamento generale dell'UE sulla protezione dei dati.

7 Politica, ricerca, policy

7.1 Svizzera: interventi parlamentari

Affare	Numero	Titolo	Depositato da	Depositato il	CN/CS	Dip.	Stato delle deliberazioni e link
Mo.	17.3508	Creazione di un centro di competenza per la cyber-sicurezza a livello di Confederazione	Joachim Eder	15.06.2017	CS	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173508
Mo.	17.3507	Un comando Cyber Defence con cybertruppe per l'esercito svizzero	Josef Dittli	15.06.2017	CS	DDPS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173507
Mo.	17.3497	Ufficio centrale di contatto e di coordinamento per la lotta contro la criminalità informatica organizzata e attiva sul piano internazionale	Marcel Dobler	15.06.2017	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173497
Mo.	17.3496	Protezione di base obbligatoria per le infrastrutture elettriche critiche	Edith Graf-Litscher	15.06.2017	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173496
Mo.	17.3475	Obbligo di segnalazione di gravi incidenti legati alla sicurezza delle infrastrutture critiche	Edith Graf-Litscher	15.06.2017	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173475
Po.	17.3433	Cybersicurezza nel settore della sanità	Bea Heim	13.06.2017	CN	DFI	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173433
Mo.	17.3199	Ampliare le competenze nell'ambito della cyberdifesa	Franz Grüter	16.03.2017	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173199
Ip.	17.3136	Cybersicurezza nel settore della sanità	Bea Heim	15.03.2017	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173136
Ip.	17.3103	Le sfide poste dal settore cyber. Quali saranno i prossimi passi nel nostro Paese?	Joachim Eder	13.03.2017	CS	DDPS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173103

Mo.	17.3591	Neutralità della rete. Mantenere la vitalità originale di Internet	Claude Béglé	16.06.2017	CN	DA-TEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173591
Ip.	17.3452	Come sostenere i media nella loro transizione verso il digitale?	Adèle Thorens Goumaz	14.06.2017	CN	DA-TEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173452
Ip.	17.3277	Le attuali sanzioni giudiziarie sono sufficienti per contenere i giganti di Internet?	Jean Christophe Schwaab	02.05.2017	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173277
Ip.	17.3276	Quale responsabilità in caso di pubblicità su Internet illegale, incitante all'odio o volta a finanziare attività criminali?	Jean Christophe Schwaab	02.05.2017	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173276
Ip.	17.3254	I vantaggi offerti dalle tecnologie moderne per le persone disabili. L'esempio dell'HbbTV	Pascale Bruderer Wyss	17.03.2017	CN	DA-TEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173254
Ip.	17.313	Vendita di animali vivi in Internet e protezione degli animali	Daniel Brélaz	15.03.2017	CN	DFI	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173130
Dom.	17.5206	Cybersicherheit. Missbrauch von gehackten Geräten des Internet of Things für Botnetze durch Sicherheitsstandards unterbinden	Balthasar Glättli	08.03.2017	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175206
Ip.	17.3069	Le statistiche attuali rilevano il potenziale della digitalizzazione?	Ruedi Noser	07.03.2017	CS	EDI	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173069
Ip.	17.3075	Digital Gender Gap. Quali sono le sfide e le opportunità della digitalizzazione nel mondo del lavoro da una prospettiva di genere?	Sibel Arslan	08.03.2017	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173075
Mo.	17.3592	Dalla governance del digitale alla governance digitale	Claude Béglé	16.06.2017	CN	DA-TEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173592
Ip.	17.3533	Potenziamento della formazione in informatica in Svizzera	Franz Grüter	15.06.2017	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173533
Ip.	17.3341	Insourcing e outsourcing. Qual è la politica dell'UFIT?	Stefan Müller-Altermatt	04.05.2017	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173341
I	17.104 0	Ampliamento delle reti di radiocomunicazione mobile per la digitalizzazione della Svizzera	Christian Wasserfallen FDP-Liberale Fraktion	06.06.2017	CN	DA-TEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20171040
Mo.	17.3498	Telefonia mobile, ristabilire la competitivà della Svizzera!	Yannick Buttet	16.06.2017	CN	DA-TEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173498

Dom.	17.5303	Gefährden Drohnen die Sicherheit der Landesflughäfen?	Priska Seiler Graf	07.06.2017	CN	DA-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175303
Dom.	17.5221	Alpbetriebe vom Telefonnetz abgehängt	Erich von Siebenthal	30.05.2017	CN	DA-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175221

8 Prodotti MELANI pubblicati

Oltre ai rapporti semestrali MELANI mette a disposizione del pubblico un certo numero di prodotti di vario tipo. I seguenti paragrafi offrono una sintesi dei blog, dei bollettini d'informazione, delle liste di controllo, delle guide e dei promemoria realizzati nel periodo in rassegna.

8.1 GovCERT.ch Blog

8.1.1 Notes About The «NotPetya» Ransomware

28.06.2017 - A new ransomware, currently named «NotPetya», has begun spreading yesterday. There are many victims, especially in Ukraine, but also large companies have been hit hard such as «Maersk» or «Merck». There are infections in Switzerland as well. As many others we have analyzed the malware and tried to harden evidence about its functioning. As there are many good papers already published, we do not want to repeat all these things but to highlight a few important facts that now can be considered being hardened evidence.

➔ https://www.govcert.admin.ch/blog/32/notes-about-the-notpetya-ransomware

8.1.2 «WannaCry»? It is not worth it!

15.05.2017 - On Friday, May 12th 2017, a ransomware called «WannaCry» hit the cyber space. Among the victims are hospitals in UK, the national telecom provider in Spain and U.S delivery service «FedEx». But WannaCry did not only hit the internet, the ransomware was also very present in newspapers worldwide. It also kept us and our partners from abroad very busy during the last weekend, analyzing the malware, reevaluating the current situation in Switzerland and world-wide, communicating with National Critical Infrastructure, and talking to the press. While we analyzed the threat as well, there are already many good papers on «WannaCry». For this reason we do for once not focus on the exact technical implementation, but try to give a comprehensive overview of this threat and the impact «WannaCry» has, with a focus on the situation in Switzerland.

➔ https://www.govcert.admin.ch/blog/31/wannacry-it-is-not-worth-it

8.1.3 When «Gozi» Lost its Head

04.04.2017 - After our automated unpacking procedure recently failed on a «Gozi» binary (MD5 c1a73ff8fb2836fe47bc095b622c6c50), we were forced to perform a manual analysis - and indeed we found some interesting new features in the first layer of the packer…

➔ https://www.govcert.admin.ch/blog/30/when-gozi-lost-its-head

8.1.4 Taking a Look at «Nymaim»

03.03.2017 - «Nymaim» is active worldwide since at least 2013 and is also responsible for many infections in Switzerland. Sinkhole Data shows that «Nymaim» is responsible for about 2% of infected devices in Switzerland that hit sinkholes the last few days. When we looked at the «Nymaim» trojan in January, we were stunned by their powerful code obfuscation techniques and wrote an «IDAPython» script to deobfuscate the code using the debugger engine. Later we found similar tools already available in the public to do this using code emulation. Nevertheless, we decided to publish a paper about our approach, as it is a very nice case study to demonstrate how debugger orchestration works in «IDAPython», and to explain different disassembly strategies that can be used. Instrumenting the debugger means to set breakpoints in scripts and to run the code in pieces, which has a very dynamic and fascinating impact on the IDA GUI.

➔ https://www.govcert.admin.ch/blog/29/taking-a-look-at-nymaim

8.1.5 The Rise of «Dridex» and the Role of ESPs

20.02.2017 - Last week, we have warned Swiss citizens about a new malspam run targeting exclusively Swiss internet users. The attack aimed to infect them with «Dridex». «Dridex» is a sophisticated eBanking Trojan that emerged from the code base of «Bugat» / «Cridex» in 2014. Despite takedown attempts by the security industry and several arrests conducted by the FBI in 2015, the botnet is still very active. In 2016, MELANI / GovCERT.ch became aware of a handful of highly sophisticated attacks against small and medium businesses (SMB) in Switzerland aiming to steal large amounts of money by targeting offline payment software. During our incident response in 2016, we could identify «Dridex» to be the initial infection vector, which had arrived in the victim's mailbox by malicious Office Word documents, and uncovered the installation of a sophisticated malware called «Carbanak», used by the attacker for lateral movement and conducting the actual fraud. Between 2013 and 2015, the «Carbanak» malware was used to steal approximately 1 billion USD from banks worldwide.

➔ https://www.govcert.admin.ch/blog/28/the-rise-of-dridex-and-the-role-of-esps

8.1.6 «Sage 2.0» comes with IP Generation Algorithm (IPGA)

30.01.2017 - On Jan 20, 2017, we came across a malware that appeared to be a new Ransomware family called «Sage 2.0». Within a couple of days we were able to collect more than 200 malware binaries across our sensors associated with this new Ransomware. Last week, Brad Duncan also wrote a SANS InfoSec Diary entry on «Sage 2.0», noticing some strange UDP packets sent to over 7'000 different Ips.

➔ https://www.govcert.admin.ch/blog/27/sage-2.0-comes-with-ip-generation-algorithm-ipga

8.2 Bollettino d'informazione MELANI

Nel primo semestre del 2017 MELANI ha pubblicato i seguenti bollettini d'informazione:

8.2.1 Malware: si raccomanda prudenza indipendentemente dal sistema operativo utilizzato

15.06.2017 - Gli artefici delle ondate di e-mail infette puntano sulla diversificazione per ampliare continuamente il proprio ventaglio di bersagli. Di conseguenza gli utilizzatori di sistemi Windows non sono più gli unici ad essere presi di mira. Nelle ultime settimane la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) ha osservato svariate ondate volte a distribuire software nocivi specificamente agli utenti svizzeri del sistema operativo sviluppato da Apple, macOS. È importante ricordare che ciascun utente dovrebbe muoversi in rete con cautela indipendentemente dal sistema operativo utilizzato.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/malware---si-raccomanda-prudenza-indipendentemente-dal-sistema-o.html

8.2.2 Crescente impiego abusivo dei nomi di servizi federali e di imprese

04.05.2017 - Negli ultimi mesi i nomi di servizi federali e di imprese conosciute sono viepiù stati impiegati abusivamente come mittenti. MELANI fornisce consigli su come comportarsi in un simile caso.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/zunehmender-missbrauch-der-namen-von-bundesstellen-und-firmen.html

8.2.3 Per un utilizzo sicuro dell'Internet delle cose

20.04.2017 - Il 24° rapporto della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), pubblicato il 20 aprile 2017, è dedicato agli incidenti informatici più importanti accaduti in Svizzera e all'estero nel secondo semestre del 2016. Il tema principale del rapporto è l'Internet delle cose.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/rapporto-semestrale-2016-2.html

8.2.4 Social Engineering: un nuovo metodo d'attacco orientato contro le imprese

20.01.2017 - Negli ultimi giorni la centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI ha ricevuto numerose segnalazioni di casi di truffe telefoniche ai danni di imprese svizzere. I criminali si spacciano per la banca della ditta, sostenendo di dover effettuare un update del sistema e-banking il giorno successivo. Fissano così un appuntamento per il quale richiedono la presenza di tutti i collaboratori del settore finanza. Ciò allo scopo di risolvere il problema del principale elemento di sicurezza, la firma collettiva e, in ultima analisi, di effettuare il pagamento fraudolento.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/social-engineering--neue-angriffsmethode-richtet-sich-gegen-firmen.html

8.3 Liste di controllo e guide

Nel primo semestre 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.
App	Il concetto di app (dall'abbreviazione inglese di Application) designa in generale ogni forma di programmi di applicazione. Nell'uso linguistico si fa nel frattempo perlopiù riferimento alle applicazioni per i moderni smartphone e tablet computer.
Attacco DDoS	Attacco Distributed-Denial-of-Service. Un attacco DoS in cui la vittima è attaccata simultaneamente da numerosi sistemi diversi.
Autentificazione 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.
Backup	Backup (in italiano: salvaguardia dei dati) designa la copia di dati nell'intento di poterli ricopiare in caso di perdita.
Bitcoin	Sistema di pagamento decentrato che può essere utilizzato in tutto il mondo e nome di un'unità di moneta digitale.
Booter / Stresser	Strumenti informatici che scatenano attacchi DDoS a pagamento («DDoS as a service»).
Border Gateway Protocol	Protocollo di routing utilizzato in Internet per connettere tra loro diversi sistemi autonomi.
Browser	Programmi per computer utilizzati soprattutto per visualizzare diversi contenuti del World Wide Web. I browser più conosciuti sono Internet Explorer, Opera, Firefox e

	Safari.
Browser / Navigatore	Programmi per computer utilizzati soprattutto per visualizzare diversi contenuti del World Wide Web. I browser più conosciuti sono Internet Explorer, Opera, Firefox e Safari.
Brute Force	Metodo di risoluzione di problemi nei settori dell'informatica, della criptologia e della teoria dei giochi, fondato sulla sperimentazione di tutti i casi possibili.
Bundle Identifier	Bundle Identifier è un'espressione che si riferisce a un identificatore che viene definito e mantenuto nello sviluppo di un'app e che generalmente assume la forma com.your-company.app-name.
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.
Content Delivery Network	Rete di server sparsi in diverse regioni e connessi tra loro attraverso Internet, utilizzati per distribuire contenuti, in particolare file multimediali di grandi dimensioni.
Defacement	Deturpamento di pagine web.
Definizioni	Descrizione
Domain Name System	Domain Name System. Con l'ausilio del DNS, Internet e i suoi servizi sono di agevole utilizzazione, perché al posto dell'indirizzo l'utente possono utilizzare nomi (ad es. www.melani.admin.ch).
Ethernet	Ethernet è una tecnologia utilizzata per le reti di dati collegate via cavo.
Exploit-Kit	Kit che consente a criminali di generare programmi, script o righe di codice mediante i quali è possibile sfruttare le vulnerabilità dei sistemi di computer.
File Win32PE	Portable Executable (PE) descrive il formato binario di programmi eseguibili. È il formato utilizzato per i file eseguibili nei sistemi Win32 e Win64.
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.
IP-Address	Indirizzo che identifica il computer in Internet (o su una rete TCP/IP; esempio: 172.16.54.87).
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. Ne può essere un esempio il controllo dei dati immessi dall'utente in un modulo web. È così possibile verificare se tutti i caratteri immessi alla richiesta di un numero telefonico corrispondono effettivamente a delle cifre. Come gli ActiveX 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.
Launcher	Programma informatico che aiuta a localizzare e avviare un programma.
Macro-malware	Malware installato tramite macro. Una macro è costituita da una sequenza di istruzioni che possono essere eseguite con un semplice richiamo.
Mail bombing	Iscrizione organizzata di indirizzi e-mail presso diversi offerenti di newsletter nell'intento di bloccare la casella di posta o i dispositivi di comunicazione del destinatario.
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 Toia, nonché le Logic Bombs.
Managed Service Provider (MSP)	Fornitore di servizi nell'ambito della tecnologia dell'informazione che si assume la responsabilità di predisporre un insieme definito di servizi per i suoi clienti e li amministra.
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.
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.
Plug-Ins	Un software di complemento che amplia le funzioni di base di un'applicazione. Esempio: i Plug-In di Acrobat per i browser di Internet consentono la visualizzazione diretta di file PDF.
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.
QR-Code	Il codice QR (Quick Response Code) sussiste in una matrice quadrata, a sua volta composta da quadratini bianchi e neri, che rappresentano i dati binari cifrati.
RAM	Random access memory: memoria di dati utilizzata soprattutto nei computer come memoria di lavoro, in prevalenza sotto forma di moduli di memoria.
Ransomware	Malware tramite il quale i proprietari dei computer infettati sono ricattati (ransom: termine inglese per riscatto). Nel caso tipico i dati sono cifrati e nuovamente messi a disposizione dall'aggressore dopo il pagamento del riscatto per la chiave di decodificazione necessaria al loro ripristino.
Remote Administration Tool	Il software di manutenzione a distanza (in inglese: Remote Administration Tool) costituisce un'applicazione nell'ambito del concetto di manu-tenzione a distanza di qualsiasi computer o sistema di computer.
RootKit	Un insieme di programmi e di tecniche che consentono di accedere inosservatamente a un elaboratore e di assumerne il controllo.
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 collega-

	mento 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.
Software Defined Radio	SDR: schemi di ricetrasmissione ad alta frequenza che implementano in un software parti minori o maggiori dell'elaborazione dei segnali.
SQL-Injection	SQL-Injection (introduzione clandestina SQL) designa lo sfruttamento di una lacuna di sicurezza nel contesto di una banca dati SQL, ossia di una lacuna che insorge a causa della mancata verifica delle variabili da trasmettere. L'aggressore tenta di introdurre clandestinamente i suoi propri comandi di banca dati per modificare i dati nel proprio senso o per assumere il controllo del server.
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 correla-

	zione 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).
Strategia di offuscamento	È definito offuscamento (in inglese «cyber-blurring») il metodo di collocare appositamente dati errati in una serie di dati per ostacolare l'attività degli hacker.
Take down	Take down (rimozione) è un'espressione utilizzata quando un provider ritira un sito dalla rete a causa della presenza di contenuti fraudolenti.
URL di dati	Schema URI che consente di includere dati in un testo fonte (HTML) come se fossero risorse esterne.
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).
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.