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 INFORMAZIONI

LA SITUAZIONE IN SVIZZERA E A LIVELLO INTERNAZIONALE

Rapporto semestrale 2016/II (luglio – dicembre)

20 APRILE 2017

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

1 Panoramica / Contenuti

1 Panoramica / Contenuti 2

2 Editoriale 5

3 L'Internet delle cose 6

3.1 Definizione 6

3.2 Internet delle cose: un'evoluzione rischiosa? 7

3.3 Ripercussioni per il futuro 7

3.4 Direttive e misure preventive 8

4 La situazione a livello nazionale 9

4.1 Spionaggio 9

4.1.1 La Svizzera possibile vittima indiretta di attività di spionaggio 9

4.2 Furto di dati 11

4.2.1 Ricatto con presunti dati di clienti 11

4.3 Sistemi industriali di controllo (ICS) 12

4.3.1 Sensibilizzazione sulle minacce relative agli ICS interconnessi 13

4.4 Attacchi 14

4.4.1 DDoS ed estorsioni: ultimi sviluppi in Svizzera 14

4.5 Social engineering, phishing 15

4.5.1 Tentativi di truffa di varia qualità 15

4.5.2 Phishing 16

4.5.3 Pagine ritenute di phishing per errore 17

4.5.4 Aumento delle iniziative di phishing awareness 18

4.6 Crimeware 19

4.6.1 Trojan bancari: imprese nel mirino 20

4.6.2 I trojan bancari sfruttano la disattenzione degli utenti 22

4.6.3 Ransomware 24

4.7 Misure preventive 25

4.7.1 Domini bloccati preventivamente in seguito all'analisi del malware Tofsee 25

4.8 Altri temi 26

4.8.1 Codice sorgente di e-voting sul sito Github 26

4.8.2 La gestione del registro per il dominio Internet «.ch» rimane a SWITCH 26

5 La situazione a livello internazionale 27

5.1 Spionaggio 27

5.1.1 Attacco contro il Comitato nazionale democratico (CND) : presa di posizione ufficiale 27

5.1.2 APT 28 collegato a numerosi eventi 27

5.1.3 «Winnti» matura: dal furto di fiche online al sofisticato spionaggio industriale contro le acciaierie 29
5.1.4 Netbotz: la videocamera che va oltre l'inquadratura 29
5.1.5 Altre campagne in prima pagina 30
5.2 Furto di dati 31
5.2.1 Yahoo Data Breach: fuga di dati di proporzioni inimmaginabili 31
5.2.2 Fuga di dati provocata da insider 31
5.2.3 Colpito di nuovo anche il sito Adultfriendfinder 31
5.3 Sistemi di controllo industriali (ICS) 33
5.3.1 Déjà vu a Kiev: nuovo blackout elettrico in Ucraina 33
5.3.2 Distributed Denial of Heating: abitanti al gelo dopo l'attacco DDoS 35
5.4 Attacchi 36
5.4.1 Avaria di Internet colpisce 900 000 clienti della Deutsche Telekom 36
5.4.2 Attacchi che prendono di mira le transazioni finanziarie 36
5.4.3 Un mercato dei ransonware molto frammentato 37
5.5 Vulnerabilità 38
5.5.1 Vulnerabilità nell'interfaccia USB 38
5.5.2 Password manager: una vulnerabilità cruciale? 39
5.5.3 Masque Attack nell'iOS 39
5.6 Misure preventive 40
5.6.1 Rete Avalanche: arresti e perquisizioni 40
5.7 Altri temi 40
5.7.1 Fine della vigilanza statunitense sulla gestione globale degli indirizzi Internet 40
5.7.2 Il gestore di punti di interscambio Internet DE-CIX chiede l'esame giudiziale delle misure di sorveglianza 41
6 Tendenze e prospettive 42
6.1 Cybercrime as a service e cyberestorsione: un circolo vizioso 42
6.2 Futura impostazione dell'autenticazione a due o più fattori 43
6.3 Tecnologie della sicurezza costantemente sotto pressione 44
7 Politica, ricerca, policy 46
7.1 Svizzera: interventi parlamentari 46
7.2 Strategia «Svizzera digitale» 48
7.3 Partecipazione della Svizzera all'esercizio «Cyber Europe 2016» 48
8 Prodotti MELANI pubblicati 50
8.1 GovCERT.ch Blog 50
8.1.1 Tofsee Spambot features .ch DGA - Reversal and Countermesaures 50

8.1.2 When Mirai meets Ranbyus 50
8.1.3 SMS spam run targeting Android Users in Switzerland 50
8.1.4 Dridex targeting Swiss Internet Users 50
8.2 MELANI Newsletter 51
8.2.1 Social Engineering: un nuovo metodo d'attacco orientato contro le imprese 51
8.2.2 e-banking: gli hacker prendono di mira i metodi di autenticazione per dispositivi mobili 51
8.2.3 Tema principale del rapporto semestrale MELANI: cyber-estorsione 51
8.2.4 Software offline per i pagamenti nel mirino degli hacker – imprese svizzere colpite .. 51
8.2.5 Numerosi documenti Office maligni in circolazione 52
8.3 Liste di controllo e guide 52
9 Glossario 52

2 Editoriale

In qualità di Head of Group Security, dal settembre 2015 Philippe Vuilleumier è responsabile della sicureza logistica e fisica presso Swisscom.

Care lettrici, cari lettori,

in passato un responsabile della sicurezza si chiedeva: «Che cosa devo fare per sventare gli attacchi alla mia organizzazione?». Oggi, con un briciolo di disillusione, bisogna chiedersi piuttosto: «Quanto tempo passerà prima che un attacco vada a segno?» Alla luce della crescente professionalizzazione degli aggressori, dello sviluppo delle possibilità tecniche e del conseguente perfezionamento di molti attacchi, è meglio partire dall'idea che il proprio ambiente sia già compromesso o che lo sarà ben presto.

Accettare questa realtà, però, non basta. Occorre trarre le debite conclusioni e adottare le misure adeguate. «Assume breach» è un concetto che a molti sembra rivoluzionario, ma che cosa ci riserverà il domani? Che cosa possono fare un'organizzazione in generale e, più nel dettaglio, il team responsabile della sicurezza, sua punta di diamante?

Noi di Swisscom siamo giunti alla conclusione che le cose da fare sono tre:

1. continuare a occuparci della nostra sicurezza di base. Ciò significa che dobbiamo tenere aggiornati i nostri inventari su infrastruttura, dati e collaboratori, installare a brevi intervalli gli update necessari per i sistemi e le applicazioni, gestire in modo coerente i rischi e prestare attenzione all'efficienza in tutte queste operazioni;

2. elaborare sistemi di sicurezza semplici per l'utente finale. La Security fornisce un grande contributo all'agilità richiesta all'interno dell'impresa fornendo soluzioni tecniche improntate alla semplicità e alla trasparenza;

3. puntare su rilevamento e capacità di reazione. Naturalmente, la prevenzione resta un fattore molto importante (parte della sicurezza di base), ma visto il continuo mutamento del panorama degli attacchi, questo fattore ha i suoi limiti. Individuare prontamente aggressioni e compromissioni ed essere in grado di arginarle e combatterle sono competenze importanti che vogliamo migliorare continuamente. A questo proposito cito con piacere anche MELANI quale partner competente e importante per Swisscom in questo frangente.

L'«Internet delle cose» è il tema principale del presente rapporto. Anche in questo contesto e in considerazione delle sfide che esso ci pone, le tre priorità sono la sicurezza di base, la semplicità e il rilevamento.

Vi auguro una buona lettura.
Philippe Vuilleumier

3 L’Internet delle cose

In futuro tutto ciò che potrà essere connesso ad Internet sarà certamente collegato. Quest’affermazione, forse un po’ esagerata, allude all’evoluzione che Internet subirà nei prossimi anni. Essa, porterà con sé svariati vantaggi, d’altro canto però, non potrà esimersi dall’essere al centro di animate discussioni riguardanti la sicurezza. In avvenire un numero sempre crescente di oggetti di uso quotidiano sarà connesso a Internet. Alcuni produttori parlano già dell’«Internet delle cose» («Internet of Everything», IoE), che collegherà persone, processi, dispositivi e dati in una rete onnicomprensiva. Il caso ricorrentemente evocato del frigorifero che ordina automaticamente il latte è certamente un esempio efficace ma solo uno tra i tanti possibili. In particolare l’ambito della domotica e dell’illuminazione controllata hanno conosciuto negli ultimi anni un vero e proprio boom.
In futuro l’Internet delle cose andrà ben oltre a quello che è oggi. Secondo gli analisti di Gartner[1], nel 2016 oltre 6 miliardi di «cose» erano già connesse a Internet. Entro il 2020 si ipotizza un aumento a oltre 20 miliardi di oggetti. E le possibilità di connettere oggetti a Internet sono ancora ben lungi dall’esaurirsi. Essi diventeranno sempre più indispensabili nella nostra vita quotidiana fino ad influenzarla. Alcuni sviluppi si stanno già delineando: i cosiddetti dispositivi «wearable», ossia le applicazioni che l’utente porta addosso o che sono cucite nei vestiti e che forniscono una miriade di dati, sono ancora agli esordi ma si estenderanno ben al di là dei già affermati fitness tracker. Anche in campo medico si utilizzeranno numerose applicazioni che permetteranno una diagnostica costante e migliore. È dunque immaginabile che potremo consultare in ogni momento sullo smartphone lo stato di tutti gli organi vitali. Un altro ambito centrale sarà quello dei veicoli senza conducente. I primi test sono già stati effettuati. Tuttavia, per garantire un funzionamento impeccabile e sicuro, è necessario dotare questi veicoli di diversi sensori interni ed esterni. Indipendentemente dall’evoluzione di queste automobili, anche sulle strade verranno installati molti sensori per controllare il continuo aumento del traffico. In questo contesto il rilevamento dei dati è dunque il tema dominante: in futuro, una schiera di sensori funzionanti in regime autarchico e autonomi che trasmettono dati a server tramite Internet ci aiuterà a prendere decisioni, a intraprendere azioni e a individuare per tempo i pericoli e quindi a evitarli.

3.1 Definizione

L’espressione «Internet delle cose» descrive la crescente interconnessione via Internet di oggetti e apparecchi di uso quotidiano. È stata utilizzata per la prima volta alla fine degli anni Novanta del secolo scorso dal pioniere della tecnologia Kevin Ashton quale base importante per lo scambio di dati tra due apparecchiature intelligenti[2]. Ad oggi non esiste tuttavia una definizione unitaria. Si può intendere questa espressione anche in senso molto ampio e utilizzarla come sinonimo di collegamento tra mondo reale e mondo virtuale[3]. Uno dei casi di applicazione consiste ad esempio nell’identificazione di oggetti concreti tramite chip RFID,

1 http://www.gartner.com/newsroom/id/3598917 (stato: 28.2.2017)
2 http://www.rfidjournal.com/articles/view?4986 (stato: 28.2.2017)
3 http://www.computerwoche.de/a/industrie-4-0-ist-das-internet-der-ingenieure,2538117 (stato: 28.2.2017)

codici QR e codici a barre. Con l'ausilio di uno scanner si crea il collegamento a Internet. In tal modo un semplice oggetto può essere trasformato in un prodotto intelligente, arricchito di informazioni e servizi. Nel settore industriale, nell'ambito dell'impiego di oggetti e sensori intelligenti, si utilizza spesso l'espressione «Industria 4.0» per alludere alla quarta rivoluzione industriale, contraddistinta dalla digitalizzazione.

3.2 Internet delle cose: un'evoluzione rischiosa?

Con le crescenti possibilità offerte da Internet (delle cose), anche i rischi e gli effetti secondari ci daranno maggiori grattacapi. Ad esempio bisognerà sempre garantire che il frigorifero ordini il latte e non che sia il latte a ordinare frigoriferi. Si porranno questioni fondamentali non solo per la manutenzione e gli standard di sicurezza, ma anzitutto anche per la sicurezza dei dati. Il senso e lo scopo dell'Internet delle cose consistono soprattutto nel permettere decisioni automatizzate e ottimizzate grazie a dati rilevati tramite sensori. Di conseguenza questo sistema genera milioni di serie di dati la cui integrità deve essere protetta. Continuando con l'esempio del nostro frigorifero, i dati rilevati forniscono un quadro interessante non solo sul consumo di latte dell'economia domestica, ma anche sull'uso di tutto il frigorifero. Questi dati possono essere utilizzati ad esempio per scopi di marketing. Nel caso estremo permetterebbero anche di verificare se un'economia domestica mangia sano o meno, un'informazione che potrebbe servire ad esempio alle casse malati come indicatore per il calcolo dei premi.

Nel secondo semestre del 2016 l'Internet delle cose ha fatto notizia soprattutto per il botnet «Mirai». Un gran numero di dispositivi mal protetti è stato hackerato. Il 21 ottobre 2016 è stato sferrato un attacco contro l'infrastruttura server del web-hoster «Dyn» provocando il blackout di molti servizi Internet popolari come Amazon, Spotify e Netflix. Quest'attacco ha dimostrato perché la sicurezza delle apparecchiature collegate all'Internet delle cose non può essere trascurata. Le centinaia di migliaia di apparecchi hackerati erano state programmate in modo che si collegassero contemporaneamente con i server della vittima designata. Con un volume di traffico dati pari a 1,2 terabyte al secondo, questo è stato uno dei più potenti attacchi DDoS sinora osservati.

L'Internet delle cose presenta differenze sostanziali rispetto alla classica tecnologia dell'informazione e della comunicazione (TIC). Contrariamente ai computer, spesso questi apparecchi di uso quotidiano in grado di connettersi a Internet sono protetti dall'accesso non autorizzato solo in misura limitata e possono quindi essere più facilmente infiltrati da malware. Anzitutto, frequentemente per accedere a questi apparecchi possono essere utilizzate le corrispettive password standard, che sovente dopo l'installazione non vengono modificate o addirittura non possono essere modificate. In secondo luogo, l'aggiornamento dei software utilizzati rappresenta un problema di fondo: infatti, solo in pochi casi il processo di update è regolamentato e molto raramente è automatizzato. Ne derivano dunque numerose sfide che negli anni a venire si complicheranno ancora di più. Rispetto alle convenzionali apparecchiature TIC, che in media sono impiegate solo per pochi anni, i dispositivi collegati all'Internet delle cose possono senz'altro essere utilizzati per un decennio o anche più a lungo.

3.3 Ripercussioni per il futuro

Il fatto che l'Internet delle cose venga sfruttato per sferrare attacchi DDoS non sarà però probabilmente il rischio maggiore a cui andiamo incontro. Un potenziale di minaccia molto

più elevato è rappresentato dalla manipolazione di tali sistemi. In particolare nel settore della logistica, le apparecchiature connesse a Internet stanno vivendo un vero e proprio boom. Al tempo stesso le possibili manipolazioni in questo settore potrebbero provocare anche enormi danni. Se ad esempio il settore logistico di un'impresa farmaceutica che ha subito una manipolazione consegna medicamenti urgenti all'indirizzo sbagliato, il problema può facilmente trasformarsi in una questione di vita o di morte. Un criminale potrebbe tentare di estorcere denaro con questi attacchi e i terroristi potrebbero cercare di creare un clima d'incertezza e destabilizzare la società.

Le problematiche legate alla sicurezza dell'Internet delle cose risiedono soprattutto nella scarsa consapevolezza dei gestori. Durante l'ultima conferenza RSA tenutasi a San Francisco, l'esperto in materia di sicurezza Lucas Lundgren ha lanciato un nuovo monito sul problema del protocollo di comunicazione mal protetto «Message Queue Telemetry Transport» (MQTT)[4]. Questo protocollo è spesso utilizzato per garantire la comunicazione delle cose tramite sensori. Il problema non risiede nel protocollo MQTT in quanto tale, ma piuttosto nel fatto che vi siano gestori che rinunciano completamente alla protezione tramite password e alla codificazione. Nel caso dei sensori funzionanti a batteria, questa rinuncia può ancora essere giustificata dal sovraccarico della CPU e dal corrispondente elevato consumo di corrente, ma in molti casi è semplicemente una questione d'ignoranza o di pigrizia[5]. Sensori che comunicano in rete senza alcuna protezione vengono installati in particolare nelle automobili, in sismografi, climatizzatori, lampade e apparecchiature tecniche per la medicina.

3.4 Direttive e misure preventive

Le diverse possibilità d'impiego dell'Internet delle cose nei vari settori e la quantità già smisurata e in crescita sempre più rapida di apparecchiature varie rendono difficile il compito di elaborare delle direttive. Nondimeno, nell'ottobre 2016 l'Organisation Cloud Security Alliance ha pubblicato un rapporto di un'ottantina di pagine[6] che offre in particolare una panoramica delle funzioni di sicurezza disponibili nelle diverse piattaforme per lo sviluppo di software. Il rapporto contiene anche delle direttive per il processo di progettazione e produzione nonché una lista di controllo che gli ingegneri possono consultare nel processo di sviluppo[7]. Anche MELANI ha pubblicato sul suo sito Internet alcune misure intese a migliorare il comportamento in fatto di sicurezza nell'Internet delle cose[8].

---

4 https://www.rsaconference.com/events/us17/agenda/sessions/6671-lightweight-protocol-serious-equipment-critical (stato: 28.2.2017)

5 https://www.heise.de/newsticker/meldung/MQTT-Protokoll-IoT-Kommunikation-von-Reaktoren-und-Gefaengnissen-oeffentlich-einsehbar-3629650.html (stato: 28.2.2017)

6 https://cloudsecurityalliance.org/download/future-proofing-the-connected-world/ (stato: 28.2.2017)

7 http://www.inside-it.ch/articles/45282 (stato: 28.2.2017)

8 https://www.melani.admin.ch/melani/it/home/themen/internet_of_things.html (stato: 28.2.2017)

Raccomandazione

Tutti gli apparecchi connessi a Internet devono essere non solo protetti (password individuali, accesso limitato), ma anche aggiornati regolarmente. L'aggiornamento dovrebbe essere sempre eseguito rapidamente, non appena gli update sono disponibili. Contrariamente a quanto avviene per i desktop computer e gli smartphone, nel caso degli interruttori intelligenti o dei frigoriferi quasi nessuno pensa che anche i software di questi dispositivi debbano essere aggiornati.

Dato che dopo l'installazione non sono stati modificati, gli oggetti e gli apparecchi che consentono di accedere a Internet mediante l'immissione di dati d'accesso standard (nome utente e password) presentano un potenziale di rischio ancora più elevato. Questi dispositivi possono essere identificati da chiunque (ad es. con un «port scanner» o un motore di ricerca come Shodan) e offrono quindi una superficie d'attacco particolarmente estesa.

MELANI mette a disposizione informazioni per proteggersi da queste minacce:

Sicurezza nell'«Internet delle cose»
https://www.melani.admin.ch/melani/it/home/themen/internet_of_things.html

4 La situazione a livello nazionale

4.1 Spionaggio

4.1.1 La Svizzera possibile vittima indiretta di attività di spionaggio

L'11 agosto 2016 Anonymous Polonia annunciava di aver piratato le reti dell'Agenzia mondiale antidoping (AMA) e del Tribunale arbitrale dello sport (TAS). Questo gruppo ha rivendicato anche un attacco DDoS contro il TAS. Il TAS è un'istituzione internazionale con sede a Losanna che propone arbitrati o mediazioni nei casi legati al mondo dello sport. La problematica del doping è un argomento sul quale il TAS è chiamato regolarmente a pronunciarsi. I fatti e il ruolo di Anonymous Polonia sono tuttora incerti, ma l'interesse per questo tipo di istituzione ha un senso se considerato nel contesto dell'esclusione di atleti russi per doping con le sue implicazioni politiche.[9] La Svizzera è chiamata in causa unicamente in quanto il TAS ha sede sul suo territorio ma non è stata presa di mira esplicitamente. Di conseguenza le implicazioni derivanti dall'attacco le concernono solo indirettamente. Ciò dimostra ancora una volta che la folta presenza di organizzazioni internazionali con sede in Svizzera espone il nostro Paese al rischio di operazioni cyber di cui dobbiamo tenere conto in modo adeguato per la sicurezza del territorio.

[9] Cfr. capitolo 5.1

Il 13 agosto 2016 la Svizzera è stata coinvolta in un nuovo caso, la pubblicazione da parte del gruppo The Shadow Broker di liste di domini e di indirizzi IP compromessi, potenzialmente utilizzati nel quadro di attacchi sferrati da «equation group»[10]. In questo lotto figuravano tre indirizzi di server basati all'Università di Ginevra. SWITCH, che offre diversi servizi in rete alle scuole universitarie svizzere, conferma che tre server sono stati compromessi tra il 2001 e il 2003, ma che due di essi sono stati disattivati nel 2009 e il terzo non è accessibile dall'esterno[11]. Sebbene sia ormai acqua passata e da allora siano stati presi provvedimenti, questo caso dimostra che il nostro Paese non è soltanto un obiettivo allettante, ma può essere utilizzato anche come tramite e ospitare infrastrutture utilizzate a fini di spionaggio. A volte queste infrastrutture possono essere ospitate da operatori negligenti[12], ma possono essere anche amministrate manomettendo server legittimi.

Le ragioni che fanno della Svizzera un bersaglio ideale sono già state elencate in rapporti precedenti[13]. Abbiamo già avuto occasione di esporre casi concreti in cui sono state colpite conoscenze o informazioni sensibili specifiche del nostro Paese. Il caso più emblematico, balzato agli onori della cronaca negli ultimi tempi, è senza dubbio quello dell'attacco all'impresa di armamento RUAG[14]. I due casi riportati sopra dimostrano che a volte il nostro Paese può essere anche una vittima collaterale di attività che non puntano direttamente alle informazioni che esso detiene.

---

10 Cfr. capitolo 5.1

11 http://www.watson.ch/Digital/NSA/715933955-NSA-hackte-Uni-Genf-und-missbrauchte-drei-Server-f%C3%BCr-Cyberangriffe (stato: 28.2.2017)

12 Questo caso era ad esempio riportato al capitolo 3.3 del nostro rapporto 2014/1 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2014-1.html (stato: 28.2.2017).

13 Cfr. in particolare il Rapporto semestrale 2015/2, capitolo 4.1 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2015-2.html (stato: 28.2.2017)

14 Rapporto semestrale 2016/1, capitolo 4.1.1 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2016-1.html (stato: 28.2.2017)

Conclusione / Raccomandazione

Da 13 anni MELANI si impegna per la protezione dai pericoli TIC in collaborazione con diversi enti statali e privati e sul suo sito mette a disposizione un formulario d'annuncio per segnalare casi sospetti:

Formulario d'annuncio MELANI:

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

Con il programma «Prophylax», il SIC realizza una campagna di prevenzione nel campo della non proliferazione e dello spionaggio economico. Il programma è inteso a sensibilizzare le imprese e le istituzioni nel campo della formazione:

Programma Prophylax:

http://www.vbs.admin.ch/de/themen/nachrichtenbeschaffung/wirtschaftsspionage.detail.publication.html/vbs-internet/de/publications/nachrichtendienst/Prophylax.pdf.html

http://www.vbs.admin.ch/it/tematiche/acquisizione-informazioni/spionaggio-economico.html

4.2 Furto di dati

4.2.1 Ricatto con presunti dati di clienti

In un comunicato stampa del 17 novembre 2016, la banca del Liechtenstein Valartis Bank ha annunciato di essere stata attaccata da hacker. L'aggressore ha avuto accesso a diverse informazioni su ordini di pagamento, soprattutto della clientela aziendale, eseguiti prima del mese di maggio del 2013. La banca ha escluso una manipolazione degli ordini di pagamento a carico dei clienti e ha dichiarato che il sistema centrale della banca non è stato violato. Inoltre, l'aggressore non avrebbe avuto accesso allo stato dei conti e simili. I clienti potenzialmente interessati dall'attacco sono stati informati dalla banca.

L'istituto bancario è venuto a conoscenza dell'attacco quando una persona l'ha contattato per e-mail comunicando di aver scoperto una perdita di dati e, contemporaneamente, offrendo i suoi servizi dietro pagamento per eliminare le lacune nel sistema di sicurezza. Valartis non ha reagito all'offerta.[15]

Secondo inside-it.ch, dato che in questo modo il ricattatore non ha avuto successo e non ha ottenuto i soldi sperati, ha tentato un secondo approccio rivolgendosi per e-mail direttamente

[15] http://www.valartisbank.li/Download.aspx?mode=download&id=IqzI6qVOde5v%2foNBMJr8xg%3d%3d (stato: 28.2.2017)

a clienti della banca. L'aggressore sembrava dunque possedere perlomeno alcuni indirizzi di posta elettronica di clienti. In questo messaggio ricattatorio, affermava di conoscere lo stato dei conti e altre informazioni. In caso di mancato pagamento dell'importo chiesto, minacciava di trasmettere i dati alle autorità finanziarie e ai media. Il ricattatore chiedeva il 10 per cento dello stato del conto in bitcoin[16].

MELANI parte dal presupposto che, dato che i clienti erano stati precedente informati dalla banca, nessuna vittima ha ceduto al ricatto. Interessante è che l'aggressore non avrebbe potuto verificare in nessun modo se la vittima avesse effettivamente versato il 10 per cento del proprio conto o una cifra inferiore, in quanto, secondo la banca, non era in possesso delle informazioni concernenti lo stato dei conti dei clienti. In questo caso, il ricattatore ha semplicemente speculato sull'onestà della vittima.

Conclusione / Raccomandazione

In questi casi MELANI sconsiglia vivamente di effettuare pagamenti, in quanto si instaurerebbe un legame di dipendenza con il ricattatore. Allo stesso tempo è comunque importante segnalare questi episodi per fermare l'aggressore.

Nel periodo in rassegna sono stati segnalati a MELANI diversi fatti analoghi. Nella maggior parte dei casi l'accesso a banche dati mal protette avviene tramite una cosiddetta «SQL-Injection», che permette di giungere ai dati. Le motivazioni dell'aggressore possono essere molteplici: in alcuni casi esistono effettivamente malintenzionati che adottato questo modo di procedere come «modello operativo» e si offrono per colmare una falla di sicurezza dietro pagamento. In altri casi invece, si tratta solo di un pretesto per estorcere più denaro possibile.

Gli hacker provenienti da differenti contesti e con diverse motivazioni cercano di distinguersi gli uni dagli altri. Al riguardo si sono affermati concetti quali «white hat», «grey hat» e «black hat»: i primi (cappelli bianchi) utilizzano le proprie conoscenze entro i limiti legali, i black hat (cappelli neri) agiscono tipicamente con intenti criminali e tentano di penetrare un sistema solo per vedere se vi riescono oppure per danneggiarlo o rubare dati. A metà strada troviamo i grey hat (cappelli grigi) che, pur infrangendo la legge, perseguono un obiettivo più «nobile», ad esempio quello di costringere i responsabili a prendere maggiormente sul serio la sicurezza e a migliorarla. I grey hat agiscono spesso in modo illegale, ma in genere rispettano un'«etica degli hacker».

4.3 Sistemi industriali di controllo (ICS)

Il sistema di comando centralizzato di una casa informa il proprietario che le tende da sole sono state abbassate. Contemporaneamente, il proprietario accende a distanza il climatizzatore per trovare una temperatura gradevole quando torna a casa. Spesso i comandi vengono impartiti con uno smartphone. Con l'aumentato utilizzo di queste comodità, un numero cre-

[16] http://www.inside-it.ch/articles/45798 (stato: 28.2.2017)

scente di utenti privati scopre la domotica degli edifici, una variante dei sistemi industriali di controllo.

Le tecnologie che trovano sempre maggiore spazio all'interno delle economie domestiche sono ormai da qualche tempo la norma in grandi complessi come uffici, fabbriche e ospedali. In questi grandi edifici la centralizzazione dei comandi di sistemi e apparecchiature sempre più numerose è necessaria per aumentare la qualità e l'efficienza della gestione. Ciò aumenta però anche il rischio di conseguenze in caso di accesso non autorizzato e manipolazione dei comandi centralizzati.

4.3.1 Sensibilizzazione sulle minacce relative agli ICS interconnessi

Per sfruttare i vantaggi della manutenzione remota, in molti casi gli ICS sono collegati a Internet. Questi sistemi consentono di sorvegliare lo stato delle apparecchiature e di impartire comandi a distanza. Se la connessione a Internet non è adeguatamente protetta, vi è il rischio che i sistemi di controllo vengano comandati in modo inopportuno da terzi non autorizzati. Alcuni motori di ricerca specializzati come Shodan[17] permettono anche a un profano di penetrare questi sistemi accessibili anche dall'esterno, contrariamente agli interessi del gestore.

Quando MELANI scopre sistemi potenzialmente esposti a queste minacce in Svizzera o riceve una segnalazione in questo senso, contatta i gestori per chiarire se sono informati sull'accessibilità del loro sistema. In ogni caso consegna una raccomandazione sulla sicurezza dei sistemi di controllo.

Alla fine dello scorso anno, dei ricercatori privati attivi nel settore della sicurezza hanno segnalato a MELANI un sistema di automazione degli edifici accessibile anche dall'esterno. Nel caso specifico vi sarebbe stata la possibilità di manipolare senza autorizzazione le condizioni climatiche all'interno dell'edificio.

Figura 1: Dettaglio del sistema di comando dell'edificio

Fortunatamente si trattava di un sistema ancora in fase di collaudo e l'edificio non era ancora occupato. Dopo aver concluso l'ultimo test, il sistema è stato isolato da Internet e da allora è accessibile soltanto ai tecnici incaricati dell'esercizio e della manutenzione.

[17] https://www.shodan.io/ (stato: 28.2.2017)

Raccomandazione

Se scoprite dei sistemi di gestione in Internet accessibili a non autorizzati, trasmetteteci i dati necesari per darci modo di informare il gestore.

Formulario di annuncio MELANI:

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

Liste di controllo e guide: Misure di protezione dei sistemi industriali di controllo (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

4.4 Attacchi

In Svizzera i cittadini e le aziende continuano a essere il bersaglio di diversi tipi di attacchi che prendono di mira in particolare i siti Internet. Soprattutto per le imprese che dipendono da una presenza affidabile in Internet, la vulnerabilità agli attacchi DDoS e ai defacing può rivelarsi problematica.

4.4.1 DDoS ed estorsioni: ultimi sviluppi in Svizzera

Nel nostro rapporto precedente ci siamo soffermati sulle aggressioni a fini meramente opportunistici che combinano attacchi DDoS con tentativi di estorsione e di ricatto. Questa tendenza in cui gli attori cercano di spaventare le vittime senza sferrare un attacco DDoS si è confermata nella seconda metà dell'anno. Come ci si poteva attendere, i criminali hanno sfruttato subito i timori suscitati dai «mega» attacchi DDoS mossi tramite la botnet MIRAI[18] per fare pressione su una vittima e ottenere bitcoin. Un attacco DDoS non ha però mai avuto luogo. Questo metodo è stato adottato alla fine dell'anno dal gruppo NewWorldHacker, che ha rivendicato anche i massicci attacchi al fornitore DNS Dyn.

Nonostante questa tendenza, altri casi ci mostrano che non si può mai escludere che alcuni attori scelgano di sferrare comunque un attacco. Il passaggio all'azione non è forzatamente sistematico ma può essere utilizzato come segno d'ammonimento per mettere sotto pressione altri possibili bersagli. Un caso sintomatico di questo modus operandi è fornito dal gruppo DD-crew DDoS, che punta a un settore d'attività molto preciso e attacca i concorrenti. Le altre imprese attive sul mercato vengono contattate separatamente, chiedendo loro di versare una somma in bitcoin se non vogliono subire la stessa sorte del loro concorrente. È inte-

[18] Cfr. capitoli 3 e 5.4

ressante notare che gli importi chiesti variano a seconda della notorietà (calcolata in base a Google Rank) e delle dimensioni dell'impresa.

Conclusione

La combinazione tra ricatto e minaccia d'attacco sembra destinata a durare. La paura generata dagli attacchi di vasta portata tramite MIRAI sarà ancora sfruttata. Inoltre, grazie alle varie offerte che propongono servizi di attacchi DDoS (Cfr. capitolo 6.1), qualsiasi attore può scegliere di sferrare attacchi. Questa situazione rende questo settore di attività criminale estremamente mutevole, con molti attori che adottano modus operandi simili.

4.5 Social engineering, phishing

Oltre a tutti gli attacchi tecnici, anche quelli che sfruttano le debolezze umane sono particolarmente popolari ed efficaci.

4.5.1 Tentativi di truffa di varia qualità

Anche nel secondo semestre del 2016 sono stati annunciati a MELANI diversi casi di «CEO fraud» (truffa del CEO). Si parla di «CEO fraud» quando l'autore chiede alla contabilità o al servizio finanziario di effettuare, per conto del direttore dell'impresa o di altri dirigenti, un pagamento su un conto che in realtà appartiene al truffatore e che, tipicamente, si trova all'estero. [19] I motivi addotti per giustificare il pagamento variano, anche se di regola si tratta di una presunta questione confidenziale urgente ed estremamente delicata. La qualità dei singoli tentativi di truffa varia in maniera considerevole. Mentre in alcuni casi viene posta solo una domanda di carattere generale ai fini del versamento urgente, in altri casi i truffatori raccolgono numerose informazioni sull'azienda presa di mira, per costruire una storia adeguata e realizzare la truffa in modo molto preciso. Spesso fa parte della montatura anche un consulente, oppure un fittizio o sedicente studio legale. Per dare una maggiore impressione di serietà alla richiesta, a volte vengono copiati o imitati anche siti Internet di banche o studi legali.

Nel periodo in rassegna non sono stati risparmiati neanche alcuni organi federali. Anche alcune divisioni delle finanze dell'Amministrazione federale, ad esempio, hanno ricevuto simili richieste truffaldine di versamento di denaro. In un altro caso, per incitare le vittime a effettuare pagamenti, è stato imitato il sito dell'Autorità di vigilanza sui mercati finanziari (FINMA).

L'accresciuta astuzia dei truffatori e la maggior cura dei particolari nel corso della pianificazione di un attacco sono evidenziate da un caso in cui il truffatore agiva telefonicamente spacciandosi addirittura per un servizio della Confederazione. Il quadro è chiaro: simulando un servizio statale ufficiale, la pressione esercitata sulla vittima per indurla ad eseguire l'azione desiderata aumenta. L'aspetto sorprendente è che sul display del telefono della vit-

[19] Vedi il Rapporto semestrale 2016/1, capitolo 4.5.2

tima appariva effettivamente un numero dell'Amministrazione federale. I truffatori avevano contraffatto il numero.

Raccomandazione

Gli attacchi di social engineering sfruttano la disponibilità, la buona fede e l'insicurezza delle persone ad esempio per accedere a dati confidenziali o indurre le vittime a compiere determinate operazioni. Fra le possibilità di attacco, questa rimane una delle più efficaci. MELANI ha pubblicato alcuni suggerimenti per proteggersi contro questo tipo di attacco.

INFO

Pericoli attuali: Social Engineering

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

4.5.2 Phishing

Anche nel secondo semestre del 2016 sono state inviate numerose e-mail di phishing. In questo contesto si osservano sempre gli stessi tipi di messaggio: alcuni chiedono dati delle carte di credito con il pretesto di «verificarli», altri chiedono informazioni su login e password di servizi Internet mediante un link integrato nell'e-mail. In questi messaggi di phishing si fa regolarmente un uso abusivo dei loghi di aziende conosciute o del servizio interessato per conferire una parvenza di ufficialità all'e-mail.

Complessivamente nel 2016 sono state segnalate, attraverso il portale antiphishing.ch gestito da MELANI, più di 4500 diverse pagine di phishing. La figura 2 illustra il numero di pagine web di phishing annunciate ogni settimana. I motivi delle oscillazioni sono disparati: alcune sono dovute a periodi di vacanze, in cui vi sono meno segnalazioni, mentre altre sono dovute al fatto che i criminali spostano regolarmente la loro attenzione da un Paese all'altro.

Figura 2: Pagine di phishing annunciate e confermate per settimana su antiphishing.ch nel secondo semestre del 2016.

4.5.3 Pagine ritenute di phishing per errore

Nel rapporto semestrale 1/2012[20] MELANI aveva già fatto presente quanto sia importante, nell'era del phishing, mantenere una comunicazione ben studiata con la clientela. Le e-mail autentiche indirizzate ai clienti generano spesso incertezza. Nel periodo in esame gli annunci dei cittadini in merito a presunte pagine di phishing sono aumentati. Ciò è sicuramente la conseguenza di una maggiore sensibilizzazione dei cittadini, ma anche del fatto che alcune imprese non si attengono a determinate direttive (cfr. prossimo riquadro).

4.5.3.1 Un classico: modifica delle condizioni generali di Paypal

Le comunicazioni di Paypal, eBay e simili relative a modifiche delle condizioni generali sono sempre seguite da annunci di presunte pagine di phishing. Anche se nell'e-mail non è presente alcun collegamento a una pagina di login, il fatto che l'utente riceva inaspettatamente un'e-mail da Paypal suscita una certa insicurezza di conseguenza MELANI riceve un rilevante numero di segnalazioni. Questo fenomeno è dovuto non da ultimo al fatto che in merito al phishing Paypal è uno dei servizi web maggiormente presi di mira e molti utenti hanno già ricevuto e-mail di phishing.

4.5.3.2 Collegamenti nascosti e collegamenti verso un server terzo

E-mail legittime di organizzazioni svizzere realmente esistenti possono, a volte, essere scambiate per e-mail di phishing scatenando, di conseguenza, un annuncio a MELANI. Durante il periodo in esame, l'annuncio pubblicitario di una ditta informava gli utilizzatori sulla possibilità di beneficiare di un credito. Il collegamento contenuto nella comunicazione, nascosto dietro un'immagine, non portava però al sito della ditta bensì a quello di società specializzata in marketing. Ciò ha scatenato in alcuni utenti una diffenza giustificata. In un altro caso, una ditta ha scritto ai propri clienti, annunciando che, nel caso di mancata reazione entro un termine stabilito, sarebbe stata fatturata loro una determinata somma di denaro a copertura dei costi amministrativi. L'e-mail non s'indirizzava direttamente al ricevente e un collegamento nascosto recava a una pagina web, dove venivano richiesti nome dell'utente e password. Anche in questo caso la procedura ha risvegliato dei sospetti in alcuni cittadini attenti che prontamente si sono rivolti a MELANI. In realtà l'e-mail proveniva effettivamente dalla ditta in questione e il collegamento portava alla corrispondente pagina web.

[20] Rapporto semestrale MELANI 2012/1, capitolo 3.8: https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2012-1.html (stato: 28.2.2017)

Conclusione / Raccomandazione

«Nessuna ditta seria chiederebbe mai i dati di login e la password via e-mail.» Questa è la risposta standard che MELANI dà sempre alle persone che segnalano un'e-mail con mittente sospetto. Nell'era della comunicazione elettronica con i clienti, questa affermazione, che di primo acchito sembra elementare, pone talvolta le ditte dinanzi a determinate sfide. Come comunicare con i clienti in modo che le e-mail non siano considerate fraudolente? E ancora: una comunicazione troppo negligente può anche influenzare negativamente il comportamento dei clienti in rapporto alle e-mail fraudolente.

Per l'invio di e-mail le aziende dovrebbero osservare i punti seguenti:

- inviare nella misura del possibile le e-mail unicamente sotto forma di pieno testo, affinché eventuali link contenuti siano chiaramente visibili e non si celino sotto altro testo (ad es. «Clicca qui»);
- i link devono essere pochi e rimandare unicamente a domini propri. Utilizzare nella misura del possibile link a pagine cifrate (https) e darne comunicazione anche ai destinatari;
- non inserire link verso siti per cui sono richiesti il nome di utente, la password o altri dati;
- inviare le newsletter per e-mail in maniera regolare;
- sulla pagina iniziale del sito, rimandare alla newsletter o collegare direttamente l'informazione a un link, affinché il destinatario possa inserire manualmente l'indirizzo principale e accedere da lì alla newsletter;
- rivolgersi al cliente con nome e cognome se questa informazione è disponibile.

Nel settore finanziario in special modo, le informazioni importanti sui conti devono essere inviate per iscritto tramite spedizione postale.

4.5.4 Aumento delle iniziative di phishing awareness

La sensibilizzazione dei propri collaboratori è fondamentale quando si tratta della sicurezza dell'azienda. Per questo motivo, un numero crescente di aziende adotta iniziative cosiddette di phishing awareness, che consistono nell'inviare ai collaboratori e-mail di phishing studiate di proposito. In seguito si analizza chi ha cliccato i link. Questo tipo di iniziative permette alla ditta non solo di sensibilizzare i propri collaboratori, ma anche di determinare il loro grado di consapevolezza (awareness) e di adottare quindi le opportune misure. A tale scopo la pagina di phishing viene salvata su un dominio che in precedenza è stato sbloccato appositamente. Lo scopo dell'esercizio consiste anche nel far sì che i collaboratori adeguatamente sensibilizzati trasmettano queste e-mail a centrali d'annuncio anti-phishing, come la pagina gestita da MELANI «antiphishing.ch». Tuttavia, con questo modo di procedere si mettono in atto diverse misure quali il take-down di pagine web e vari inserimenti in programmi filtro. Ovviamente queste reazioni compromettono i risultati del test di awareness. Per le pagine web bloccate o cancellate, non si possono più ricavare informazioni sul grado di sensibilizzazione dei collaboratori.

Raccomandazione

Un’adeguata e ricorrente sensibilizzazione dei collaboratori di un’impresa ma anche della popolazione è una delle colonne portanti della sicurezza in Internet. Le iniziative di phishing awareness sono una delle possibili forme di quest’opera di sensibilizzazione. Per garantire uno svolgimento ineccepibile, prima dell’esecuzione di un test di questo genere andrebbero informati perlomeno tutti gli attori coinvolti nell’infrastruttura. Si tratta in particolare del servizio di registrazione del dominio top level (per i domini .ch è SWITCH), registrar e hosting provider e l’eventuale provider (esterno) dei servizi di posta elettronica. Infine è consigliabile informare anche MELANI, affinché possa rispondere agli eventuali annunci voluti dall’organizzatore dell’iniziativa di awareness e non adotti misure contro il sito web.

4.6 Crimeware

Il crimeware è una forma di malware che dal punto di vista criminologico rientra nel campo della criminalità informatica e giuridicamente rientra nel settore del danneggiamento di dati e dell'abuso di un impianto per l’elaborazione di dati. Anche nel secondo semestre del 2016 la maggior parte delle infezioni è da attribuire a «Downadup» (noto anche come «Conficker»), un worm che esiste già da più di otto anni e che si diffonde tramite una falla di sicurezza rilevata nel sistema operativo Windows nel 2008 e perciò riparata da lungo tempo. Al secondo posto troviamo il malware «Necurs», specializzato nell’invio del trojan di crittografia «Locky» e del malware di e-banking «Dridex». Al terzo posto troviamo la rete bot «Mirai», resa celebre dall’attacco al fornitore di servizi Internet «Dyn» che infetta apparecchiature dell’Internet delle cose.

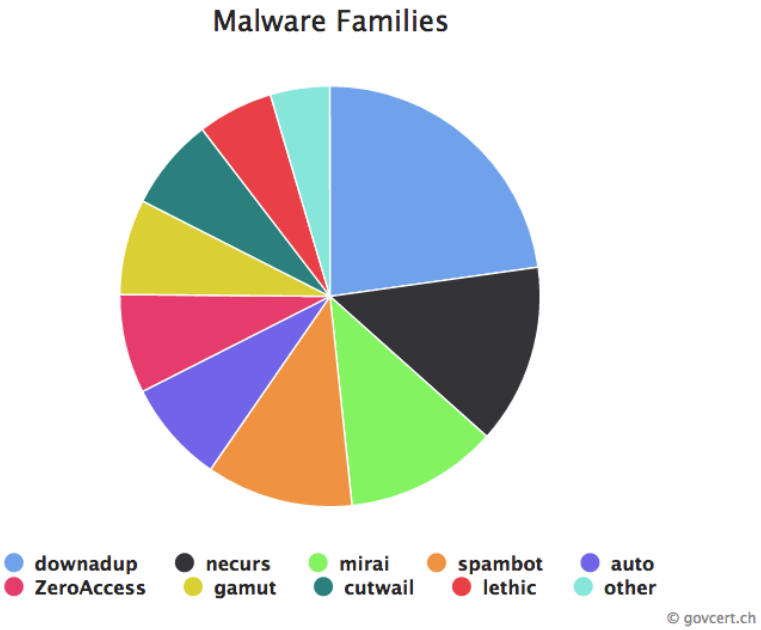

Figura 3: Distribuzione dei malware in Svizzera secondo i dati in possesso di MELANI. Il giorno di riferimento è il 31 dicembre 2016. Dati aggiornati disponibili al seguente indirizzo: http://www.govcert.admin.ch/statistics/dronemap/

4.6.1 Trojan bancari: imprese nel mirino

Nell'ultimo semestre lo spettro della famiglia dei trojan bancari non ha subito grosse variazioni. In Svizzera sono ancora attive le famiglie di malware «Retefe» e «Gozi». Mentre Gozi viene diffuso anche tramite infezioni di siti Internet, Retefe si diffonde attraverso e-mail con fatture falsificate di imprese esistenti più o meno note. Il documento word allegato alle e-mail contiene un JavaScript o un file eseguibile che modifica le impostazioni di Internet Explorer o Firefox inserendovi un proxyserver appartenente all'aggressore. Se lo desidera, l'aggressore può quindi deviare ogni dominio visitato dall'utente verso un server di sua scelta. Retefe ha anche la capacità di infettare cellulari e in seguito di deviare al truffatore l'SMS con il numero di autenticazione della transazione (mobile TAN). Secondo i rapporti del fornitore di servizi di sicurezza Trendmicro[21] il malware Android, che cattura la password unica inviata tramite SMS, è stato perfezionato dai truffatori. Sembrerebbe che criminali abbiano quindi dotato il malware di capacità anti-analisi, device routing e di accesso remoto. Il malware induce l'utente a concedere diversi diritti all'applicazione come ad esempio l'accessibility service, che permette di simulare le interazioni dell'utente. Anche «Dridex» viene diffuso tramite e-mail con fatture falsificate. Se fino al giugno del 2016 perlomeno in Svizzera erano stati attaccati con Dridex solo clienti privati di sistemi e-banking, nel luglio dello stesso anno i truffatori hanno cambiato la strategia di attacco prendendo di mira, da quel momento in poi, anche i software per pagamenti offline. Si tratta di software utilizzati da numerose imprese per effettuare in internet un numero cospicuo di pagamenti a una o più banche. Se dopo la prima infezione gli aggressori scoprono un software di questo tipo per i pagamenti, caricano il malware «Carbanak» specifico per questi casi. La figura 5 illustra in modo schematico il metodo d'infezione.[22]

---

21 http://blog.trendmicro.com/trendlabs-security-intelligence/new-smssecurity-variant-roots-phones-abuses-accessibility-features-teamviewer/ (stato: 28.2.2017)

22 Il malware è ricomparso alla fine del mese di febbraio 2017 con una grande ondata di spam: attraverso fatture di Swisscom falsificate si è cercato d indurre i destinatari a installare i trojan. https://www.govcert.admin.ch/blog/28/the-rise-of-dridex-and-the-role-of-esps (stato: 28.2.2017)

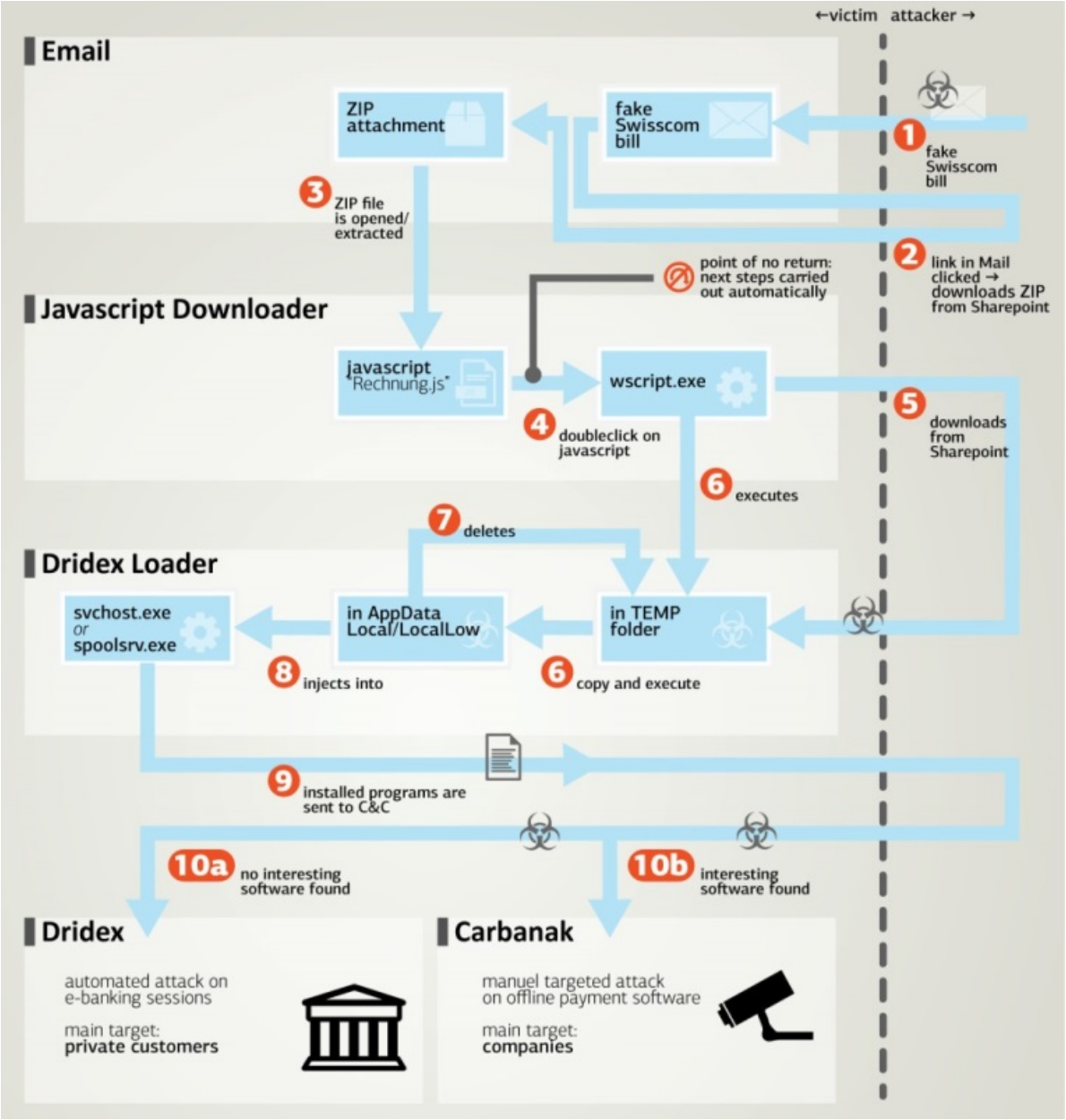

Figura 4: Illustrazione schematica del metodo d'infezione utilizzato nel febbraio 2017 per l'ondata di spam con fatture Swisscom falsificate.

Raccomandazione

Applicare ai computer utilizzati per il traffico dei pagamenti le seguenti misure di sicurezza:

- per effettuare i pagamenti offline e con e-banking servitevi di un computer particolare, che non usate per navigare in Internet, leggere e-mail ecc.;
- convalidate i pagamenti utilizzando una firma collettiva su un secondo canale (ad es. e-banking). Informatevi presso la vostra banca circa queste possibilità;
- se utilizzate un token hardware (ad es. Smart Card, USB-Dongle) rimuovetelo dal computer dopo aver terminato di utilizzare il software per i pagamenti;
- non salvate i dati per l'accesso all'e-banking e al software per i pagamenti (n. di contratto, password ecc.) nel computer o nel software;
- informatevi presso il produttore del vostro software per i pagamenti in merito ad ulteriori misure di sicurezza e attivate la funzione di aggiornamento automatico del programma;
- segnalate immediatamente alla vostra banca i pagamenti sospetti;
- per evitare un'infezione da Dridex e altri malware nella vostra azienda, MELANI raccomanda di adottare le misure seguenti:
  - assicuratevi che gli allegati potenzialmente dannosi che ricevete per e-mail vengano bloccati già nel gateway della vostra posta elettronica o rilevati dal filtro spam.
    Gli allegati pericolosi possiedono, tra le altre, le estensioni indicate nella seguente newsletter di MELANI:
    https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/offline-payment-software.html;
  - assicuratevi che questi allegati pericolosi vengano bloccati anche se inviati a destinatari della vostra impresa sotto forma di file d'archivio, ad esempio ZIP o RAR, ma anche come file d'archivio protetti (come un file ZIP protetto da password);
  - infine, si consiglia di bloccare anche tutti gli allegati che contengono macro (ad es. allegati Word, Excel o PowerPoint contenenti macro) a meno che non siano assolutamente indispensabili. Eventualmente l'invio e/o la ricezione di questi allegati potrebbero essere limitati a determinati mittenti o destinatari.

4.6.2 I trojan bancari sfruttano la disattenzione degli utenti

Nonostante siano considerate sicure, anche le moderne tecniche di autenticazione a due fattori come CrontoSign, PhotoTAN o SecureSign non sono immuni da tentativi di truffa. Alla fine di novembre 2016 sono stati annunciati a MELANI diversi casi in cui gli hacker erano riusciti a penetrare proprio questi sistemi per eseguire pagamenti fraudolenti. Tramite tecniche di ingegneria sociale, i malintenzionati inducevano i clienti di sistemi e-banking a convalidare pagamenti fasulli via PhotoTAN, CrontoSign o SecureSign.

Figura 5: Mosaico (a sinistra) e codice QR (a destra) per effettuare il login e convalidare un pagamento

Al momento del login o della convalida di un pagamento nel portale di e-banking viene visualizzato un *codice QR* o un *mosaico* (cfr. fig. 5) che il cliente può scansionare sullo smartphone con un'app o con un apparecchio separato. In seguito, a seconda del prodotto, il login o la convalida del pagamento avvengono direttamente nell'app, oppure quest'ultima genera un codice che il cliente deve inserire nel portale dell'e-banking. Tuttavia, molti clienti si lasciano ingannare da tecniche di ingegneria sociale e convalidano anche pagamenti che potrebbero riconoscere come fraudolenti, ad esempio quando nell'app viene chiaramente indicato il conto di un beneficiario sbagliato o quando i dati di pagamento vengono visualizzati già durante la procedura di login.

I fabbricanti hanno reagito migliorando la visibilità, affinché l'utente possa distinguere ancora meglio tra il processo di login e quello di autorizzazione del pagamento.

Figura 6: La nuova presentazione migliorata del generatore di password uniche mostra che non si tratta di un login ma di un'autorizzazione di pagamento.

Raccomandazione

Nell'accedere al portale di e-banking via smartphone con metodi di autenticazione mTAN, PhotoTAN, CrontoSign o SecureSign, MELANI raccomanda di adottare le seguenti misure di sicurezza:

- al momento del login al portale di e-banking con il dispositivo mobile (ad es. smartphone o lettore photo-TAN dedicato), accertatevi che stiate effettivamente confermando il login e non già convalidando un pagamento;
- prima di convalidare un pagamento, leggete sempre tutto il testo sul dispositivo mobile e controllate importo e beneficiario (nome, IBAN) del pagamento;
- informatevi in merito a ulteriori misure di sicurezza offerte dal vostro fornitore di servizi finanziari (ad es. esclusione standardizzata di pagamenti in Paesi con cui non intrattenete alcuna relazione d'affari).

4.6.3 Ransomware

Anche nel periodo in rassegna, sono stati segnalati a MELANI numerosi casi di ransomware (ossia di trojan che cifrano documenti a scopo di estorsione). Tra questi si registrano attacchi contro amministrazioni e PMI. Per difendersi è di vitale importanza eseguire un backup funzionante su un supporto esterno che non possa essere attaccato dal ransomware . Ancora meglio sarebbe impedire al ransomware di arrivare a questo punto adottando le opportune misure preventive. MELANI ha pubblicato alcune raccomandazioni in questo senso (cfr. il prossimo riquadro). La cifratura, e quindi la perdita temporanea di dati, rappresenta infatti solo una parte del problema. Occorre anche considerare che nel tempo occorrente per il caricamento del backup gran parte dell'azienda può essere paralizzata. Siccome oggi la maggior parte delle aziende è dipendente da TIC funzionanti, un'interruzione può comportare considerevoli perdite finanziarie. Per le infrastrutture critiche, un'interruzione dell'attività potrebbe avere conseguenze ancora più gravi.

In Svizzera circolano soprattutto i ransomware «Cerber», «Locky» e «Mischa/Petya». Cerber è stato diffuso, tra l'altro, con e-mail contenenti apparenti promesse di guadagno. Per quanto riguarda i canali di contagio, creano ancora molti problemi le e-mail con candidature fittizie che vengono inviate in modo mirato ai servizi del personale. Ma proprio nei servizi del personale, come del resto negli uffici stampa, i collaboratori devono costantemente aprire documenti provenienti da fonti sconosciute. In questi casi si raccomanda di utilizzare computer separati dalla rete e di stampare quindi le candidature. Anche le fatture o i mandati di comparizione falsificati sono metodi apprezzati dai criminali. In generale si può affermare che i truffatori sfruttano caratteristiche della vittima quali la curiosità, il timore e le prospettive di guadagno o di vincita.

Raccomandazione

- Eseguite regolarmente copie di sicurezza (backup) dei dati; il salvataggio dei file dovrebbe avvenire offline su un supporto esterno, ad esempio su un disco rigido esterno. Assicuratevi che il supporto venga scollegato dal computer subito dopo il salvataggio dei dati;
- aggiornate regolarmente le applicazioni e i plug-in installati (ad es. programma antivirus, browser);
- MELANI raccomanda di non aprire e-mail sospette, anche se apparentemente provengono da mittenti fidati. In caso di dubbio chiedete al mittente (se conosciuto e non via e-mail) in che cosa consiste esattamente l'allegato;
- i servizi che a causa della propria funzione devono aprire allegati di e-mail provenienti da mittenti sconosciuti devono utilizzare computer appositamente predisposti a tale scopo e che siano isolati nel miglior modo possibile dal resto della rete dell'azienda, per impedire la diffusione di eventuali infezioni su tale rete.

Misure contro i ransomware:

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

Ransomware: minacce attuali, prevenzione e reazione del BSI:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.html

Progetto No More Ransom:

https://www.nomoreransom.org/decryption-tools.html

Regole di comportamento: E-Mail

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

4.7 Misure preventive

4.7.1 Domini bloccati preventivamente in seguito all'analisi del malware Tofsee

Molti malware integrano un algoritmo di generazione di dominio («Domain generation algorithm», DGA) pensato per creare nomi di domini che permettono ai computer infettati (bot) di comunicare con l'infrastruttura di comando e di controllo (C&C). La possibilità di generare dinamicamente nomi di domini diversi a intervalli regolari, anziché definirli in anticipo in maniera definitiva, presenta il vantaggio di rendere molto più complessa l'adozione di eventuali misure contro la comunicazione dei bot verso l'infrastruttura C&C. Per prevedere i nomi di dominio dinamici che saranno utilizzati dai criminali è infatti necessario capire l'algoritmo utilizzato. È questo il lavoro iniziato dalla squadra di MELANI a fine dicembre 2016. Un'analisi del malware Tofsee, il cui scopo principale è inviare spam su larga scala tramite computer compromessi, ha permesso di capire il funzionamento del DGA. È statoconstatato che una delle sue peculiarità consisteva nel generare nomi di domini che utilissero il dominio

di primo livello nazionale («Country Code Top-Level Domain» o «ccTLD»), ciò per quasi la metà dei casi in esamine. In seguito MELANI ha lavorato con il registry del ccTLD.ch SWITCH e Registrar of Last Resort, una fondazione attiva nella lotta contro i nomi di dominio maligni. Questa collaborazione ha permesso di impedire per 12 mesi la registrazione dei nomi di dominio in .ch suscettibili di essere prodotti da questo DGA specifico (oltre 500).

4.8 Altri temi

4.8.1 Codice sorgente di e-voting sul sito Github

In dicembre, il Cantone di Ginevra ha pubblicato parte del codice sorgente del suo sistema di e-voting sul sito Github. L'iniziativa risponde a una volontà di trasparenza, ma potrebbe anche permettere di beneficiare di eventuali contributi esterni per migliorare il dispositivo. Il sistema ginevrino di e-voting è stato acquisito anche da altri Cantoni.

4.8.2 La gestione del registro per il dominio Internet «.ch» rimane a SWITCH

All'inizio del 2016 l'Ufficio federale delle comunicazioni (UFCOM) ha messo a pubblico concorso la gestione dei nomi di dominio .ch[23]. La Fondazione SWITCH ha vinto il concorso in quanto la sua offerta ha ottenuto il punteggio più alto tra tutte le altre pervenute[24]. In particolare il suo dossier si è distinto grazie all'ottimo concetto per la lotta contro la criminalità informatica. SWITCH esercita già oggi la funzione di gestore del registro per i nomi di dominio .ch. Per almeno altri cinque anni continuerà a gestire la banca dati nazionale dei nomi di dominio .ch e a garantire l'interconnessione elettronica con il sistema mondiale dei nomi di dominio (DNS).

Il Consiglio federale ha classificato i domini svizzeri di primo livello quale infrastruttura critica.In quanto tale essi necessitano di una particolare protezione, dato che un'interruzione comprometterebbe estesi settori della vita pubblica in Svizzera. MELANI si adopera per garantire la sicurezza e la disponibilità dei nomi di dominio svizzeri in stretta collaborazione con il gestore del registro.

---

[23] https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-61133.html (stato: 28.2.2017)

[24] https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-63597.html, https://www.SWITCH.ch/it/news/SWITCH-wins-tender/ (stato: 28.2.2017)

5 La situazione a livello internazionale

5.1 Spionaggio

5.1.1 Attacco contro il Comitato nazionale democratico (CND) : presa di posizione ufficiale

Nel precedente rapporto semestrale di MELANI[25] è già stato menzionato il cyberattacco contro il Comitato nazionale democratico (CND), attribuito, secondo il rapporto dell'impresa di sicurezza Crowdstrike, a Cozy Bear e Fancy Bear[26]. Nella seconda metà dell'anno, nuove informazioni, provenienti verosimilmente dalla stessa campagna elettorale, sono state rivelate sulle piattfaforme wikileaks e DCLeaks. Tra i dati pubblicati vi sono in particolare circa 58 000 messaggi che si suppone provengano dall'account privato compromesso del responsabile della campagna di Hillary Clinton, John Podesta.

Il 7 ottobre 2016, in una presa di posizione congiunta, il dipartimento della sicurezza interna («Department Of Homeland Security») e l'ufficio del direttore dei servizi d'informazione («Office of the Director of National Intelligence») statunitensi hanno accusato il governo russo di aver tentato di perturbare le elezioni presidenziali con una serie di attacchi agli account di posta elettronica di personalità e istituzioni politiche[27]. Un rapporto investigativo pubblicato il 29 dicembre 2016 punta il dito contro gli attori Cozy Bear e Fancy Bear[28]. In tale contesto sono state annunciate sanzioni contro enti e cittadini russi.

L'aspetto inedito di questo caso è senza dubbio la precisione con la quale le autorità russe al massimo livello sono state accusate da un altro Stato di aver diretto un cyberattacco. D'altronde, il bersaglio designato dell'operazione, ossia un'elezione presidenziale già molto tesa, ha amplificato la risonanza del caso[29].

5.1.2 APT 28 collegato a numerosi eventi

Il gruppo noto con i nomi Sofacy, Fancy Bear, Pawn Storm e APT 28[30] è stato indicato come probabile responsabile di numerosi attacchi sferrati nel periodo in esame. L'11 agosto 2016 Anonymous Polonia ha annunciato di aver piratato l'Agenzia mondiale antidoping (AMA) e il

---

25 Rapporto semestrale 2016/1 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2016-1.html (stato: 28.2.2017)

26 https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ (stato: 28.2.2017)

27 https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national (stato: 28.2.2017)

28 https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity (stato: 28.2.2017)

29 Tutta la tematica dei metodi d'influenza, alla luce delle ultime elezioni presidenziali americane, sarà trattata più da vicino nel capitolo 5.1 del rapporto 2016/1: https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2016-1.html (stato: 28.2.2017)

30 I nomi sono quelli utilizzati da diverse imprese o autorità che hanno indagato sugli attacchi in questione.

Tribunale arbitrale dello sport (TAS)[31]. L'identità esatta e il ruolo svolto da questo gruppo non sono chiari. Il 19 agosto 2016 la piattaforma Threat Connect ha pubblicato un'analisi dell'operazione collegandolaa Fancy Bear[32]. Questa tesi si basa in particolare sul procedimento di registrazione dei nomi di dominio utilizzati per imitare le organizzazioni che i il gruppo criminale sfruttava come copertura.

Nel caso WADA gli hacker hanno utilizzato un dominio del genere per sganciare un attacco spear phishing. Gli aggressori cercavano di ottenere i dati per l'accesso ad «adams» («Anti-Doping Administration & Management System»), il sistema in cui sono registrati i dati relativi ai controlli antidoping degli atleti. L'attacco,confermato dall'agenzia, ha permesso soprattutto di compromettere l'account di Yuliya Stepanova, la mezzofondista russa all'origine delle rivelazioni e di conseguenza delle sanzioni adottate contro gli atleti russi accusati di aver assunto sostanze dopanti. In seguito, nel mese di settembre, dati di numerosi atleti di tutto il mondo sono stati pubblicati da un gruppo firmatosi Fancy Bear. Occorre precisare che in seguito l'AMA ha evocato la possibilità che alcuni dei dati pubblicati fossero falsi.

Il 20 settembre, la Süddeutsche Zeitung e le emittenti pubbliche tedesche NDR e WDR hanno riportato che nel mese precedente alcuni politici tedeschi sono stati bersaglio di e-mail di spear phishing[33] apparentemente provenienti da servizi della NATO. Come nel caso degli attacchi contro il Bundestag nel 2015, il quotidiano cita fonti in seno al governo che attribuiscono queste attività al gruppo Sofacy. Il 24 settembre nuove rivelazioni hanno precisato che l'attacco avrebbe colpito anche l'emittente WDR[34].

In dicembre, nuove pubblicazioni hanno accusato lo stesso gruppo. Il primo articolo è apparso sul quotidiano Le Monde, il quale rivela un probabile attacco all'OSCE, poi confermato dall'organizzazione stessa[35]. Alla fine del mese, un rapporto della società crowdstrike valuta le operazioni della campagna di spionaggio Sofacy in modo del tutto diverso[36]. Analizzando un'applicazione Android sviluppata da un ufficiale ucraino per gli artiglieri suoi connazionali[37], crowdstrike scopre delle tracce di X-Agent, un malware utilizzato soltanto da Fancy Bear (alias Sofacy). Per esempio la manomissione avrebbe permesso di localizzare più facilmente, e potenzialmente distruggere, i pezzi d'artiglieria dell'esercito ucraino.

---

31 Questa istituzione ha sede a Losanna. Il caso è ripreso nella parte del presente rapporto dedicata alla Svizzera.

32 https://www.threatconnect.com/blog/fancy-bear-anti-doping-agency-phishing/ (stato: 28.2.2017)

33 http://www.sueddeutsche.de/politik/bundesregierung-ist-alarmiert-hackerangriff-aufdeutsche-parteien-1.3170347 (stato: 28.2.2017)

34 http://www.spiegel.de/politik/deutschland/cyberattacke-russische-hacker-attackieren-wdr-journalisten-a-1113780.html (stato: 28.2.2017)

35 http://www.lemonde.fr/international/article/2016/12/28/l-osce-victime-d-une-attaque-informatique_5054744_3210.html (stato: 28.2.2017)

36 https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/ (stato: 28.2.2017)

37 Quest'ultima è stata distribuita su forum frequentati da militari e mirava a incrementare l'efficacia di utilizzo di un obice (D-30 Howitzer).

5.1.3 «Winnti» matura: dal furto di fiche online al sofisticato spionaggio industriale contro le acciaierie

A inizio dicembre 2016, il gruppo industriale tedesco Thyssenkrupp dichiarava al settimanale Wirtschaftswoche[38] di essere caduto vittima di un atto di cyberspionaggio. Un gruppo di hacker noto come «Winnti» era riuscito già in primavera a penetrare nelle reti dell'impresa. Dopo la scoperta del fatto da parte del team di esperti di sicurezza interno, per ripristinare il sistema sono occorsi sei mesi di misure difensive. Gli aggressori sono comunque riusciti a sottrarre alcuni dei dati registrati.

Tra gli obiettivi, oltre alle sedi dei settori di «Industrial Solutions» in Europa, India, Argentina e Stati Uniti, vi era anche il laminatoio di Hohenlimburg del settore acciaierie del gruppo industriale tedesco. Fortunatamente non si sono registrati danni fisici. A quanto pare l'unica motivazione del gruppo di hacker consisteva nello spionaggio.

L'Ufficio Federale per la Sicurezza Informatica («Bundesamt für Sicherheit in der Informationstechnik», BSI) ha confermato che «Winnti» può essere ricollegato anche ad attacchi perpetrati contro altre imprese. Il gruppo si distingue per la capacità di introdurre accessi remoti ben occultati in ambienti di sistema altrui e si è fatto conoscere nel 2009 con attacchi a piattaforme di gioco online, da cui sottraeva fiche e gettoni per rivenderli sul mercato nero. Dal 2015 ha esteso il proprio campo di attività allo spionaggio informatico aziendale.

5.1.4 Netbotz: la videocamera che va oltre l'inquadratura

Negli ambiti estremamente sensibili in cui agiscono le autorità di uno Stato e le grandi imprese, si fa largo uso dei sistemi di sorveglianza del produttore statunitense Netbotz, quali ad esempio videocamere o sistemi di monitoraggio dei server. Tuttavia, secondo il programma televisivo «Fakt» del canale tedesco ARD, queste apparecchiature contengono vie d'accesso nascoste sfruttate dai servizi segreti americani.[39] Fakt fa riferimento a un rapporto classificato segreto dei servizi d'informazione tedeschi («Bundesnachrichtendienst», BND), secondo cui una fonte avrebbe avvertito il BND già nel 2004 circa la possibile esistenza di una porta di servizio nei prodotti di Netbotz. Le verifiche tecniche effettuate hanno permesso di constatare che il sistema Netbotz cercava effettivamente di instaurare una connessione con un server del Dipartimento della difesa americano. Netbotz aveva palesemente cercato di vendere i propri sistemi con aggressive offerte di sconto al ministero degli esteri tedesco e a potenziali clienti nel settore high tech e nel settore degli armamenti. Il programma del canale ARD dedicato al giornalismo d'inchiesta condanna soprattutto il fatto che né il BND né l'Ufficio federale della Protezione della costituzione(«Bundesamt für Verfassungsschutz», BfV) e neppure le aziende interessate abbiano informato in merito alla scoperta degli accessi remoti occulti. Oggi Netbotz appartiene al gruppo francese Schneider Electric, che produce molti componenti di base di tutta una serie di comandi industriali.

---

38 http://www.wiwo.de/unternehmen/industrie/spionageangriff-auf-thyssenkrupp-grossalarm-haette-die-risiken-erhoeht/14948264.html (stato: 28.2.2017).

39 http://www.mdr.de/fakt/industriespionage-100.html (stato: 28.2.2017).

5.1.5 Altre campagne in prima pagina

Se quella di Sofacy è indubbiamente stata la campagna più discussa nella seconda metà del 2016, molte altre rivelazioni hanno posto in evidenza le pratiche di cyberspionaggio utilizzate in tutto il mondo. Come spesso accade, queste operazioni sono state svelate da società di sicurezza private in seguito a indagini svolte con clienti colpiti. A causa del gran numero di campagne risulta difficile citarle tutte, sistematicamente, in queta sede, motivo per cui abbiamo deciso di focalizzarci su alcuni esempi ed in particolare sulla campagna di spionaggio The Dropping Elephant[40], un attore discretamente sofisticato di presunta origine indiana (secondo Kaspersky e On the StrongPity[41]), che attacca in particolare sistemi di cifratura. Symantec ha dato notizia delle attività di un gruppo chiamato Strider[42] che ha sferrato attacchi molto specifici contro un numero limitato di bersagli (Kaspersky ha battezzato la stessa operazione ProjectSauron[43]). Infine, una società israeliana (NSO Group) è stata accusata di aver sfruttato delle lacune su iPhone (in seguito colmate da Apple) a fini di sorveglianza[44].

Un'altra informazione importante inerente lo spionaggio informatico concerne la pubblicazione, avvenuta il 13 agosto 2016 da parte del gruppo The Shadow Brokers, di una serie di strumenti e malware proveniente dall'arsenale di Equation Group, gruppo che svolge attività di cyberspionaggio sofisticate che si suppone siano legate alla NSA.The Shadow Brokers ha dichiarato di aver pubblicato solo una parte dei file in suo possesso e di aver messo all'asta il resto. Numerosi esperti attesteranno in seguito l'autenticità dei file. Il 31 ottobre 2016 il gruppo pubblica un nuovo archivio con nomi di dominio e indirizzi IP manomessi per sferrare attacchi[45]. L'identità di The Shadow Brokers e la fonte delle sue informazioni sono oggetto di molte speculazioni ma non sono state trovate prove formali.

Non di rado l'attribuzione di un attacco sofisticato (del tipo APT) poggia su elementi di natura tecnica (ad es. l'infrastruttura utilizzata) e su modus operandi molto specifici. Il livello di attendibilità dell'attribuzione varia da caso a caso. La valutazione richiede spesso l'integrazione di elementi politici e strategici. Le vittime degli attacchi non sono scelte a caso ma pianificati accuratamente. Occorre pertanto chiedersi quale aggressore abbia interesse a colpire un'organizzazione specifica. Se la risposta a tale domanda può valere per diversi casi l'attribuzione dell'attacco risulterà rafforzata.

---

40 https://securelist.com/blog/research/75328/the-dropping-elephant-actor (stato: 28.2.2017).

41 https://securelist.com/blog/research/76147/on-the-strongpity-waterhole-attacks-targeting-italian-and-belgian-encryption-users (stato: 28.2.2017).

42 http://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets (stato: 28.2.2017).

43 https://securelist.com/analysis/publications/75533/faq-the-projectsauron-apt/ (stato: 28.2.2017).

44 https://motherboard.vice.com/en_us/article/nso-group-new-big-player-in-government-spyware?trk_source=recommended (stato: 28.2.2017).

45 Per le implicazioni svizzere di questa rivelazione cfr. capitolo 4.

5.2 Furto di dati

In un'economia e società digitali i dati sono una delle materie prime, se non addirittura l'unica. In pratica ogni azienda gestisce una banca dati contenente una gran quantità di informazioni personali (dei clienti). La sicurezza deve quindi essere adeguatamente considerata. Tuttavia, le fughe di dati, vale a dire l'acquisizione illecita di dati, sono un fenomeno con cui siamo confrontati regolarmente.

5.2.1 Yahoo Data Breach: fuga di dati di proporzioni inimmaginabili

A metà dicembre 2016, Yahoo ha denunciato una fuga di dati di proporzioni incredibili. In un incidente del 2013, autori sconosciuti erano riusciti ad accedere a un miliardo di dati. Fortunatamente pare che i dati sottratti non riguardassero carte di credito. Tuttavia, negli ambienti criminali anche informazioni personali quali nome, data di nascita, numeri telefonici e indirizzi e-mail sono merce di pregio, in quanto costituiscono la base per ulteriori attacchi con tecniche di ingegneria sociale. Ecco perché i criminali collegano sempre più spesso nomi e indirizzi e-mail e sono in grado di rivolgersi personalmente ai destinatari. Già nel settembre 2016, Yahoo ha reso noto un deflusso di dati, risalente all'anno 2014, che riguarda i conti di oltre 500 milioni di utenti Yahoo.

5.2.2 Fuga di dati provocata da insider

Il gruppo Sage è conosciuto nel mondo intero come uno dei maggiori fornitori di software aziendali e finanziari per piccole e medie imprese. L'attacco che ha apparentemente colpito il gruppo a inizio agosto 2016 può aver interessato i dati di 300 aziende che utilizzano i software finanziari di Sage. Il gruppo Sage memorizza diversi dati dei clienti, tra cui nomi, indirizzi, date di nascita, numeri di assicurazione sociale, relazioni di conto e altri dati finanziari. Dato che l'attacco è stato perpetrato tramite un normale login, si è ipotizzato sin all'inizio che si trattasse dell'opera di un insider, ipotesi che ha peraltro trovato conferma. Questo incidente fornisce, a tutti i responsabili della sicurezza, per l'ennesima volta, la prova che oltre a proteggersi dagli attacchi dall'esterno non si dovrebbero trascurare nemmeno quelli che possono provenire dall'interno.

5.2.3 Colpito di nuovo anche il sito Adultfriendfinder

Il portale per adulti Adultfriendfinder è stato di nuovo vittima di un accesso illecito ai propri dati. Nel novembre 2016 il portale ha denunciato la fuga di un totale di 412 milioni di dati. Adultfriendfinder era già salito alla ribalta delle cronache nel 2015 per un incidente analogo, che aveva toccato 3,5 milioni di serie di dati. Per i criminali, i dati presenti sui portali per adulti sono un affare particolarmente remunerativo, poiché questi dati possono essere utilizzati fruttuosamente per ulteriori scopi. Secondo il portale LeakedSource, i dati sottratti comprendono indirizzi e-mail, password talvolta addirittura non protette, nomi utente, indirizzi IP e informazioni dei browser[46]. LeakedSource ha stigmatizzato il fatto che l'operatore non abbia

[46] http://www.leakedsource.com/blog/friendfinder (stato: 28.2.2017)

correttamente cifrato i dati e abbia memorizzato le password in testo chiaro o le abbia protette soltanto con l'obsoleta funzione hash «SHA 1».

Raccomandazione

Se si osservano gli indirizzi e-mail che emergono da banche dati di questo tipo, una volta hackerate, si constata che tra di essi compaiono anche numerosi indirizzi aziendali, benché i servizi Internet delle aziende interessate non abbiano certamente nulla a che fare con questo tipo di portali. Molte ditte permettono un uso moderato per scopi privati della loro infrastruttura aziendale, e in particolare dell'accesso a Internet. Comunque, l'utilizzo di indirizzi e-mail aziendali per scopi privati dovrebbe essere chiaramente disciplinato. Anche l'impiego delle infrastrutture informatiche dell'azienda per lo scambio di e-mail private cela dei pericoli: gli allegati sospetti non si dovrebbero aprire, né in ufficio né a casa.

Regole di comportamento per le e-mail

https://www.melani.admin.ch/melani/it/home/schuetzen/verhaltensregeln.html ➔ E-Mail

Regole di comportamento per le password

La password dovrebbe essere modificata a intervalli regolari (ogni tre mesi circa), ma al più tardi quando presumete che possa essere conosciuta da terzi.

Ulteriori regole:
https://www.melani.admin.ch/melani/it/home/schuetzen/verhaltensregeln.html ➔ Password

Se siete un'azienda che gestisce banche dati alle quali i clienti possono accedere online, dovreste assicurarvi di non essere la prossima vittima di un attacco. La lista di controllo disponibile sul nostro sito Web può essere utile per scongiurare una sottrazione di dati.

Informazioni sulla sicurezza IT per le PMI:

https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/checklist-per-siti-web-pmi.html

Portale della Confederazione per le PMI:

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

5.3 Sistemi di controllo industriali (ICS)

Il problema dell'Internet delle cose viene esaminato da vicino nel capitolo consacrato al tema principale del presente rapporto semestrale. Già da tempo vengono utilizzati oggetti tecnologici connessi alla rete. Sensori e attori vengono coordinati, automatizzati e ottimizzati per mezzo di comandi centralizzati. Questi comandi controllano reti elettriche, flussi di traffico, impianti di climatizzazione degli edifici o apparecchiature tecniche di medicina negli ospedali.

5.3.1 Déjà vu a Kiev: nuovo blackout elettrico in Ucraina

A quasi un anno di distanza dal blackout che aveva colpito alcune parti dell'Ucraina a fine 2015, in merito al quale si era riferito nel penultimo rapporto semestrale[47], la zona a nord di Kiev è di nuovo precipitata nel buio. Anche stavolta appena prima di Natale, per la precisione sabato 17 dicembre 2016, poco prima che scoccasse la mezzanotte, i clienti della società elettrica statale Ukrenergo approvvigionati dalla sottostazione Pivnichna sono rimasti per circa un'ora senza corrente[48]. Ukrenergo ha informato i suoi clienti di non sapere se il blackout fosse dovuto a un guasto a qualche componente o a un attacco hacker. Qualche settimana dopo Oleksandr Tkachuk, capo di stato maggiore dei servizi di sicurezza ucraini, ha annunciato che sia il nuovo blackout sia gli attacchi al sistema finanziario e ad altre infrastrutture erano stati orchestrati dai servizi di sicurezza russi in collaborazione con fornitori di software privati e cybercriminali[49]. Stando alle dichiarazioni di Tkachuk, gli attacchi in questione erano stati concepiti dalle stesse persone già coinvolte in precedenti attacchi a mezzo del malware BlackEnergy. Ad oggi tali affermazioni non sono ancora state verificate da specialisti indipendenti. Sinora le accuse sono state sostenute soltanto da ricercatori ucraini attivi nel settore della sicurezza appartenenti alle organizzazioni «Information Systems Security Partners (ISSB)» e «Honeywell Cyber Security Labs», durante una relazione tenuta nell'ambito della conferenza «S4 2017» consacrata alla sicurezza dei sistemi di informazione e comunicazione[50]. Stando alle loro dichiarazioni, questi specialisti avrebbero partecipato all'inchiesta sull'incidente in questione. Secondo quanto affermato stavolta le unità di controllo telecomandate (RTUs) non sarebbero state rese inutilizzabili sovrascrivendo il firmware. Nell'ultimo attacco infatti sarebbero state semplicemente disattivate a distanza, di conseguenta anche il ripristino dell'approvvigionamento energetico si è svolto in tempi più brevi. Secondo i ricercatori, i criminali avrebbero potuto causare danni molto più ingenti. In questo senso l'attacco non puntava a causare il massimo danno possibile, elemento che induce a presumere che si sia trattato piuttosto di una dimostrazione di potere da parte dei sabotatori.

Gli obiettivi dell'attacco sono stati infiltrati da software maligno attraverso una massiccia campagna di e-mail nel luglio del 2016. Dopodiché gli aggressori sono rimasti per vari mesi nella rete allo scopo di analizzarla e di prepararsi ad attaccare le apparecchiature bersaglio. Oltre alla società di approvvigionamento elettrico sono caduti vittima di questo attacco anche

---

47 Rapporto semestrale MELANI 2015/2: https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2015-2.html (stato: 28.2.2017)

48 https://motherboard.vice.com/en_us/article/ukrainian-power-station-hacking-december-2016-report (stato: 28.2.2017)

49 http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN15U2CN (stato: 28.2.2017)

50 https://www.youtube.com/watch?v=lTwsDLO3C44 (stato: 28.2.2017)

il ministero delle finanze, la tesoreria e il fondo pensionistico statale dell'Ucraina. Il 6 dicembre 2016 è stato sferrato contro questi obiettivi un attacco DDoS e contemporaneamente sono state danneggiate componenti interne alla rete e delle banche dati sono andate distrutte. L'incidente ha causato un'interruzione e ritardi nel traffico statale dei pagamenti.

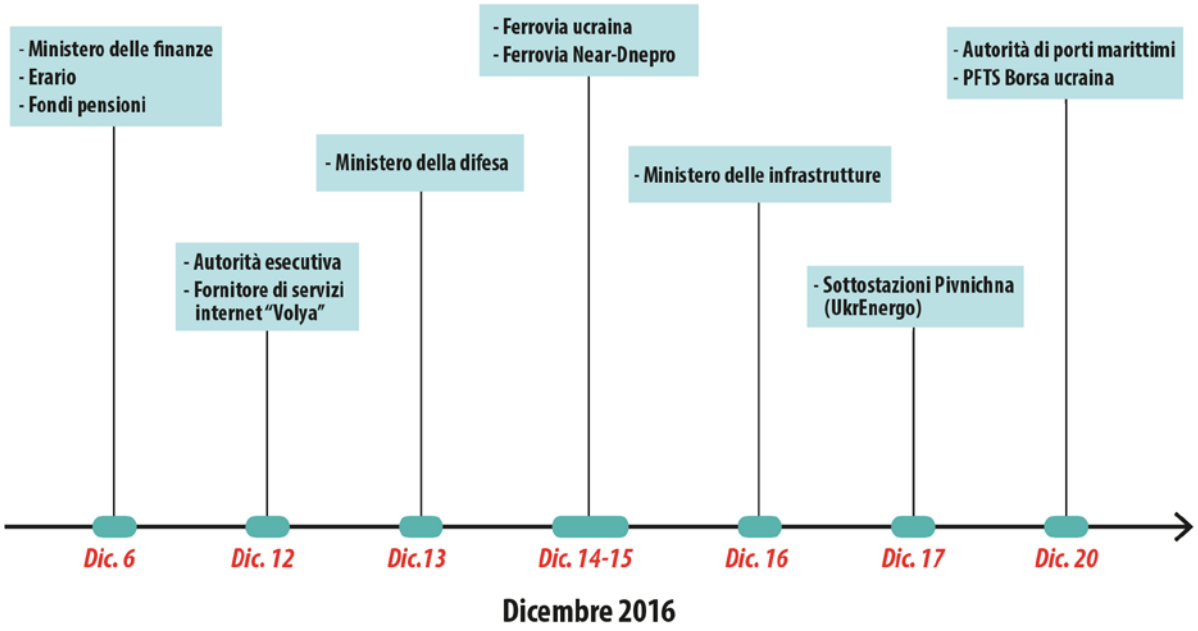

Figura 7: I vari attacchi in ordine cronologico (fonte: S4 Events)

Il 14 dicembre 2016 i sabotatori hanno preso di mira anche l'amministrazione delle ferrovie statali ucraine. Anche stavolta, per distogliere l'attenzione hanno sferrato un attacco DDoS ai danni della biglietteria online. Nel frattempo hanno manipolato la gestione automatizzata dei trasporti dei treni merci. I ricercatori vedono dei paralleli con l'attacco del 2015 sulla base di osservazioni riguardanti le strategie utilizzate dai sabotatori per espandersi nelle reti infiltrate. Essi hanno constatato dei progressi analizzando i macrovirus contenuti negli attacchi mirati sferrati via e-mail. Rispetto alle semplici macro del 2015, i codici responsabili del funzionamento in senso stretto rappresentavano ormai soltanto l'1 per cento del totale. Il 30 per cento delle righe programmate servivano a ostacolare l'analisi delle macro e il rimanente 69 per cento soltanto a nascondere la malignità del malware.

I ricercatori coinvolti hanno avuto l'impressione che l'Ucraina fosse sfruttata dagli avversari come terreno d'addestramento per questo tipo di cyberattacchi allo scopo di mettere alla prova le proprie capacità offensive. Essi hanno fatto sapere che occorreranno ancora alcuni mesi per un'analisi approfondita dell'incidente. Fino a quel momento i risultati raccolti non potranno essere verificate da specialisti indipendenti.

Nel contesto dei sistemi di controllo industriali, occorre essere prudenti, principalmente per quanto riguarda i nascenti allarmismi legati a scoperte clamorose di attacchi. Questa affermazione proviene da Robert M. Lee, il quale ha potuto partecipare all'analisi dell'incidente del 2015. Se vengono applicate in modo coerente opportune misure di protezione, è possibile scoprire e impedire attacchi temibili anche nelle possibili conseguenze. La ditta specializzata in cybersicurezza SentinelOne, ad esempio, si è vista costretta a pubblicare una rettifica

riguardo a una delle sue analisi di malware dopo che sulla base di tale analisi erano state diffuse notizie su attacchi statali contro il settore energetico negli Stati Uniti. L'unico indizio consisteva nel fatto che su uno dei sistemi presi di mira fosse attivo anche un sistema di gestione dell'energia. Tuttavia, il malware stesso non presentava caratteristiche che mirassero in modo specifico ai sistemi di controllo.

5.3.2 Distributed Denial of Heating: abitanti al gelo dopo l'attacco DDoS

Nella città di Lappeenranta, situata nella parte orientale della Finlandia, gli abitanti di due edifici si sono ritrovati per un certo tempo senza riscaldamento e acqua calda. Il guasto è stato causato da un attacco DDoS che ha messo fuori uso il sistema generale di comando della domotica dell'edificio[51]. Il sistema tentava di riavviarsi per ripristinare il funzionamento e respingere gli attacchi ma è rimasto coinvolto in un circolo vizioso e il riscaldamento è rimasto spento. I sistemi di comando della domotica finlandesi erano finiti nel mirino di gestori di reti botnet in cerca di apparecchiature configurate in modo poco sicuro o contenenti falle. Il riscaldamento è stato infine rimesso in funzione frenando il traffico di dati ai livelli superiori della rete, respingendo in questo modo l'attacco DDoS. Il fabbricante del sistema ha dichiarato che nel Paese nello stesso periodo sono stati osservati diversi attacchi di questo tipo.

I sistemi potrebbero essere gestiti in modo sicuro se fossero compartimentati come raccomandato. Ma per comodità e per semplificare l'interfaccia utente, essi vengono regolarmente connessi a Internet.

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).

Liste di controllo e guide: Misure di protezione dei sistemi industriali di controllo (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

[51] http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter (stato: 28.2.2017)

5.4 Attacchi

5.4.1 Avaria di Internet colpisce 900 000 clienti della Deutsche Telekom

Il 27 novembre 2016 è stato sferrato un attacco globale a un gran numero di router di reti domestiche. In Germania l'attacco ha mandato in avaria i collegamenti Internet di 900 000 clienti di Telekom. L'avaria è stata provocata dall'impiego di una nuova versione del malware Mirai, già utilizzato il 21 ottobre 2016 per l'attacco ai server DNS della società Dyn[52]. Mirai è un malware che colpisce il sistema operativo Linux, utilizzato soprattutto in apparecchiature dell'Internet delle cose. Nell'attacco del 27 novembre, Mirai ha cercato nei router delle reti domestiche di clienti finali una falla per installare il malware. Siccome i router delle reti domestiche della Deutsche Telekom hanno un sistema operativo proprietario, il tentativo di installazione del malware è fallito. I ripetuti tentativi di attacco hanno però mandato in tilt le apparecchiature. Deutsche Telekom ha messo a disposizione dei suoi clienti un aggiornamento del software.

5.4.2 Attacchi che prendono di mira le transazioni finanziarie

Nel periodo in rassegna vi sono stati diversi casi di dirottamento di transazioni finanziarie saliti alla ribalta dei media internazionali. I casi che presentiamo testimoniano la grande diversità delle potenziali vittime. Il 6 novembre, la banca britannica TESCO Bank annunciava la manomissione di quasi 40 000 conti, con perdite finanziarie per circa la metà di essi. Ciò ha costretto la banca ad adottare misure urgenti e a bloccare le transazioni finanziarie. Alcuni mesi dopo, il modus operandi esatto degli attaccanti non era stato ancora chiarito. La comunicazione lacunosa della banca è stata del resto oggetto di critiche in Gran Bretagna, malgrado l'impegno da parte della banca a rimborsare i clienti colpiti. Non si può affatto escludere che l'incidente abbia conseguenze finanziarie per l'istituto. L'autorità di regolamentazione del settore finanziario ha infatti la possibilità di comminare una multa in base alla responsabilità della banca nell'incidente.

Oltre agli attacchi volti a compromettere direttamente i sistemi delle banche prendendo di mira in particolare il sistema di pagamento SWIFT[53] , anche i bancomat sono un obiettivo possibile per i cybercriminali. In agosto, una serie di attacchi ha permesso di sottrarre 12 millioni di bath (corrispondenti a CHF 343'000) in Tailandia. Il fornitore di servizi di sicurezza FireEye attribuisce questo attacco a un malware da esso analizzato e denominato Ripper[54], che una volta installato sul sistema del bancomat i criminali devono farlo interagire con una carta chip falsificata. Ciò dimostra il notevole grado di organizzazione dei criminali nella manomissione dei macchinari nonché la capacità di produrre le carte per accedere fisicamente al bancomat. In novembre, l'impresa di sicurezza Group-IB ha pubblicato un rapporto concernente un gruppo di criminali denominato Cobalt, ritenuto responsabile di una serie di inci-

---

[52] Vedi il fulcro del capitolo 3

[53] Cfr. in particolare il rapporto semestrale 2016/1, capitolo 5.4.1 «Cyber-rapinatori di banche rubano 81 milioni di dollari americani» https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2016-1.html (stato: 28.2.2017)

[54] https://www.fireeye.com/blog/threat-research/2016/08/ripper_atm_malwarea.html (stato: 28.2.2017)

denti in Europa che avrebbero permesso ai criminali di prelevare denaro direttamente dai bancomat, dopo aver compromesso i sistemi di diverse banche[55]. La peculiarità di questi casi consisterebbe nell'assenza di manipolazione fisica dei bancomat.

Attacchi sono sferrati anche contro le nuove forme di moneta digitale, come abbiamo già riportato nei rapporti precedenti[56]. Nel periodo in rassegna, la piatttaforma di scambio Bitfinex è stata oggetto di un pirataggio consistente risultato nella sottrazione di 120 000 bitcoins, che al cambio attuale (febbraio 2017) equivalgono a oltre 130 milioni di franchi svizzeri. Gli autori hanno dovuto compromettere il sistema di firma multipla installato presso i clienti di Bitfinex. L'impatto del furto sui mercati è stato importante con una perdita del corso del bitcoin del 13 per cento in due giorni dopo l'annuncio dell'incidente.

Infine, Carbanak, che era stato al centro dell'attenzione per i suoi pesanti attacchi contro le banche nel 2015[57], conferma la sua intenzione di diversificare. Secondo i ricercatori dell'impresa Trustwave[58], il settore alberghiero é stato vittima di attacchi spear phishing con ampio ricorso all'ingegneria sociale e finalizzati a rubare dati di carte di credito dopo aver compromesso terminali di punti vendita.

Conclusione

Gli sviluppi di questi ultimi anni dimostrano che l'utente non è l'unico potenziale punto debole della catena dei sistemi di pagamento. Le banche stesse vengono direttamente colpite attraverso i loro sistemi interni o i loro bancomat. Peraltro, i cybercriminali sono molto interessati anche alle nuove monete accumulate solo in forma digitale.

5.4.3 Un mercato dei ransonware molto frammentato

Come abbiamo già rilevato nel capitolo dedicato a questo tema nella parte «Svizzera», il settore dei ransomware ha conosciuto un importasnte periodo di attività anche nella seconda parte dell'anno. I numerosi incidenti internazionali testimoniano la grande diversità di attacchi, di obiettivi e di modus operandi. Abbiamo già evidenziato la logica imprenditoriale dei criminali nel nostro rapporto precedente. Essi migliorano i loro prodotti, cercano nuovi sbocchi e si prendono persino cura dei loro clienti (le vittime) tramite ad esempio FAQs[59] o la possibilità di dialogare direttamente con gli operatori del ransomware. Il mercato dei ransomware sembra attraversare una fase di consolidamento, con molti gruppi, obiettivi e mo-

55 http://www.reuters.com/article/us-cyber-banks-atms-idUSKBN13G24Q (stato: 28.2.2017)

56 Cfr. rapporto semestrale 2014/1, capitolo 4.10 «Attacchi alle monete virtuali» https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2014-1.html (stato: 28.2.2017)

57 Cfr. rapporto semestrale 2015/1, capitolo 5.1.2 «Carbanak – la rapina in banca elettronica» https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2015-1.html (stato: 28.2.2017)

58 https://www.trustwave.com/Resources/SpiderLabs-Blog/New-Carbanak-/-Anunak-Attack-Methodology/ (stato: 28.2.2017)

59 Elenco delle risposte a domande poste dalla vittima, che figurano nel messaggio di ricatto.

dus operandi assai variati. La situazione appare invece del tutto diversa in altri settori dell'attività cybercriminale, ad esempio in quello del cavalli di Troia bancari, dove alcuni marchi ben affermati fanno la parte del leone.

Uno dei casi eclatanti è quello che ha colpito la rete dei trasporti pubblici di San Francisco. Il 25 novembre 2016, un attacco ha paralizzato la biglietteria e costretto la società ad annunciare la gratuità dei servizi fino al ripristino dei sistemi per mezzo di barriere. L'aggressore ha inoltre affermato di essere entrato in possesso dei dati sensibili, ma la società lo ha smentito.

Alcuni giorni dopo, nuove rivelazioni[60] hanno permesso di tracciare un profilo più preciso dell'aggressore, apparentemente responsabile anche di altri attacchi simili. Egli non avrebbe però puntato ai trasporti pubblici di San Francisco quale obiettivo preciso, ma soltanto cercato in modo automatico sistemi vulnerabili.

Conclusione

L'esempio dimostra che, anche quando non prende di mira direttamente sistemi di burotica, come sembra fare in questo caso,, un attacco può avere effetti a catena e provocare danni molto concreti. Infatti la problematica non si limita alla possibilità o meno di ripristinare l'integrità dei sistemi, va anche tenuto conto del tempo necessario a effettuare quest'operazione. Infatti durante questa fase d'impasse, si dovrà ricorrere a soluzioni provvisorie atte a gestire la crisi.

5.5 Vulnerabilità

Oltre alle numerose vulnerabilità rese note anche nel secondo semestre 2016, il presente rapporto mette in luce tre lacune che illustrano in modo esemplare la vulnerabilità dei nostri sistemi e programmi in altrettanti ambiti diversi.

5.5.1 Vulnerabilità nell'interfaccia USB

Tutti sanno che inserendo una pennetta USB altrui nel proprio computer si corre un certo rischio, e che sarebbe meglio astenersene. E ciò, nonostante i sistemi operativi siano ormai impostati in modo da non eseguire più automaticamente i file presenti su queste chiavette e chiedano dapprima all'utente quale azione debbano compiere. Infatti se proprio questo elemento di sicurezza dovesse essere annientato, che cosa succederebbe? Come spiega l'esperto di sicurezza Samy Kamkar nel suo blog[61], l'inserimento di un dispositivo USB da lui appositamente predisposto può spalancare le porte all'installazione di malware. Questo sistema funziona anche se il computer è bloccato. Il software sviluppato dall'esperto si presenta all'interfaccia USB come dispositivo Ethernet, simulando in tal modo un collegamento Internet tramite USB. In questo modo è possibile non solo catturare i cookie e intercettare il

60 https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked/ (stato: 28.2.2017)

61 https://samy.pl/poisontap/ (stato: 28.2.2017)

traffico Internet, ma anche installare in modo permanente una porta di servizio. L'unica condizione per la riuscita dell'attacco è che sul computer attaccato sia installato un browser.

Conclusione / Raccomandazione

Quante volte avete lasciato incustodito il vostro computer, a una conferenza, in biblioteca o al bar, durante la pausa di mezzogiorno o per andare alla toilette? Per un aggressore, queste sarebbero occasioni d'oro per compiere tentativi di spionaggio mirati. Come contromisura non bisogna mai lasciare incustodito il computer, oppure disattivate sia le interfacce USB sia le altre.

5.5.2 Password manager: una vulnerabilità cruciale?

Sull'uso dei password manager e sulla loro sicurezza si discute molto. C'è chi ha grande fiducia in questi strumenti, poiché permettono di utilizzare password sicurissime, lunghe e complesse. Alcuni programmi ricordano addirittura che una password e scaduta e occorre cambiarla o propongono una password sicura. L'unica cosa da tenere a mente è la master password. E proprio su questo punto intervengono gli scettici: se un aggressore riuscisse infatti a rubare la banca dati o a decifrare la master password, potrebbe accedere in un colpo solo a tutte le altre. Si tratta insomma di una potenziale miniera d'oro per i criminali. Ancora peggio sarebbe se una di queste casseforti delle password contenesse una falla. E proprio una falla di questo tipo è stata individuata a fine luglio 2016 nel plug-in Firefox del programma «LastPass». Sembra che si potesse accedere alle password visitando un sito web appositamente predisposto.[62] La falla è stata sanata.

5.5.3 Masque Attack nell'iOS

I cosiddetti Masque Attack, apparsi per la prima volta nel 2014, consentono agli hacker di sostituire app originali dell'App Store di Apple con app manipolate recanti la firma aziendale con lo stesso Bundle Identifier[63]. I criminali possono così creare contenuti maligni con lo stesso Bundle ID dell'originale. Se l'originale è popolare aumenta naturalmente anche la portata dell'attacco e la probabilità che gli utenti scarichino la versione manipolata. È vero che Apple ha chiuso le falle di sicurezza responsabili del problema, ma Trendmicro ha comunque rilevato ancora numerose app manipolate[64]. La causa del problema è stata infine illustrata in un rapporto pubblicato nel novembre 2016. I criminali sfruttavano una funzione nel processo di generazione della firma digitale che consentiva di ereditare i dati. Apple ha poi risolto il problema nel iOS 10. I dispositivi su cui è installato iOS 9.3.5 o una versione precedente sono però tuttora attaccabili.

---

62 https://blog.lastpass.com/2016/07/lastpass-security-updates.html/ (stato: 28.2.2017)

63 Bundle Identifier è un'espressione per l'identificazione, che viene definita e manenuta durante lo sviluppo di un'App, di norma nella forma com.your-company.app-name.

64 http://blog.trendmicro.de/masque-attack-missbraucht-das-code-signing-in-ios-fuer-faelschungen/ (stato: 28.2.2017)

5.6 Misure preventive

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

5.6.1 Rete Avalanche: arresti e perquisizioni

Dal 2009 alcuni hacker hanno utilizzato la rete criminale internazionale denominata Avalanche per compiere attacchi malware, phishing e spam. Inviavano a vittime ignare e-mail con allegati o link dannosi, al ritmo di più di un milione a settimana. La rete Avalanche è stata anche utilizzata come piattaforma di distribuzione per dirigere attacchi di massa globali e reclutare corrieri di denaro. Il danno totale causato a livello globale è stimato a svariate centinaia di milioni di euro, benché il danno effettivo sia difficile da valutare, dato che attraverso questo portale venivano amministrate diverse famiglie di malware. Le indagini sulla piattaforma sono iniziate nel 2012. Il 30 novembre 2016 l'infrastruttura è stata finalmente smantellata. Alla disattivazione della piattaforma hanno partecipato investigatori di 30 Paesi. Sono state arrestate 5 persone, effettuate 37 perquisizioni domiciliari e sequestrati 39 server. Le autorità di perseguimento penale hanno individuato vittime in 180 Paesi. 221 server sono stati spenti dopo aver informato i rispettivi provider, pregandoli di effettuare un take down[65].

Conclusione

L'esempio dimostra che le autorità di perseguimento penale riescono a procedere con successo contro la criminalità in Internet soprattutto quando collaborano a livello internazionale coinvolgendo anche ditte private.

5.7 Altri temi

5.7.1 Fine della vigilanza statunitense sulla gestione globale degli indirizzi Internet

Il 30 settembre 2016 ha segnato la fine dello storico ruolo di vigilanza esercitato dagli Stati Uniti sull'ente che gestisce gli indirizzi Internet a livello globale (ICANN).[66] Da allora la gestione globale degli indirizzi Internet sottostà alla vigilanza di una comunità globale in cui sono rappresentati tutti i gruppi d'interesse (stakeholder). Si è così compiuto un passo importante verso una gestione globale, multi-stakeholder, del sistema dei nomi di dominio e degli indirizzi IP (DNS).

---

65 http://www.staatsanwaltschaften.niedersachsen.de/download/113197 (stato: 28.2.2017)

66 https://www.bakom.admin.ch/bakom/it/pagina-iniziale/l-ufcom/informazioni-dell-ufcom/ufcom-infomailing/ufcom-infomailing-43/gli-stati-uniti-cedono-la-vigilanza-sull-icann.html, https://digitalwatch.giplatform.org/processes/iana (stato: 28.2.2017)

In virtù del cosiddetto «Contratto IANA»[67] tra il governo statunitense e l'ICANN, gli Stati Uniti esercitavano sin dal 1998 l'alta vigilanza sulla gestione del sistema DNS. In tal senso, esercitavano una funzione di verifica e convalida per le modifiche della banca dati centrale di tutti i domini top level (ad es. .swiss, .com o codici di nazione come .ch). Il Contratto IANA è scaduto a fine settembre 2016 e non è più stato rinnovato[68].

Il nuovo quadro istituzionale, inteso a garantire una vigilanza globale e più democratica su Internet, accorda alle sottounità dell'ICANN (incluso il Comitato consultivo governativo GAC, in seno al quale la Svizzera è rappresentata dall'UFCOM) determinati poteri di controllo sul consiglio d'amministrazione (ICANN Board): blocco del preventivo, approvazione di modifiche degli statuti, destituzione del consiglio d'amministrazione o di suoi singoli membri.

L'ICANN ha ancora sede in California e quindi sottostà essenzialmente al diritto statunitense e alle possibilità di intervento delle autorità americane. Ciò nonostante, il passo compiuto rappresenta un'importante svolta nella trasformazione dell'ICANN in un'istituzione globale. Ma per rafforzare la sua diversità e garantire la considerazione delle necessità e degli interessi della comunità globale saranno necessari altri passi, per la realizzazione dei quali l'UFCOM, come pure altri stakeholder svizzeri, fornisce suggerimenti e appoggio.

Gli internauti non dovrebbero aver notato granché di questo cambiamento, poiché la transizione avvenuta non ha modificato il funzionamento tecnico corrente del sistema DNS.

5.7.2 Il gestore di punti di interscambio Internet DE-CIX chiede l'esame giudiziale delle misure di sorveglianza

La società DE-CIX, che gestisce il punto di interscambio Internet di Francoforte, ha denunciato la Repubblica federale tedesca presso la Corte amministrativa di Lipsia[69], chiedendo l'esame giudiziale della prassi applicata dai servizi d'informazione tedeschi («Bundesnachrichtendienst», BND) in materia di sorveglianza delle telecomunicazioni.

La denuncia si basa in particolare su una perizia[70] di Hans-Jürgen Papier, professore di diritto ed ex presidente della Corte costituzionale tedesca, il quale solleva importanti dubbi sulla legalità della prassi attuale e sostiene che il segreto delle telecomunicazioni debba essere considerato come diritto dell'uomo. Per questo il diritto in questione deve essere riconosciuto anche agli stranieri e ogni sua restrizione deve essere correttamente prevista da una legge in senso formale. Il governo tedesco sostiene invece che per sorvegliare dati esclusivamente di provenienza estera non sia necessaria una legge.

---

67 https://www.ntia.doc.gov/files/ntia/publications/ianacontract.pdf; https://www.icann.org/en/system/files/files/contract-01oct12-en.pdf (stato: 28.2.2017)

68 https://www.icann.org/news/announcement-2016-10-01-en (stato: 28.2.2017)

69 https://www.de-cix.net/de/about-de-cix/media-center/press-releases/information-on-the-lawsuit-against-the-federal-republic-of-germany (stato: 28.2.2017)

70 http://rsw.beck.de/rsw/upload/NVwZ/NVwZ-Extra_2016_15.pdf; https://netzpolitik.org/2016/ex-praesident-des-bundesverfassungsgerichts-bnd-zugriff-auf-internet-knoten-wie-de-cix-ist-insgesamt-rechtswidrig/ (stato: 28.2.2017)

In Svizzera la legge federale sulle attività informative ha fornito la base legale formale necessaria per l'esplorazione di segnali via cavo di telecomunicazioni estere. Qualsiasi misura a questo riguardo deve essere non solo preventivamente autorizzata dal capo del Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS), ma anche approvata dal Tribunale amministrativo federale, e in quanto a ciò soggiace dunque non solo a un controllo politico, ma anche al controllo di un giudice indipendente.

6 Tendenze e prospettive

6.1 Cybercrime as a service e cyberestorsione: un circolo vizioso

Il Cybercrime as a service è costituito da una gamma di offerte commerciali per l'acquisto degli strumenti utili per un attacco informatico senza grandi conoscenze tecniche, ad esempio l'utilizzo di diversi malware, il noleggio di una botnet, il lancio di un attacco DDoS o un servizio di riciclaggio di denaro. Il fenomeno non è nuovo: servizi cybercriminali erano già disponibili da tempo in forum underground, ma erano riservati, per la maggioranza, a gruppi di criminali informatici, che garantivano una divisione del lavoro e una grande efficienza. Un'organizzazione siffatta permette agli attori di specializzarsi, perfezionando competenze specifiche da vendere o da scambiare.

Con il boom della cyberestorsione la situazione è evoluta. Un serie di offerte ha alimentato il l'apertura del mercato dell'attacco informatico come prodotto. Prendiamo l'esempio degli attacchi distributed denial of service (DDoS) sferrati per costringere la vittima a un pagamento in bitcoins: attualmente chiunque o quasi può acquisire l'uso di uno Stresser/Booter[71] per sferrare un attacco DDoS. Basta scegliere la vittima e una formula di attacco, con prezzo ed efficacia variabili. È possibile acquistare anche l'utilizzo di una botnet di apparecchi interconnessi compromessi dal malware Mirai. La situazione è analoga nel campo dei ransomware, che possono essere acquistati chiavi in mano e attivati anche da persone senza particolari conoscenze di informatica.

Di fronte a tale situazione, la domanda circa la dinamica propria di questo mercato è la seguente: è la forte richiesta di questi servizi a indurre i cybercriminali a produrre una gamma di strumenti su misura? Oppure è l'offerta che ne ha incentivato l'uso da parte di molti autori?

In realtà si verificano entrambe le cose. La situazione sembra essere caratterizzata da un circolo vizioso. Per capire la dinamica in atto occorre capire come mai la cyberestorsione è divenuta popolare per così tanti autori. Come abbiamo già evocato, questo tipo di attacchi genera grandi somme di denaro e permette un processo di cashout molto facilitato[72]: un pagamento in bitcoin è inviato direttamente dalla vittima e può essere «lavato» e reso intracciabile tramite un servizio di bitcoin mixing. Inoltre, la ricerca di vittime è molto facile dato che il loro numero è potenzialmente illimitato. Infine, questo tipo di attacco è stato mediatizzato in un modo senza precedenti: molte vittime sono note e le «success story» criminali vengono

[71] Offerte di «DDoS as a service», possono essere noleggiate e proposte come apparentemente legittime, offrendo il servizio quale stress test di un servizio in linea.

[72] Fa riferimento al passaggio tra l'atto criminale e i contanti utilizzabili.

diffuse ad ampio raggio, mentre gli arresti di criminali sembrano rarefarsi alimentando un sentimento d'impunità. Di conseguenza l'effetto incentivante è molto forte: numerosi autori potenziali nello spazio reale , generalmente provenienti dalla piccola criminalità, provano a fare fortuna nello spazio virtuale. La domanda c'è, l'offerta segue naturalmente e il mercato vi si adegua proponendo una gamma di servizi facilmente utilizzabili per ogni tipo di autore. DaL'offerta su misura e la sua estrema accessibilità stimolano il mercato permettendo a molti autori di esercitare queste attività.

Gli ideatori di queste offerte sono naturalmente il nocciolo del problema; nonostante il numero sia relativamente limitato – da 100 a 200 nel 2015 secondo Andy Archibald, direttore della National Crime Agency (UK) – l'effetto moltiplicatore notevole.[73] Tale apertura, il numero di autori e di prodotti nonché il forte sviluppo di queste attività rendono molto difficile il controllo delle attività cybercriminali e il lavoro delle autorità penali.

6.2 Futura impostazione dell'autenticazione a due o più fattori

Nel luglio del 2016[74], il «National Institute of Standards and Technology (NIST)» americano ha annunciato che in futuro non avrebbe più raccomandato l'autenticazione tramite SMS nelle proprie direttive sulle identità digitali ma che l'avrebbe addirittura sconsigliata. Se in molti luoghi si insiste ancora per convincere gli internauti a utilizzare sistematicamente l'autenticazione a due fattori, il fattore SMS, il più popolare e semplice da utilizzare, è già considerato inidoneo.

Per poter accedere in modo sicuro a servizi Internet come l'e-banking viene utilizzato, oltre alla password, almeno un secondo meccanismo di autenticazione. Idealmente, questo secondo meccanismo passa attraverso un secondo canale di comunicazione indipendente, spesso appunto tramite un SMS sul telefono cellulare. Ma oggi la maggior parte dei cellulari è costituita da smartphone, ossia da piccoli computer che, in quanto tali, possono essere infettati da malware in grado, in particolare, di intercettare i messaggi trasmettendoli ai truffatori. Inoltre oggi le operazioni bancarie vengono spesso effettuate direttamente tramite smartphone, sicché il login e la seconda autenticazione avvengono tramite lo stesso dispositivo. Questa circostanza vanifica la sicurezza supplementare che dovrebbe essere garantita dalla password unica inviata per SMS.

Ma l'insufficiente sicurezza dei dispositivi finali non è la sola minaccia che pesa sul secondo fattore SMS: queste informazioni possono essere intercettate o dirottate anche a livello della rete. I ricercatori nel campo della sicurezza hanno avvertito già anni fa dei problemi di sicurezza posti dal protocollo SS7[75], che consente tra l'altro il roaming tra i vari operatori di reti mobili. All'estero i telefoni cellulari possono collegarsi a reti estere; il gestore di rete estero annuncia l'operazione nella rete del Paese d'origine dell'abbonato, la quale in seguito trasmette alla rete estera le chiamate e i messaggi SMS da recapitare. Questa operazione può essere simulata senza che il telefono cellulare si trovi effettivamente all'estero. In tal caso i

---

73 https://www.connectinternetsolutions.com/cyber-crime/ (stato: 28.2.2017)

74 https://pages.nist.gov/800-63-3/sp800-63b.html (stato: 28.2.2017)

75 https://www.blackhat.com/presentations/bh-europe-07/Langlois/Presentation/bh-eu-07-langlois-ppt-apr19.pdf (stato: 28.2.2017)

messaggi SMS vengono dunque trasmessi a gestori di rete all'estero, dove possono essere intercettati. L'intercettazione è possibile perché il protocollo SS7 con cui vengono gestite le comunicazioni è stato originariamente concepito come protocollo aperto, quando ancora era data per scontata una fiducia di base tra tutti i provider di telecomunicazioni mobili. Ma nel frattempo, con l'aumento del numero di operatori nel mondo intero, è ormai possibile che alcune aziende non si attengano a tutte le regole e in determinate circostanze non possano impedire attività fraudolente o addirittura collaborino con i truffatori.

Su un piano meno tecnico, potrebbero verificarsi episodi di complicità in operazioni di ingegneria sociale. In un caso concreto, i truffatori hanno convinto alcuni collaboratori compiacenti del servizio clienti di un fornitore di servizi di telecomunicazione a inviare una carta SIM sostitutiva a un indirizzo accessibile agli autori[76], che ha permesso loro di impossessarsi di una serie di conti online.

L'autenticazione a più fattori poggia su almeno due componenti. Queste componenti possono basarsi sulla conoscenza (ad es. di una password), sul possesso (ad es. una carta magnetica) oppure su una caratteristica unica (ad es. un'impronta digitale). A causa della crescente fusione tra telefono e computer e della concentrazione delle reti di comunicazione, la rete mobile non può più essere considerata un canale di comunicazione a sé stante e indipendente da Internet. Così, il messaggio SMS soddisfa ormai soltanto in parte la componente «possesso». Di conseguenza, occorrerebbe possibilmente passare ad altri metodi di autenticazione per i servizi online, in special modo per servizi con grande potenziale di danneggiamento. Un metodo esemplare di autenticazione sicura basata sul cellulare è rappresentato, in caso di corretto utilizzo, dalle applicazioni smartphone che decifrano una password unica codificata dal fornitore di servizi. Un'altra alternativa è rappresentata dai sistemi Mobile ID, nei quali le caratteristiche di autenticazione vengono già codificate nella carta SIM. Siccome i servizi vengono sempre più spesso utilizzati direttamente sullo smartphone, per l'autenticazione è consigliabile ricorrere a elementi indipendenti come le chiavi di sicurezza fisiche separate, il cui impiego viene già offerto da molti grandi servizi web[77].

Conclusione

Se il vostro servizio online dovesse ancora ricorrere agli SMS per l'autenticazione o la reimpostazione della password, non vi è motivo di andare in panico. Anche se questo metodo presenta ormai qualche vulnerabilità e non è più la variante più sicura, l'impiego di due o più fattori garantisce sempre una sicurezza moltiplicata rispetto a una protezione basata soltanto su nome utente e password.

6.3 Tecnologie della sicurezza costantemente sotto pressione

Per incrementare la sicurezza, oltre ai comuni prodotti quali gli scanner antivirus, le tecniche di micro virtualizzazione e i sistemi di identificazione/prevenzione di accessi non autorizzati,

[76] http://www.forbes.com/sites/laurashin/2016/12/20/hackers-have-stolen-millions-of-dollars-in-bitcoin-using-only-phone-numbers/#42981a5c22db (stato: 28.2.2017)

[77] http://fc16.ifca.ai/preproceedings/25_Lang.pdf (stato: 28.2.2017)

vengono spesso impiegate funzionalità di Windows quali «AppLocker» e «EMET»[78]. Questi due programmi aumentano la sicurezza dei sistemi Windows in modo determinante. «AppLocker» consente di definire esattamente in quali directory possono essere eseguiti certi programmi, rendendo più difficile per gli eventuali aggressori riuscire a mettere a segno un'infezione iniziale. «EMET» ostacola invece l'esecuzione di exploit.

I programmatori di malware tentano ovviamente di aggirare questi meccanismi di protezione. Questo dato di fatto non è una novità, ed è già stato ripetutamente descritto[79,80], ma dallo scorso autunno si registra un netto aumento di questo tipo di attacchi. I criminali inseriscono ad esempio in documenti office codici macro che contengono uno script PowerShell. In questi casi l'aggressore approfitta del fatto che gli script PowerShell sono ammessi nella maggior parte degli ambienti. Altri metodi si avvalgono di regsvr32 e di scriptlets per ottenere lo stesso risultato. L'Exploit-Kit Angler ha inoltre acquisito la capacità di avviare gli exploit in modo da annientare l'effetto protettivo di EMET. I criminali fanno leva sulle routine per l'allocazione della memoria che fanno parte direttamente dei programmi attaccati (ad es. Flash)[81].

Conclusione / raccomandazione

L'impiego delle nuove tecnologie della sicurezza è sempre più frequente e permette di proteggersi efficacemente contro molti dei vettori di attacco sinora conosciuti. Ma i pirati informatici hanno i mezzi e la volontà necessari per cercare (e scoprire) il modo di aggirare ogni nuovo meccanismo di sicurezza. Ciò nonostante, l'impiego di questi meccanismi di sicurezza è ancora sensato, poiché essi rendono la vita difficile ai criminali e sono ancora in grado di rendere inoffensivi molti dei vettori di attacco attualmente utilizzati. Tuttavia, raccomandiamo di tenere d'occhio attentamente le possibilità offerte agli aggressori da PowerShell e di introdurre ad esempio le opportune misure di sicurezza, quali una firma digitale per tutti gli script e le macro. Esistono anche svariati Behaviour Blocking Engine in grado di riconoscere perlomeno in parte simili attacchi. Anche Microsoft ha introdotto nel DeviceGuard di Windows 10 ulteriori funzioni che ostacolano questo tipo di attacco.

[78] Il toolkit Microsoft Enhanced Mitigation Experience (EMET) comprende in particolare le funzioni «Address Space Layout Randomization (ASLR)» e «Data Execution Prevention (DEP)».

[79] http://subt0x10.blogspot.ch/2016/04/bypass-application-whitelisting-script.html (stato: 28.2.2017)

[80] http://leastprivilege.blogspot.ch/2013/04/bypass-applocker-by-loading-dlls-from.html (stato: 28.2.2017)

[81] https://www.fireeye.com/blog/threat-research/2016/06/angler_exploit_kite.html (stato: 28.2.2017)

7 Politica, ricerca, policy

7.1 Svizzera: interventi parlamentari

Atto parlamentare	N.	Titolo	Depositato da	Depositato il	Camera	Ufficio	Stato delle deliberazioni e link
Ip	16.4115	Identità elettronica	Rosmarie Quadranti	16.12.2016	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164115
Mo	16.4089	Rafforzare gli strumenti di politica di sicurezza all'estero	Damian Müller	15.12.2016	CS	DDPS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164089
Po	16.4073	Cyberrischi. Per una protezione globale, indipendente ed efficace	Roger Golay	15.12.2016	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164073
Po	16.3706	Economia digitale e mercato del lavoro	Beat Vonlanthen	27.09.2016	CS	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163706
Ip	16.3694	Siamo pronti per il mondo del lavoro 4.0?	Stefan Müller-Altermatt	22.09.2016	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163694
Ip	16.4161	Julian Assange, un difensore dei diritti umani che deve essere protetto?	Jean-Luc Addor	16.12.2016	CN	DFAE	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164161
Ip	16.4131	In che modo la Svizzera può partecipare alle ricerche sull'intelligenza artificiale per preservare i valori morali universali attraverso il digitale?	Claude Béglé	16.12.2016	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164131
Ip	16.4012	Formazione duale. Come rimanere campioni del mondo?	Claude Béglé	14.12.2016	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164012
Ip	16.4001	Airbnb and Co. Regole delle piattaforme Internet o leggi svizzere in materia di responsabilità?	Carlo Sommaruga	14.12.2016	CN	DFGP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164001
Ip	16.3960	Adeguare il nostro sistema educativo alla nuova visione del mondo imposta dalla digitalizzazione	Claude Béglé	08.12.2016	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vi-

							sta/geschaeft?AffairId=20163960
Po	16.3914	Come introdurre un'etica dell'algoritmo?	Claude Béglé	28.11.2016	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163914
Mo	16.3902	Vietare le clausole di parità tariffaria stabilite dalle piattaforme di prenotazione on line a scapito degli albergatori	Pirmin Bischof	30.09.2016	CS	CET-CS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163902
Ip	16.3861	Creazione di un consiglio consultivo "Svizzera digitale"	Fathi Derder	30.09.2016	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163861
Ip	16.3837	Droni civili. Proteggere meglio le infrastrutture sensibili	Manuel Tornare	30.09.2016	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163837
Ip	16.3829	Unità di sicurezza informatica della Confederazione e il "darknet"	Christian Imark	29.09.2016	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163829
In	16.1058	Evoluzione del mercato pubblicitario. Deflusso di capitali all'estero e finanziamento dei media	Jacqueline Badran	28.09.2016	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161058
Ip	16.4003	Digitalizzazione. Non mettere a rischio la Svizzera quale cassaforte mondiale dei dati	Marcel Dobler	14.12.2016	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164003
Ip	16.4002	Prospettive di traffico 2040. Che ne è della digitalizzazione nello scenario di riferimento?	Thierry Burkart	14.12.2016	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164002
Po	16.3918	Rivoluzione digitale. Come integrare le persone che non usano Internet?	Claude Béglé	29.11.2016	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163918
Po	16.3789	Digitalizzazione nel settore dei trasporti pubblici. Quali sfide per la protezione dei dati?	Evi Allemann	29.09.2016	CN		https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163789
In	16.1059	Attacchi terroristici e sicurezza delle centrali nucleari	Balthasar Glättli	28.09.2016	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId

							=20161059
Ip	16.4050	Digitalizzazione della dogana svizzera e riduzione dell'onere amministrativo	Viola Amherd	15.12.2016	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164050
Po	16.4078	Digitalizzazione. Permettere il voto elettronico senza carta	Marcel Dobler	15.12.2018	CN	CaF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164078
Mo	16.4011	Digitalizzazione. Evitare i doppioni nella rilevazione dei dati	Daniela Schneeberger	14.12.2016	CN	DFI	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164011
Fr	16.5429	Tisa-Informationsleck. Angriffe auf Datenschutz, Netzneutralität und Open-Source-Software	Balthasar Glättli	21.09.2016	CN	DEFR	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20165429

7.2 Strategia «Svizzera digitale»

Nel 2016 il Consiglio federale ha adottato la strategia «Svizzera digitale», la quale sostituisce la Strategia del Consiglio federale per una società dell'informazione in Svizzera, risalente al 2012.

Il nuovo documento definisce, nell'ambito dell'approccio «free, open and secure Internet», gli obiettivi strategici relativi alla parte «free and open Internet» per quanto riguarda la Svizzera.

La Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) è invece incentrata sulla parte «secure Internet» e definisce gli obiettivi strategici relativi ai temi sicurezza, fiducia, affidabilità e resilienza per quanto riguarda il nostro Paese.

Il fulcro della strategia «Svizzera digitale» consiste nello sfruttamento sistematico delle opportunità di digitalizzazione, affinché la Svizzera possa profilarsi come habitat attraente e come piazza economica e di ricerca innovativa e all'avanguardia. In tale ambito il Consiglio federale persegue i seguenti obiettivi prioritari: «innovazione, crescita e benessere nel mondo digitale», «pari opportunità e partecipazione di tutti», «trasparenza e sicurezza» e «contributo allo sviluppo sostenibile»; inoltre, definisce i principi fondamentali da seguire per lo sviluppo digitale.

7.3 Partecipazione della Svizzera all'esercizio «Cyber Europe 2016»

L'esercizio «Cyber Europe», ormai giunto alla quarta edizione, è considerato uno dei maggiori e più importanti esercizi di cyberguerra al mondo. L'evento, di cadenza biennale, viene organizzato dall'ENISA ed è incentrato sia sull'aspetto tecnico sia sull'aspetto operativo di

una crisi cyber. All'ultima edizione hanno partecipato 29 Stati membri dell'UE e i Paesi dell'AELS, tra cui anche la Svizzera. La prima parte, quella tecnica, è iniziata già nell'aprile del 2016 e ha permesso ai collaboratori del settore Cybersecurity di analizzare incidenti tecnici complessi, innovativi e realistici negli ambiti più disparati. Il 13 e 14 ottobre è quindi seguita la parte operativa, alla quale hanno partecipato esperti di oltre 300 organizzazioni attive in particolare nei settori Telecomunicazioni, Cloud Service Provider, Cybersecurity Software e Service Provider, reparti responsabili della Cybersecurity nonché ministeri e istituzioni dell'UE. Cyber Europe 2016 ha affrontato temi quali l'«Internet delle cose», i «droni», il «cloud computing», il «mobile malware» e il «ransomware». Per la prima volta, l'intero scenario è stato integrato con attori, giornalisti, ditte simulate e social media, per tener sufficientemente conto dell'aspetto «public affairs». «stronger together», il motto di Cyber Europe, esprime la convinzione che la cooperazione su tutti i piani rappresenti la chiave di volta per riuscire a gestire i grandi incidenti informatici internazionali.

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 Tofsee Spambot features .ch DGA - Reversal and Countermesaures

22.12.2016 - The malware, which MELANI / GovCERT identified as Tofsee, has tried to spam out hundreds of emails within a couple of minutes. However, this wasn't the reason why it popped up on the radar. The reason why this particular sample caught our attention were the domains queried by the malware. The domains appear to be algorithmically generated, and about half of the domains use the country code top level domain (ccTLD) of Switzerland.

➔ https://www.govcert.admin.ch/blog/26/tofsee-spambot-features-.ch-dga-reversal-and-countermesaures

8.1.2 When Mirai meets Ranbyus

15.12.2016 - In the past weeks, MELAN / GovCERT has seen a rise of malicious Microsoft office documents that are being spammed out to Swiss internet users with the aim to infect them with a malicious software (malware) called Dridex. Dridex is an ebanking Trojan which is already around for some time now.

➔ https://www.govcert.admin.ch/blog/23/dridex-targeting-swiss-internet-users

8.1.3 SMS spam run targeting Android Users in Switzerland

13.07.2016 - MELANI / GovCERT.ch received several reports today about malicious SMS that have been sent to Swiss mobile numbers. The SMS is written in German and claims to come from the Swiss Post. But in fact, the SMS has been sent by hackers with the aim to infect Smartphones in Switzerland with a Trojan horse.

➔ https://www.govcert.admin.ch/blog/24/sms-spam-run-targeting-android-users-in-switzerland

8.1.4 Dridex targeting Swiss Internet Users

08.07.2016 - In the past weeks, MELANI / GovCERT has seen a rise of malicious Microsoft office documents that are being spammed out to Swiss internet users with the aim to infect them with a malicious software (malware) called Dridex. Dridex is an ebanking Trojan which is already around for some time now. The attackers are operating various botnets with Dridex infected computers. While most of these botnets do have a strong focus on financial institu-

tions from abroad (such as US or UK), one particular botnet is also targeting financial institutions in Switzerland.

➔ https://www.govcert.admin.ch/blog/23/dridex-targeting-swiss-internet-users

8.2 MELANI Newsletter

Nel secondo semestre del 2016 MELANI ha pubblicato le seguenti newsletter:

8.2.1 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

8.2.2 e-banking: gli hacker prendono di mira i metodi di autenticazione per dispositivi mobili

Nelle scorse settimane MELANI ha ricevuto diverse segnalazioni di casi in cui degli hacker hanno indotto le vittime a convalidare pagamenti fraudolenti via e-banking adottando tecniche di ingegneria sociale.

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

8.2.3 Tema principale del rapporto semestrale MELANI: cyber-estorsione

Il 23° rapporto della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), pubblicato in data odierna, esamina i principali incidenti informatici che si sono verificati a livello nazionale e internazionale nel primo semestre del 2016. Il rapporto si focalizza sugli attacchi sempre più frequenti, sferrati ricorrendo alla cyber-estorsione e sui furti di dati.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/rapporto-semestrale-2016-1.html

8.2.4 Software offline per i pagamenti nel mirino degli hacker – imprese svizzere colpite

25.07.2016 - Negli ultimi giorni MELANI ha osservato vari attacchi a software offline per i pagamenti ad opera del malware Dridex. Di solito questi programmi sono usati dalle imprese per effettuare in Internet un grande numero di pagamenti a una o più banche. Se i computer

dotati di tali software vengono infettati, i danni potenziali che ne derivano sono dunque gravi. MELANI raccomanda pertanto alle imprese di adottare con urgenza tutti i provvedimenti necessari a proteggere i computer utilizzati da questo genere di frode.

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

8.2.5 Numerosi documenti Office maligni in circolazione

08.07.2016 - Nelle scorse settimane la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI ha ricevuto numerosi annunci inerenti documenti di Microsoft Office nocivi, diffusi via e-mail con l'obiettivo di infettare il computer delle vittime con software maligni (malware). Per questo motivo MELANI ha deciso di mettere esplicitamente in guardia dall'apertura di simili documenti Office, consiglia agli utenti di internet una particolare cautela nei confronti di questo genere di documenti e di non eseguire alcun macro Office.

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

8.3 Liste di controllo e guide

Nel secondo semestre del 2016 MELANI non ha pubblicato nuove liste di controllo o guide.

9 Glossario

Definizioni	Descrizione
Accessibility Service	Un Accessibility Service è un'applicazione che mette a disposizione un'interfaccia utente per fornire sostegno agli utenti affetti da disabilità o a quelli che temporaneamente non sono in grado di interagire pienamente con il vostro dispositivo.
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.
Algoritmi Domain Generation	Gli algoritmi Domain Generation vengono utilizzati da molte famiglie di malware per generare periodicamente una moltitudine di nomi di dominio che in seguito vengono utilizzati come punti di contatto per i server Command & Control.
App	Il concetto di app (dall'abbreviazione inglese di Ap-

	plication) 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. passwort, 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.
Barcode	Si designa barcode o codice a barre una scrittura leggibile con un dispositivo optoelettronico, composta da barre parallele e spazi vuoti.
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»).
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.
Codice QR	Il codice QR (Quick Response Code) consiste in una matrice di forma quadrata a quadretti bianchi e neri che rappresentano i dati utilizzando un codice bidimensionale.
Codice RFID	L'acronimo RFID (Radio Frequency Identification, identificazione a radio frequenza) designa una tecnologia utilizzata dai sistemi ricetrasmittenti per identificare e localizzare automaticamente senza contatto oggetti ed esseri viventi tramite onde radio.
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.
Cookies	Piccolo file di testo depositato sul computer dell'utente alla visita di una pagina Web. Con l'ausilio dei cookies è per esempio possibile salvaguardare le impostazioni personali di una pagina Internet. Essi possono però anche essere sfruttati in modo abusivo per registrare le abitudini di navigazione dell'utente e allestire in tale modo un profilo di utente.
Defacement	Deturpamento di pagine Web.
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.
Etica Hacker	L'etica Hacker designa un insieme di valori etici intesi a caratterizzare in modo inconfondibile la cultura Hacker.
Fast Flux	Fast Flux è una tecnica DNS utilizzata dalle botnet e che consente di occultare l'ubicazione dei web server.
Google-Rank	L'algoritmo PageRank è una procedura utilizzata per valutare o soppesare una quantità di documenti interconnessi, quali ad esempio il World Wide Web, in base alla loro struttura.
Grey-Hat	Categoria di hacker che possono anche contravvenire

	alle leggi o alle interpretazioni restrittive dell'etica della pirateria informatica, ma per raggiungere un obiettivo etico.
ICANN	Internet Corporation for Assigned Names and Numbers (ICANN) L'ICANN e un'organizzazione senza scopo di lucro con sede nella cittadina costiera californiana di Marina del Rey. ICANN decide in merito ai principi di gestione dei Top Level Domain. Così facendo ICANN coordina gli aspetti tecnici di Internet, senza peraltro stabilire norme di diritto vincolanti.
Internet delle cose	L'espressione «Internet delle cose» indica che nel mondo digitale il computer è integrato in misura crescente da «oggetti intelligenti», ossia dall'applicazione dell'intelligenza digitale agli oggetti reali.
Javascript	Un linguaggio di script orientato sugli oggetti per lo sviluppo di applicazioni. Gli JavaScripts sono elementi di programma integrati nel codice HTML, che consentono determinate funzioni nel browser di Internet. 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.
Macro-malware	Malware installato tramite macro. Una macro è costituita da una sequenza di istruzioni che possono essere eseguite con un semplice richiamo.
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.
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.
Plaintext	Per plaintext si intendono i dati che possono essere trasformati direttamente in testo tramite una codifica dei caratteri.
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.
Port scan	Un port scan è un software che consente di verificare quali sono i servizi offerti da un sistema che funziona con TCP o UDP attraverso il protocollo Internet (IP).
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.
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.
Router	Apparecchiature del settore delle reti di computer, della telecomunicazione o anche di Internet che collegano o separano più reti di computer. I router sono ad esempio utilizzati nelle reti domestiche per effettuare il collegamento tra la rete interna e Internet.
Script PowerShell	PowerShell è un framework multipiattaforma di Microsoft che consente di automatizzare, configurare e gestire sistemi ed è composto da un interprete a riga di comando (shell) e da un linguaggio di scripting.
Servizi di e-currency	Valore monetario sotto forma di credito nei confronti dell'ente emittente, salvato su un supporto dati e rilasciato dietro riscossione di una somma di denaro, il cui valore non è inferiore al valore monetario emesso e che viene accettato come mezzo di pagamento da aziende diverse dall'ente emittente.

SHA	L'espressione secure hash algorithm (SHA) designa un gruppo di funzioni crittografiche di hash standardizzate.
Carta SIM	La carta SIM (in inglese: Subscriber Identity Module) è una carta chip inserita nel telefono mobile che serve all'identificazione dell'utente.
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.
Software per i pagamenti offline	Software installato localmente per la registrazione di pagamenti.
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 correlazione con l'ISDN, la rete fissa e la rete mobile, e all'incirca dal 2000 impiegato in misura crescente anche nelle reti VoIP.
Take down	Take down (rimozione) è un'espressione utilizzata quando un provider ritira un sito dalla rete a causa della presenza di contenuti fraudolenti.
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 riav-

	viato. 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.