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

SICUREZZA DELLE INFORMAZIONI

LA SITUAZIONE IN SVIZZERA E A LIVELLO INTERNAZIONALE

Rapporto semestrale 2018/II (luglio – dicembre)

30 APRILE 2019
CENTRALE D'ANNUNCIO E D'ANALISI PER LA SICUREZZA DELL'INFORMAZIONE MELANI
https://www.melani.admin.ch/

1 Indice

2 Editoriale

Il ruolo attuale e futuro dello Stato nel settore della cibersicurezza

La dott.ssa Myriam Dunn Cavelty è capo sostituto del Center for Security Studies al Politecnico di Zurigo, dove svolge attività di ricerca e insegna politica di cibersicurezza.

Ancora dieci anni fa la cibersicurezza era un tema di nicchia discusso soprattutto tra esperti, ma nel frattempo l'acuirsi delle minacce l'ha inserita di diritto nell'ordine del giorno dei dibattiti sulla politica della sicurezza e a occuparsene sono i massimi esponenti governativi.

Il ruolo dello Stato e del suo apparato burocratico è soggetto a un processo politico negoziale tuttora in atto in molti Paesi del mondo. La cibersicurezza è un tema trasversale, che si interfaccia con molti ambiti politici. Una delle principali sfide in un'epoca contrassegnata dalla penuria di risorse è trovare la giusta combinazione tra nuove strutture e impiego efficiente delle competenze esistenti con l'opportuno coinvolgimento dei principali attori dell'economia e della società. Si rivelano particolarmente difficili l'integrazione (verticale) delle strategie nazionali di cibersicurezza nel quadro della sicurezza nazionale e in una strategia globale che comprenda tutti gli ambiti politici nonché il coordinamento (orizzontale) e il controllo dei diversi organi che si occupano di cibersicurezza.

Un aspetto trova tutti concordi: è possibile raggiungere un livello soddisfacente di cibersicurezza solo se Stato, economia e società interagiscono, mentre spesso i singoli attori seguono obiettivi e interessi diversi. Ne risultano almeno tre campi di tensione nei quali deve posizionarsi ogni politica di cibersicurezza.

Nel primo campo di tensione tra Stato ed economia deve essere formulata una politica volta a mettere in sicurezza le infrastrutture critiche, che neutralizzi le conseguenze negative della liberalizzazione, della privatizzazione e della globalizzazione dal punto di vista della politica della sicurezza senza inibirne gli effetti positivi. Nel secondo tra Stato e cittadini, è necessario trovare l'equilibrio auspicato dalle istanze politiche tra una maggiore sicurezza e la salvaguardia dei diritti dei cittadini nello spazio digitale. Nel terzo tra cittadini ed economia, devono essere create le condizioni quadro per lo sviluppo di un ecosistema della sicurezza funzionante nel quale si delinei un equilibrio ottimale tra sicurezza e funzionalità e vengano creati incentivi per un maggiore impegno a favore della sicurezza da parte degli offerenti di servizi.

Ciò che è naturale per gli attori del mondo economico e della società civile vale anche per lo Stato: la contestuale assunzione di una molteplicità di ruoli. La consapevolezza dell'eterogeneità dell'agire statale è una buona premessa per dipanare i conflitti di ruolo a livello politico, affrontarli sistematicamente e plasmare così una politica proattiva per il futuro.

Myriam Dunn Cavelty

3 Tema principale: gestire le soluzioni critiche di hardware e software con i produttori

I produttori di hardware e software in determinati Paesi non sono finiti sotto i riflettori solo da quando Snowden ha divulgato documenti «top secret». Poco dopo l'ingresso della cinese Huawei sul mercato globale sono emersi dubbi sull'ineccepibilità dei suoi prodotti e sull'indipendenza dalle autorità. Con le rivelazioni di Snowden del 2013 ha trovato parziale conferma il sospetto che anche società produttrici statunitensi come Cisco, Microsoft, Google e altre concedono alle autorità di accedere ai loro prodotti per sorvegliare gli utenti. In seguito alle accuse di spionaggio russo negli Stati Uniti, le autorità americane hanno vietato l'utilizzo di software sviluppati da Kaspersky all'interno dell'amministrazione americana. Questa tematica è dibattuta anche negli ambienti dell'economia e della pubblica amministrazione in Svizzera.

Da un lato, nell'ottica di misure di sicurezza precauzionali, vi sono buoni motivi per essere più oculati nell'impiego di prodotti di determinate società. Dall'altro, una parte non trascurabile della discussione è tuttavia dovuta a meri interessi di politica economica. Si impone dunque un confronto differenziato, che prescinda dai produttori.

3.1.1 Hardware e software come strumento per perseguire interessi statali

Con la crescente digitalizzazione dei processi operativi, le necessarie soluzioni hardware e software sono una componente fondamentale e critica. A prima vista, l'offerta sul mercato è estremamente variegata e ampia in considerazione dei più diversi approcci di soluzione. Tuttavia, se si osservano i Paesi da cui provengono gli offerenti, questa diversità risulta essere più che altro apparente. Il mercato è esplicitamente dominato dalle imprese statunitensi, seguite a ruota dalla Cina e da singoli concorrenti globali, ad esempio la coreana Samsung, la russa Kaspersky e la tedesca SAP.

Analizzando le basi giuridiche vigenti nei Paesi di origine in riferimento all'industria nazionale delle tecnologie dell'informazione e della comunicazione (TIC), emerge chiaramente che essa non rappresenta soltanto un gradito motore economico. Il suo ruolo centrale nell'elaborazione, nella fornitura e nell'archiviazione di informazioni è noto e le mire in materia da parte degli organi statali sono sancite nelle leggi.

È un dato di fatto che, senza le soluzioni hardware e software sviluppate dalle imprese statunitensi, cinesi e di altri Paesi, verrebbe a mancare la fitta digitalizzazione dei processi oggi conosciuti. A sua volta, questa digitalizzazione va di pari passo con la teorica semplificazione dell'accesso ai sistemi TIC dei produttori nazionali e, quindi, alle informazioni archiviate, elaborate o messe a disposizione.

3.1.2 Esclusione del produttore, cibersovranità e norme internazionali

Il potenziale accesso ai produttori di TIC da parte degli Stati in cui hanno sede le imprese e la conseguente possibilità di ottenere il controllo globale su hardware e software danno adito a dibattiti sulla corretta gestione di questi rischi.

In linea di principio, alcuni degli approcci praticati su larga scala mirano ai produttori e agli offerenti di soluzioni hardware e software.

I produttori possono essere generalmente esclusi dalle procedure di appalto se sospettati di essere asserviti a un Stato. È avvenuto, per esempio, nell'amministrazione statunitense, che nel mese di dicembre del 2017 ha vietato l'impiego di prodotti sviluppati dal gruppo Kaspersky,

che ha sede in Russia. Recentemente, anche di fronte al possibile acquisto di prodotti Huawei i Paesi più disparati hanno chiesto di escludere questi produttori dalle procedure di appalto.

Tali approcci possono fornire apparenti soluzioni (in materia di sicurezza) nel breve e medio termine per sottrarsi a un eventuale controllo dei processi digitali da parte di Stati terzi. In diversi Paesi, tra cui la Svizzera, è in corso un ampio dibattito sulla possibilità di liberarsi dalla dipendenza dai due giganti della tecnologia, ossia Stati Uniti e Cina.

Anche a livello di politica internazionale della sicurezza, il tema degli accessi e delle ingerenze statali sui produttori di soluzioni TIC è all'ordine del giorno da diverso tempo. Ad esempio, il rapporto stilato nel 2015 dal gruppo di esperti governativi delle Nazioni Unite («United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security», UN GGE) ha definito le prime norme volte a limitare queste azioni. Il rapporto successivo del 2017, che avrebbe dovuto concretizzare queste norme, non è riuscito a ottenere il necessario consenso in un quadro di rapporti molto inaspriti tra gli Stati.

3.1.3 I produttori di hardware e software alla mercé degli interessi statali

Nel famoso romanzo «1984» di George Orwell, espressione di utopia negativa sulla natura del potere assoluto, ricorre più volte la convinzione che chi controlla il passato controlla il futuro e chi controlla il presente controlla il passato. Questo paradigma è imperniato sull'idea dell'accesso assoluto e indisturbato a informazioni e dati. A nessuno dei Paesi di origine dei maggiori produttori di TIC è attribuita la stessa velleità di totalitarismo globale. Il fatto di poter accedere in modo mirato, entro le basi giuridiche esistenti, a informazioni e dati tramite i produttori nazionali di hardware e software rappresenta tuttavia un decisivo vantaggio comparativo a cui nessuno di questi Stati è disposto a rinunciare spontaneamente autolimitando le proprie facoltà.

In questo contesto devono essere inquadrate anche le dichiarazioni pubbliche rilasciate dagli Stati Uniti, che non intendono consentire alla Cina di rilevare la loro leadership tecnologica. Le sanzioni e le messe al bando di produttori sono dunque da interpretare come pure decisioni di politica economica e della sicurezza, solo limitatamente basate su considerazioni di vario tipo concernenti la sicurezza nel senso di autoprotezione. La flessione delle vendite di componenti TIC da parte dei produttori statunitensi va di pari passo con la perdita di un controllo efficace su queste soluzioni hardware e software in funzione presso i clienti finali.

I produttori di soluzioni TIC sono alla mercé degli interessi dei loro Paesi di origine e anche in futuro, conformemente alle legislazioni vigenti, saranno obbligati a collaborare con i rispettivi organi statali. Non è ipotizzabile che una qualunque impresa privata si opponga al diritto vigente nel proprio Paese persino in un caso estremo. È altresì prevedibile che la Cina e gli Stati Uniti continuino a lottare per conquistare la supremazia sul mercato globale dei prodotti TIC.

3.1.4 Carenza di alternative

È tutt'altro che certo che la piazza industriale svizzera riesca, nel prossimo futuro, a sviluppare alternative all'egemonia degli offerenti stranieri di soluzioni hardware e software. Anche una politica industriale concertata, atipica per la Svizzera, in questo ambito produrrebbe i suoi eventuali effetti solo a lungo termine. La digitalizzazione dei processi operativi, «eHealth», l'introduzione della rete 5G e simili sviluppi sono già in atto, ma i componenti e le soluzioni necessari per le TIC non sono prodotti in Svizzera – se non in misura esigua e con un dispendio elevato.

La Svizzera, nella sua qualità di piccola economia aperta, dipende dai produttori stranieri di TIC, d'altro canto può essere beneficiare dal fatto di poter soppesare i diversi interessi degli Stati con industrie TIC leader di mercato. Nell'ambito della digitalizzazione, l'economia svizzera rimarrà parzialmente dipendente dai produttori stranieri di TIC. Anche in vista di possibili accessi e ingerenze da parte di altri Stati, dovrebbe dunque essere creata una gestione sistematica del rischio che affronti in via continuativa i rapporti con i produttori, i fornitori e l'indotto delle soluzioni hardware e software.

Valutazione

Le tematiche suesposte comportano le seguenti valutazioni di fondo delle minacce nell'ambito dei produttori TIC con società madri straniere:

- il dispositivo giuridico dei Paesi in cui hanno sede i principali attori su scala globale nel settore delle soluzioni hardware e software legittima praticamente qualunque reperimento di informazioni concernenti obiettivi stranieri, purché risponda all'interesse del rispettivo Paese;
- un impegno delle imprese TIC, sancito a livello puramente contrattuale, di salvaguardare il diritto svizzero non è da considerare una garanzia sufficiente, poiché dovrebbe essere vincolato a condizioni e accompagnato da controlli periodici in loco. Ciò comprende anche gli impianti situati all'estero in grado di influenzare a livello tecnico e gestionale l'attività delle imprese svizzere collegate in termini organizzativi o mediante quote di proprietà;
- a seconda dell'hardware e del software e in base alla scelta dei fornitori di servizi, dovrebbero essere adottate misure adeguate che impediscano il più possibile l'accesso non autorizzato a sistemi e dati, ma possano almeno individuarlo e fermarlo;
- per ogni progetto di acquisto devono essere pianificate misure adeguate al rischio, da evidenziare nei costi. Non è dunque da escludere che l'offerta apparentemente più conveniente comporti poi costi aggiuntivi interni per implementare opportune misure di accompagnamento oppure l'acquisto di un ulteriore servizio per il controllo e la protezione.

4 La situazione a livello nazionale

4.1 Spionaggio

4.1.1 Nel mirino anche il laboratorio Spiez, riferimento per l'OPAC

Nel suo ultimo rapporto semestrale, MELANI ha riferito dell'impiego abusivo di un invito pubblico a una conferenza internazionale organizzata dal Laboratorio Spiez. Per sferrare un attacco mirato e indurre i destinatari ad aprire l'allegato, gli hacker hanno utilizzato l'invito come modello e lo hanno inviato a diversi destinatari con mittente falsificato a nome dell'Ufficio federale della protezione della popolazione (UFPP) e del Laboratorio Spiez

Che il Laboratorio Spiez fosse nel mirino degli hacker è emerso con la notizia, diffusa nel mese di settembre del 2018, dell'arresto di quattro persone avvenuto il 13 aprile dello stesso anno

in Olanda[1]. Gli arrestati sono stati accusati di tentata intrusione nella rete wireless dell'Organizzazione per la proibizione delle armi chimiche (OPAC), attiva a livello internazionale. Si ipotizza che i quattro presunti collaboratori russi del servizio segreto «GRU» siano entrati in Olanda dall'aeroporto di Schiphol esibendo passaporti diplomatici, abbiano quindi noleggiato un'auto che hanno stazionato nel parcheggio dell'Hotel Marriot all'Aja, situato nelle immediate vicinanze degli uffici dell'OPAC. Nel baule dell'auto è stata riposta un'attrezzatura che viene utilizzata per penetrare nelle reti wireless e può essere impiegata per compiere ciberattacchi. L'antenna del dispositivo attivato era nascosta sotto un cappotto lasciato sul ripiano posteriore dell'auto. I quattro arrestati sono stati espulsi il giorno stesso dall'Olanda, dove hanno dovuto lasciare il loro equipaggiamento.

È emerso che anche il Laboratorio Spiez era un potenziale bersaglio di questo gruppo. Nel bagaglio degli arrestati è stato trovato, tra l'altro, un biglietto ferroviario da Utrecht a Basilea. In un notebook gli inquirenti hanno scoperto ricerche concernenti l'ufficio consolare dell'ambasciata russa di Berna e il Laboratorio[2]. L'OPAC e il Laboratorio Spiez erano coinvolti nelle indagini sull'avvelenamento dell'ex spia russa Sergei Skripal e di sua figlia avvenuto nel mese di marzo del 2018 a Salisbury, in Gran Bretagna. Il Servizio delle attività informative della Confederazione (SIC) ha confermato di essere stato direttamente coinvolto nell'operazione insieme ai suoi partner olandesi e britannici, quindi ha contribuito a impedire che fossero commessi atti illegali contro un'infrastruttura critica svizzera.

Sebbene il Laboratorio Spiez adempisse le prescrizioni riguardanti oggetti particolarmente a rischio anche prima, la protezione è stata aumentata adottando ulteriori misure per estendere lo standard di sicurezza.

4.1.2 Infrastrutture critiche nel mirino dell'operazione Sharpshooter

Nel mese di dicembre del 2018 McAfee, società che produce software per la sicurezza informatica, ha pubblicato un rapporto concernente la scoperta di una campagna APT perpetrata contro imprese operanti nei settori della difesa, dell'energia, del nucleare e della finanza[3]. La campagna, nota con il nome di «Sharpshooter», è cominciata il 25 ottobre 2018 con l'invio di documenti infetti ad appartenenti di 87 organizzazioni in tutto il mondo, ma soprattutto negli Stati Uniti. Secondo il rapporto, la campagna avrebbe colpito anche imprese svizzere del settore finanziario. Attualmente il Servizio delle attività informative della Confederazione SIC non è a conoscenza di eventuali infezioni concernenti ditte con sede in Svizzera.

Mediante pratiche di ingegneria sociale («social engineering») i destinatari dei messaggi sono indotti ad aprire i documenti infetti. La lettera era camuffata da candidatura e conteneva un link a un documento in Dropbox nel quale veniva asserito che si trovasse il dossier di candidatura. Questo metodo è particolarmente insidioso perché gli uffici del personale ricevono spesso candidature spontanee, pertanto aprire simili documenti è per loro una consuetudine. Le imprese che hanno messo in atto misure di sicurezza correttamente non hanno corso grossi rischi. L'infezione si è propagata mediante una macro contenuta nel documento Word. Nel

---

1 https://www.government.nl/government/members-of-cabinet/ank-bijleveld/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw (stato: 31 gennaio 2019)

2 https://www.justice.gov/opa/page/file/1098571/download (stato: 31 gennaio 2019)

3 https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf (stato: 31 gennaio 2019)

frattempo, in numerose imprese queste macro sono state bloccate oppure si attivano solo dopo la conferma di un messaggio di allerta. Se la macro viene eseguita nonostante tutti gli avvertimenti, il malware Sharpshooter si infiltra nella memoria di lavoro di Word, dopo di che installa una backdoor modulare chiamata «Rising Sun». Tra le sue funzioni, questa componente annovera la raccolta e l'invio di informazioni su documenti, nomi utente, configurazioni di rete e impostazioni di sistema. Inoltre, il malware può scaricare altre funzioni. Tra l'altro, è in grado di cancellare le tracce per non essere scoperto. In tal modo, può svuotare la memoria o cancellare le sue attività. Il malware comunica mediante un server del tipo «command and control», controllato dagli hacker.

Nell'analisi della campagna, McAfee ha individuato indizi che potevano ricondurre al gruppo Lazarus: Rising Sun contiene il codice e dati di configurazione provenienti dalla famiglia di trojan «Duuzer», utilizzato anche nell'attacco sferrato contro Sony, che viene fatto risalire al gruppo Lazarus. Diverse società che si occupano di cibersicurezza attribuiscono tali attacchi alla Corea del Nord. Tuttavia, nel caso in questione, viene utilizzata una diversa routine di decrittazione, inducendo a ritenere che Rising Sun possa essere il frutto di un ulteriore sviluppo di Duuzer. Non è dunque possibile accertare il legame tra questa campagna e il gruppo Lazarus. I metodi, le tracce e i malware sono ormai noti in tutto il mondo e risultano idonei anche per condurre le cosiddette operazioni «false flag», ossia sotto falsa bandiera, nel senso che tentano di far ricadere il sospetto su terzi non coinvolti.

4.2 Sistemi di controllo industriali

4.2.1 Sistemi di controllo industriali e IoT

Fortunatamente, nel secondo semestre del 2018 non sono stati commessi attacchi di sabotaggio eclatanti. Non è stata data notizia di attacchi mirati contro sistemi di controllo industriali, tuttavia hanno destato una certa attenzione le infezioni perpetrate tramite malware tradizionali, come i ransomware nelle reti dei sistemi di controllo all'estero[4] (cfr. anche cap. 5.3.5). Moderni impianti in rete vengono messi in esercizio continuamente e anche i sistemi più vecchi, un tempo isolati, sono collegati a Internet per ottenere una maggiore efficienza mediante il loro inserimento in altri processi operativi. Tuttavia, con la messa in rete e il collegamento a Internet degli oggetti più svariati («Internet of Things», IoT) aumenta anche il rischio di rimanere vittime dei multiformi pericoli di Internet, possibilmente rivolti contro sistemi raggiungibili e vulnerabili.

4.2.2 Ciberattacco fallito a Ebikon – il Comune sventa un presunto attacco all'approvvigionamento idrico

La Svizzera è nota per la qualità elevata della sua acqua potabile. Per assicurarne l'approvvigionamento, i Comuni compiono sforzi notevoli e rinnovano periodicamente i loro impianti. In questa occasione vengono installati anche i più moderni sistemi di controllo. Persino le delegazioni di Paesi europei si rivolgono volentieri alla Svizzera per ottenere informazioni sulle esperienze compiute con l'operatività dei nuovi sistemi[5].

---

4 https://dragos.com/year-in-review/ (stato: 31 gennaio 2019)

5 https://www.ebikon.ch/verwaltung/aktuelles/news/daenemark-auf-besuch-in-ebikon (stato: 31 gennaio 2019)

Purtroppo, questi impianti interessano anche gli hacker di tutto il mondo. Infatti, lo scorso autunno il Comune di Ebikon ha registrato diverse migliaia di tentativi di intrusione nella rete del controllo operativo autonomo del suo sistema di approvvigionamento idrico[6].

Per i motivi più disparati gli hacker sono alla perenne ricerca di servizi penetrabili dall'esterno. Testano le eventuali lacune di sicurezza e cercano di penetrare nei sistemi individuati sia con noti dati di accesso standard sia con identità prelevate altrove. Nel caso di Ebikon, i tentativi sono fortunatamente rimasti vani, inoltre la loro scoperta ha consentito di adeguare a posteriori le misure di sicurezza. Tuttavia, anche se l'attacco fosse riuscito e le misure di prevenzione e intercettazione avessero fallito, il Comune sarebbe stato in grado di riavviare i sistemi automatici e di continuare a gestire manualmente gli impianti.

Il caso di Ebikon è un ottimo esempio per dimostrare come le misure adottate nelle diverse fasi della struttura di cibersicurezza[7] contribuiscano a sventare tentativi reali di attacco contro un'infrastruttura vitale e, se necessario, a reagire. Vale la pena di investire non solo nella prevenzione, ma anche nei provvedimenti da adottare al verificarsi dell'evento. Un approccio possibile è offerto dallo standard minimo TIC dell'Ufficio federale per l'approvvigionamento economico del Paese (UFAE).

Raccomandazione

Nell'ambito della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) adottata dal Consiglio federale nel 2012, l'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) ha analizzato le vulnerabilità di diversi settori vitali di fronte ai ciber-rischi. Sono stati studiati l'approvvigionamento energetico, di acqua potabile e di generi alimentari così come il trasporto stradale e ferroviario. Sulla base dei risultati ottenuti, l'UFAE ha sviluppato lo Standard minimo per migliorare la resilienza delle TIC, rivolto in particolare ai gestori di infrastrutture critiche in Svizzera, tuttavia attuabile parzialmente o integralmente da ogni impresa.

Lo Standard minimo per migliorare la resilienza delle TIC comprende le funzioni «identificare», «proteggere», «intercettare», «reagire» e «ripristinare». Inoltre, offre agli utenti 106 concrete istruzioni operative per migliorare la resilienza delle TIC di fronte ai ciber-rischi.

Standard minimo per migliorare la resilienza delle TIC

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

4.2.3 MadIoT – Il potenziale pericolo di una botnet sugli elettrodomestici

Molti si ricorderanno ancora del blackout che ha interessato l'Italia il 28 settembre 2003. Una reazione a catena ha provocato un sovraccarico delle reti di trasmissione e ha lasciato l'intero Paese senza elettricità[8]. Il blackout fu provocato da un arco elettrico formatosi su un albero in

6 https://www.inside-it.ch/articles/53204 (stato: 31 gennaio 2019)

7 https://www.nist.gov/cyberframework (stato: 31 gennaio 2019)

8 http://www.rae.gr/old/cases/C13/italy/UCTE_rept.pdf (stato: 31 gennaio 2019)

Svizzera. Diverse circostanze sfavorevoli hanno causato questa instabilità e il sovraccarico della rete elettrica. Ma che cosa sarebbe successo se l'instabilità fosse stata provocata intenzionalmente manomettendo il consumo di elettricità su numerosi elettrodomestici?

Riflessioni di questo tipo sono state fatte da alcuni ricercatori della Princeton University nell'ambito di uno studio[9] presentato alla USENIX Security Conference tenutasi nel mese di agosto del 2018. Esso si fonda sull'ipotesi che un attore malintenzionato riesca a costruire una botnet su dispositivi dell'Internet delle cose («Internet of Things», IoT) con un elevato consumo di energia tra cui gli impianti di condizionamento, i riscaldamenti e le lavatrici. Se i loro consumi sono coordinati geograficamente e inaspettatamente influenzati in misura elevata, negli scenari delineati dai ricercatori è stato possibile introdurre nella rete elettrica queste instabilità, come quelle che avevano provocato il summenzionato blackout in Italia[10].

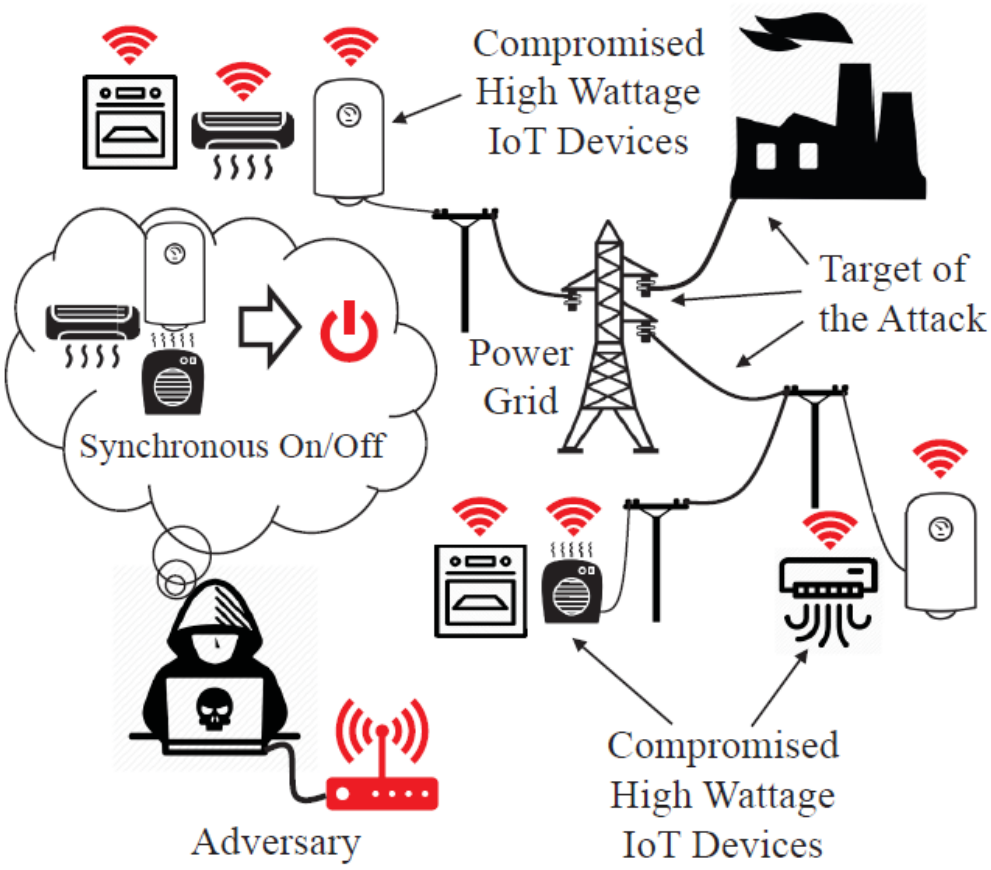


Figura 1: Schema di attacco «Manipulation of demand via IoT» (fonte: usenix.org, https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-soltan.pdf)

Negli scenari di attacco descritti, la novità consiste nel fatto che i blackout non sono stati provocati danneggiando la produzione energetica o la trasmissione, bensì hanno preso di mira i consumatori. I terminali degli utenti usufruiscono spesso di una protezione solo marginale,

9 https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-soltan.pdf (stato: 31 gennaio 2019)

10 https://securityintelligence.com/how-an-iot-botnet-could-breach-the-power-grid-and-cause-widespread-blackouts/ (stato: 31 gennaio 2019)

soprattutto in confronto alle centrali elettriche o alle reti di trasmissione, dove da anni sono investite ingenti risorse nella sicurezza.

La stabilità della rete elettrica si basa sull'affidabilità delle previsioni di consumo, basate soprattutto sui dati storici empirici. Mediante una manipolazione concertata di dispositivi vulnerabili con un consumo elevato, contrariamente alle previsioni dei consumatori, sono state superate le consuete riserve di tolleranza. A titolo di esempio, in piena estate tutti i riscaldamenti elettrici potrebbero essere accesi contemporaneamente a pieno regime da un hacker. Questo modus operandi è chiamato «Manipulation of demand via IoT (MadIoT)».

Le ipotesi alla base delle simulazioni possono apparire inverosimili, ma le ripercussioni della botnet Mirai nel 2016 hanno evidenziato inequivocabilmente i potenziali danni di una botnet IoT. Già nel 2017 Sophos, società britannica che produce software per la sicurezza, ha dimostrato in un esperimento che i dispositivi IoT potenzialmente esposti nelle abitazioni intelligenti possono diventare in breve tempo oggetto di attacchi da diverse parti[11]. L'azienda che offre soluzioni per la sicurezza informatica ha rilevato una concentrazione elevata di questi apparecchi a rischio anche in Svizzera.

Non solo i gestori delle infrastrutture dell'energia, ma anche i produttori di apparecchi IoT devono contribuire a evitare che simili attacchi diventino realtà. Gli sforzi di prescrivere standard minimi di buone pratiche sono numerosi, ma sono diventati obbligatori solo in un numero ridottissimo di regioni e settori. Una presentazione schematica[12] redatta dal britannico «Department for Digital, Culture, Media & Sport» (DCMS) offre una buona visione d'insieme e confronta le direttive e le linee guida esistenti.

Raccomandazione

Scoprite sistemi di controllo raggiungibili dall'esterno o protetti in modo inadeguato in Internet, segnalateci le relative indicazioni affinché possiamo informare i gestori.

Formulario d'annuncio MELANI

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

Lista di controllo con misure di protezione dei sistemi di controllo industriali

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

4.3 Attacchi (DDoS, Defacements, Drive-By)

I privati, le organizzazioni e le imprese in Svizzera rimangono bersagli di diversi tipi di attacchi.

11 https://www.computerworld.ch/security/hacking/smart-home-in-minuten-hacker-da-1435426.html (stato: 31 gennaio 2019)

12 https://iotsecuritymapping.uk/ (stato: 31 gennaio 2019)

4.3.1 Modem Quickline abusati per «SNMP Amplification Attack»

Come pubblicato in un comunicato stampa dell'11 ottobre 2018 da Quickline, noto fornitore di accesso a Internet, il provider ha dovuto lottare contro episodi di malfunzionamento per due settimane. Il problema ha riguardato i servizi di televisione, Internet e telefonia, seppure non tutti i clienti siano stati colpiti allo stesso modo e in pari misura. La causa è stata identificata in una vulnerabilità di un certo tipo di modem. Dalle analisi è emerso che i cibercriminali non hanno preso di mira direttamente i clienti, serviti soprattutto per sferrare un attacco contro terzi secondo il cosiddetto «SNMP Amplification Attack». In questo caso viene utilizzato il «Simple Network Management» dei dispositivi per lanciare un invio massivo di richieste e indirizzarlo quindi verso l'obiettivo per sovraccaricarlo e saturarne le risorse. I modem non sono infettati a tal fine, ma gli hacker sfruttano soltanto il fatto che il sistema SNMP è aperto. I problemi di funzionamento presso i clienti si sono verificati poiché le richieste hanno involontariamente sovraccaricato anche i modem, provocando quindi instabilità. Dal momento che non tutti i clienti Quickline utilizzano gli stessi modem, sono stati colpiti circa 9000 clienti, quindi solo il 5 per cento. Non è noto per quanto tempo i modem siano rimasti vulnerabili a questo tipo di attacco. Per eliminare le falle di sicurezza, Quickline ha adottato diverse misure, in particolare inserendo filtri nella rete e aumentando la sicurezza dei modem colpiti. Inoltre, ha avviato azioni legali.

4.3.2 Dati fiscali nella rete – app con un'impostazione errata

Compilare la dichiarazione fiscale è spesso un lavoro noioso e non esattamente il passatempo preferito di molti. La società zurighese Zurich Financial Solutions (www.zufiso.ch) ha sviluppato l'app per smartphone Steuern59.ch per facilitare l'intero processo. L'app può essere acquistata e scaricata nel PlayStore o nell'AppleStore. L'app promette di compilare la dichiarazione fiscale per soli 59 franchi. Basta fotografare i documenti necessari con lo smartphone e caricarli sull'app. Tuttavia, è emerso che tutti questi documenti sensibili sono stati caricati su un cloud server non protetto di Amazon Web Services (AWS), quindi erano accessibili a tutti i membri di AWS. Nelle impostazioni standard i dati sono «privati», quindi non visionabili pubblicamente. Modificando queste impostazioni su «pubblici», appare un avviso[13]. Tuttavia i programmatori, presumibilmente di origine indiana, che sono stati ingaggiati per sviluppare l'app, hanno commesso un errore: hanno selezionato l'impostazione «pubblici» e si sono apparentemente dimenticati di ripristinare l'opzione «privati». Un ricercatore in materia di sicurezza ha scoperto l'errore nella configurazione e ha informato l'operatore, ma solo dopo essersi rivolto alla rivista tedesca Heise è stato preso sul serio dalla società[14]. Questo caso solleva il problema della gestione delle falle scoperte («responsible disclosure»): come i ricercatori debbano segnalare le falle di sicurezza scoperte e come queste segnalazioni debbano essere gestite dalle aziende. La società che gestisce Steuern59.ch ha ammesso di aver esternalizzato la produzione dell'app in India, ignara del lavoro poco accurato degli sviluppatori. Gli 80 clienti colpiti che utilizzavano l'app sono stati informati dell'incidente, dopo che la falla era stata risolta in collaborazione con il ricercatore che si occupa di cibersicurezza. I dati sono ora memorizzati su una cloud svizzera chiamata «n'cloud»[15].

---

13 https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html (stato: 31 gennaio 2019)

14 https://www.inside-it.ch/articles/52273 (stato: 31 gennaio 2019)

15 https://www.heise.de/newsticker/meldung/Steuern59-ch-Geschaeftsfuehrung-entschuldigt-sich-fuer-Daten-leck-4169772.html (stato: 31 gennaio 2019)

4.4 Ingegneria sociale e phishing

4.4.1 Torna ad aumentare il numero delle truffe telefoniche presso le aziende

All'inizio di luglio del 2018 sono state nuovamente registrate telefonate in cui i criminali si spacciavano per dipendenti di una banca. In queste occasioni si chiedeva all'interlocutore di eseguire pagamenti oppure veniva annunciato il necessario aggiornamento dell'e-banking, da testare successivamente.

Normalmente i criminali cercano di convincere i collaboratori di un'azienda a installare un software ad accesso remoto (ad esempio NTR-Cloud o Teamviewer), dopo di che si collegano al computer della vittima e fingono di installare un aggiornamento dell'e-banking. I criminali fanno poi credere che l'aggiornamento debba essere testato e sollecitano la vittima a inserire i propri dati di accesso all'e-banking della società ed eseguire un pagamento di prova, per verificare il funzionamento del sistema. Se il pagamento è protetto da una firma collettiva, i malviventi cercano di convincere la vittima a riunire tutti gli aventi facoltà di firma per autorizzare il pagamento.

In un'altra variante, le vittime ricevono istruzioni di non utilizzare l'e-banking per alcuni giorni a causa di aggiornamenti urgenti. Nel caso di operazioni indifferibili, la vittima dovrà contattare un numero di telefono indicato dai malviventi. La vittima che telefona al presunto collaboratore della banca per svolgere l'operazione nell'e-banking sarà invitata a fornire il nome utente, la password e anche il codice univoco. I criminali ottengono così l'accesso all'e-banking dell'azienda e possono ripetere questa azione fino a quando la vittima non si insospettisce.

Raccomandazione

Gli esempi evidenziano la persistente attualità dei metodi di ingegneria sociale. Le imprese dovrebbero controllare quali informazioni che le concernono sono disponibili online. Non pubblicate mai nei Vostri siti gli indirizzi e-mail della direzione o dei collaboratori. Utilizzate indirizzi e-mail impersonali (ad es. «contabilità@xyz.ch»).

Diffidate di chi vi contatta con richieste insolite e verificate in modo critico l'identità del vostro interlocutore. Se qualcuno si mette in contatto con voi o vi formula richieste in modo inconsueto, si raccomanda di consultare i colleghi all'interno dell'azienda per verificare la correttezza dell'incarico. Sensibilizzate in proposito i collaboratori, in particolare quelli che rivestono posizioni chiave.

Non rivelate mai a terzi i dati di accesso personali per telefono, e-mail o su Internet. Gli istituti finanziari non vi chiederanno mai telefonicamente, per e-mail o con un SMS di fornire dati personali confidenziali.

Non installate mai software e non aprite link se vi viene richiesto per telefono o per scritto. Non consentite mai un accesso remoto al vostro computer. Nessuna banca vi chiederà di partecipare ai test di qualunque aggiornamento di sicurezza.

Tutti i processi che riguardano il traffico pagamenti dovrebbero essere chiaramente regolamentati all'interno dell'azienda ed essere sistematicamente osservati dai collaboratori in tutti i casi.

4.4.2 Tentativi di estorsione – un bluff redditizio

Da qualche tempo esiste una forma di truffa strettamente correlata all'utilizzo dei social media. Nella maggior parte dei casi una persona molto avvenente contatta la potenziale vittima tramite i social media, si finge interessata nei suoi confronti e la induce a spogliarsi davanti alla webcam. La vittima non sa di essere filmata, ma i video così ottenuti saranno poi utilizzati per ricattarla. Questo metodo di estorsione è chiamato «Sextortion». Se la vittima si rifiuta di pagare, il materiale viene pubblicato. Questa forma di truffa è piuttosto onerosa. Dal momento che viene instaurato un contatto diretto tra l'autore e la vittima, aumenta anche il rischio di essere arrestati.

Dal mese di marzo del 2018 (in Svizzera da luglio), i criminali utilizzano uno stratagemma molto meno oneroso e rischioso. Sempre in una e-mail sostengono di avere accesso al computer e alla webcam e minacciano di pubblicare immagini e filmati a sfondo sessuale. In questi casi, tuttavia, gli autori della truffa bluffano poiché non esistono né fotografie né riprese video, dal momento che non c'è stato alcun contatto personale. Tale truffa è nota come «fake sextortion». Con questo metodo i criminali hanno incassato parecchio denaro nel secondo semestre del 2018 nonostante le modeste somme richieste. In base alle analisi degli indirizzi bitcoin contenuti nelle e-mail che sono stati segnalati a MELANI e sui quali doveva essere pagato il riscatto, nel secondo semestre del 2018 sono stati versati circa 100 bitcoin, attualmente pari a un controvalore di circa 360 000 franchi. Dal momento che l'invio di e-mail di massa è praticamente gratuito, il guadagno è proporzionalmente elevato. Non si sa se tali indirizzi bitcoin siano utilizzati esclusivamente per questo tipo di truffa.

Come «prova» che il computer è stato compromesso, nelle e-mail è spesso indicata una password proveniente da una fuga di dati. Nella maggior parte dei casi la password è obsoleta e non viene più utilizzata. Per convincere la vittima che il suo telefonino è stato compromesso, nel frattempo vengono utilizzati anche numeri di cellulare. Questi dati «non sensibili» provenienti da diverse fughe di dati sono pubblicati più spesso negli ultimi tempi. In un'altra variante la prova che l'account di posta elettronica sia stato pregiudicato è fornita con un messaggio inviato dall'indirizzo dell'utente stesso. In realtà, i truffatori hanno solo falsificato il mittente, con un inganno semplice e che può essere messo in pratica senza grandi conoscenze informatiche. Per commettere questa truffa non è necessario avere accesso all'account di posta elettronica.

Le e-mail dei ricattatori sono redatte in diverse lingue, tra cui francese, inglese, italiano e tedesco. Il modus operandi non è cambiato nella sostanza, tuttavia i criminali lavorano per ottimizzare i loro tentativi di estorsione, al fine di aumentare la pressione esercitata sulle vittime e costringerle a pagare. Il seguente elenco cronologico illustra le principali innovazioni adottate dai truffatori nel corso del 2018.

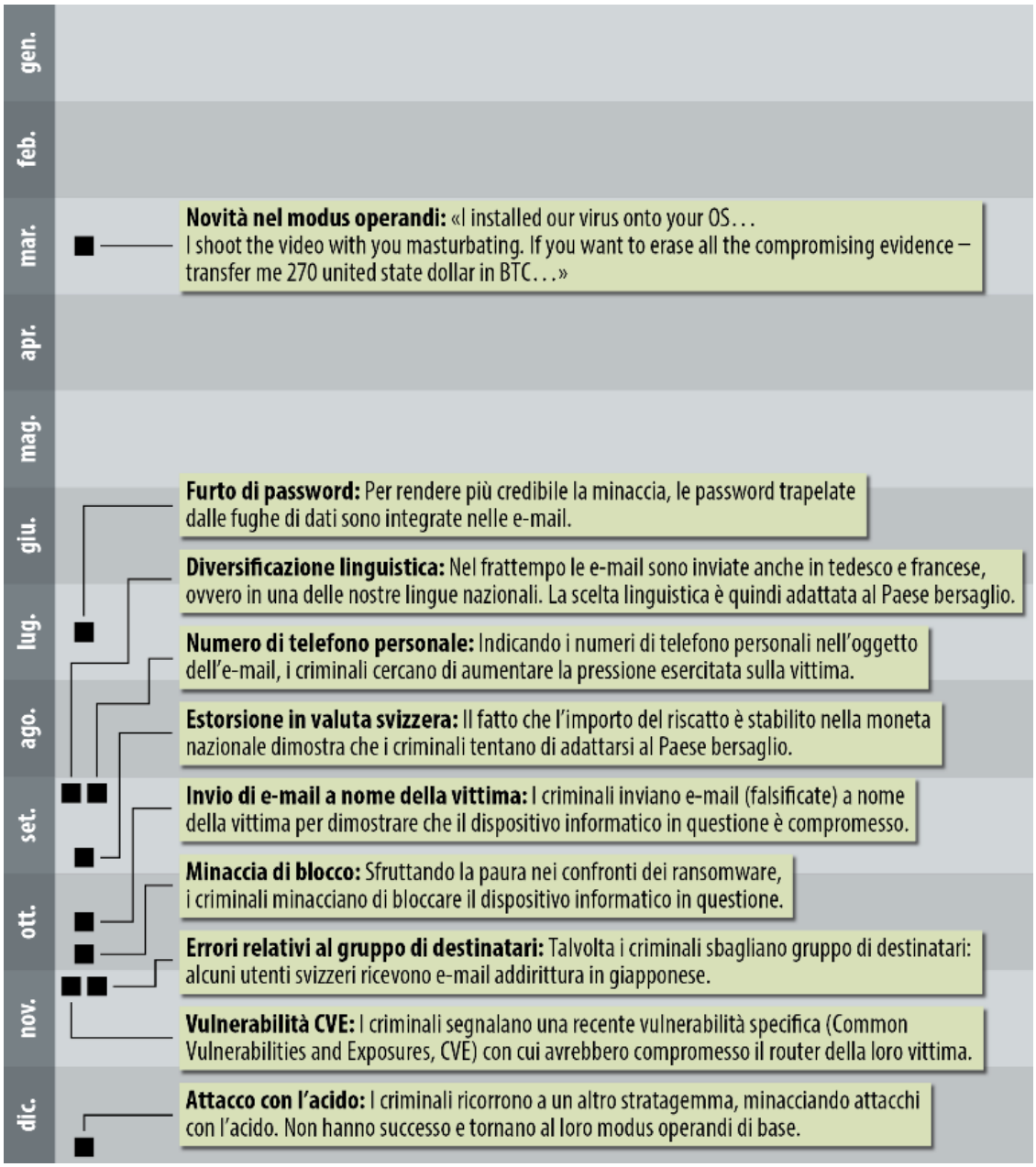


Figura 2: Evoluzione delle varianti di «fake sextortion» nel 2018

Una sottocategoria del fenomeno è rappresentata dai ricatti con la minaccia di un attacco con esplosivo o con acido. In entrambe le varianti si chiede di pagare il riscatto sempre in bitcoin per evitare l'attentato. Si è tuttavia constatato che i destinatari sono più intimiditi e hanno più paura quando sono minacciati fisicamente, quindi tendono a rivolgersi alle autorità prima di pagare il riscatto. In ogni caso, sugli indirizzi bitcoin segnalati a MELANI in rapporto con questa minaccia non sono state riscontrate transazioni.

Raccomandazione

Fino a quando le vittime di questi ricatti continueranno a pagare il riscatto, tale modo di procedere verrà incoraggiato: c'è da aspettarsi che le ondate continuino, seguano emulatori e le truffe aumentino ulteriormente. Quindi non pagate mai un riscatto. Potete contribuire alla prevenzione tematizzando il modus operandi dei truffatori nel vostro ambiente professionale e privato.

In questo modo sensibilizzate collaboratori, conoscenti e parenti, affinché non diventino vittime di tali truffe. Il sito www.stop-sextortion.ch , lanciato dalle autorità, fornisce informazioni utili e permette di segnalare le e-mail di fake sextortion.

4.4.3 I dati di accesso a Office 365 utilizzati per la truffa dei bonifici

Nei precedenti rapporti semestrali[16] è già stato tematizzato che i dati di accesso a Office 365, la versione online dei prodotti di Office, sono molto ambiti dai criminali. Con oltre 100 milioni di utenti mensili, gli account di Office 365 sono diventati un bersaglio popolare tra i criminali informatici. L'attacco inizia con una normale e-mail di phishing in cui viene finto, ad esempio, che il limite di spazio a disposizione sia stato superato e che sia necessario effettuare il login per risolvere il problema. Va da sé che il link fornito porta a un sito web fraudolento.

Nel periodo in esame le credenziali così ottenute di Office 365 hanno consentito sempre più spesso la cosiddetta truffa dei bonifici («wire fraud»). Sono i casi in cui i criminali cercano fatture elettroniche presenti nei conti manipolati, le copiano, vi inseriscono un diverso numero IBAN e le riemettono. I bersagli privilegiati sono le aziende che fatturano somme ingenti a destinatari esteri. Da un lato questo modus operandi è particolarmente lucrativo, dall'altro è più difficile individuare il conto di un destinatario abusivo, poiché si tratta di conti all'estero.

Quanto sofisticati siano questi attacchi lo dimostra un esempio fornito dalla società di sicurezza Proofpoint. Dopo aver ottenuto l'accesso all'account di Office 365 del CEO di una società, i criminali informatici hanno cercato nelle e-mail e nell'agenda informazioni utili per creare una vicenda credibile. Durante una riunione registrata nell'agenda del CEO con un importante fornitore, l'hacker ha scritto al capo Finanze di trasferire un milione di dollari statunitensi per concludere l'affare. Nella comunicazione ha precisato di essere impegnato nella riunione, quindi di non riuscire a telefonare. Il capo Finanze ha dato seguito alla richiesta e ha pagato.[17]

Secondo l'FBI, autorità statunitense per la sicurezza, questo modus operandi, chiamato «Business E-Mail Compromise (BEC)», è ormai diventato uno dei più dannosi in ambito finanziario. Negli Stati Uniti nel 2018.sono stati segnalati all'Internet Crime Complaint Center (IC3) casi

16 MELANI rapporto semestrale 2/2017 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2-2017.html (stato: 31 gennaio 2019)

17 https://www.proofpoint.com/us/corporate-blog/post/microsoft-office-365-attacks-circumvent-multi-factor-authentication-lead-account (stato: 31 gennaio 2019)

che hanno provocato perdite complessive pari a 1,2 miliardi di dollari statunitensi. Questo tipo di attacco colpisce in particolare il settore immobiliare.[18]

Raccomandazione

Se una società lavora nella cloud di Office 365, i dati rubati consentono agli hacker di accedere a tutti i suoi documenti. Oggi, mettere in sicurezza questi dati soltanto con nome utente e password è estremamente pericoloso. Ogni qualvolta possibile, attivate dunque l'autenticazione a due fattori, che tuttavia deve essere applicata correttamente. Infatti, il sistema può essere manipolato anche ricorrendo all'autenticazione unica («single sign-on», SSO) o all'autenticazione a più fattori («multi-factor authentication», MFA), se l'autenticazione non è attuata trasversalmente tra i sistemi. Tali lacune possono essere sfruttate dai cibercriminali.

I collaboratori dovrebbero essere sensibilizzati in modo che tutti seguano sempre i processi stabiliti dalla società e le misure cautelari. Nel caso dei bonifici, ad esempio, si raccomanda di osservare il principio del doppio controllo con firma collettiva.

4.4.4 Giochi a premi contraffatti

Cioccolata in regalo per un anno intero, un buono di IKEA o un nuovo iPhone: i presunti giochi a premi sono molto diffusi in rete. Ne abbiamo già riferito nel nostro ultimo rapporto semestrale[19]. In tutti questi giochi a premi le domande sono scelte in modo tale che chiunque possa rispondervi facilmente. Al fine di mietere quante più vittime, gli autori della truffa vogliono infatti che il maggior numero possibile di concorrenti «vinca». Nel periodo in esame è emersa una nuova variante. I potenziali vincitori sono attirati tramite facebook su un presunto sito della Denner e sono indotti a credere di aver vinto 750 franchi. Una volta che hanno fornito nome e numero di telefono, i partecipanti sono pregati di telefonare a un numero 0901 a pagamento. Per entrare in possesso della presunta vincita, devono rispondere al maggior numero possibile di domande. In realtà la molteplicità delle domande serve solo a trattenere le vittime a lungo sulla linea a pagamento. Va da sé che la vincita è un miraggio.

---

18 https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf (stato: 25 aprile 2019)
https://www.ic3.gov/media/2018/180712.aspx#fn2 (stato: 31 gennaio 2019)

19 Rapporto semestrale MELANI 2018/I
https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2018-1.html (stato: 31 gennaio 2019)

Raccomandazione

Vagliate con occhio critico i messaggi che promettono vincite allettanti e non inoltrateli mai. La cosa migliore da fare è ignorarli.

INFO

La protezione dei consumatori ha messo a punto una serie di consigli in proposito:

https://www.konsumentenschutz.ch/was-tun-bei-einer-abofalle/

4.4.5 Phishing

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

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

Nel 2018 sono stati segnalati complessivamente 5756 diversi casi inequivocabili di pagine web di phishing sul portale antiphishing.ch, gestito da MELANI. La figura 3 mostra i siti web di phishing segnalati ogni settimana. Colpisce il picco toccato negli ultimi tre mesi del 2018. Il motivo principale è una campagna su larga scala che ha interessato le carte di credito UBS in quel periodo.

Figura 4: Phishing di carte di credito UBS negli ultimi tre mesi del 2018.

Già diversi anni fa MELANI aveva previsto che anche per i siti di phishing sarebbero stati utilizzati sempre più spesso siti web crittografati con l'URL «https://», tuttavia questo sviluppo è stato più lento del previsto. Dal terzo trimestre del 2016 la società di sicurezza PhishLab registra un crescita costante e alla fine del 2018 ha annunciato per la prima volta una quota del 50 per cento di siti di phishing crittografati.[20] Questa constatazione dovrebbe tuttavia avere a che fare non tanto con un modus operandi mirato dei criminali, ma semplicemente con la sempre maggiore frequenza di siti web crittografati. Dal momento che la stragrande maggioranza dei siti di phishing è hackerata, i criminali «ne approfittano» e usano la crittografia in modo consapevole e, in parte, anche inconsapevole.

4.4.6 Richieste di blocco secondo l'articolo 15 ODIn

Per contrastare gli abusi di indirizzi Internet svizzeri ed evitare forti pericoli per gli utenti della rete, nella revisione dell'ordinanza concernente gli elementi d'indirizzo nel settore delle telecomunicazioni (ORAT, RS 784.104; in vigore dal 1° gennaio 2010) è stato introdotto un nuovo articolo secondo cui il gestore del registro «.ch» (SWITCH) è tenuto a bloccare un nome di dominio e a sopprimerne l'attribuzione a un server di nomi se sussiste il sospetto fondato che questo nome di dominio sia utilizzato per appropriarsi di dati degni di protezione tramite metodi illegali (phishing) o diffondere tramite questo dominio software dannosi (malware) e un ente per la lotta contro la cibercriminalità riconosciuto dall'Ufficio federale delle comunicazioni (UFCOM) ha presentato una richiesta di blocco del nome di dominio.

Dal 15 giugno 2010 MELANI è l'ente riconosciuto dall'UFCOM ed è pertanto autorizzato a chiedere a SWITCH di bloccare nomi di dominio «.ch» e sopprimere la loro attribuzione a un server di nomi se vi è il sospetto fondato di phishing o della propagazione di malware.

I blocchi richiesti da MELANI riguardano prevalentemente siti di phishing. Dopo che nel 2016 e nel 2017 sono stati bloccati oltre 30 siti, il numero è sceso a 16 nel 2018. Questo numero esiguo deriva dal fatto che sono bloccati soltanto i siti utilizzati esclusivamente per compiere attacchi di phishing o propagare malware. Tuttavia, la maggior parte dei siti di phishing si trova su sistema manomessi sui quali sono memorizzati anche altri contenuti. In questi casi i domini non sono bloccati, ma si cerca di eliminare dalla rete il sito fraudolento tramite il provider.

[20] https://info.phishlabs.com/blog/49-percent-of-phishing-sites-now-use-https (stato: 31 gennaio 2018)

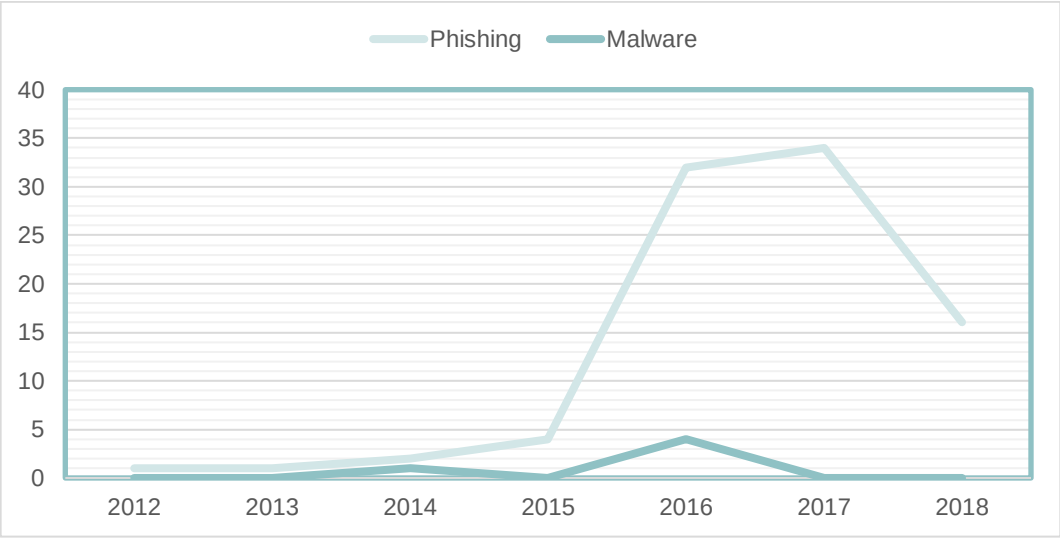


Figura 5: Blocchi chiesti da MELANI secondo l'articolo 15 ODIn. In celeste le richieste di blocco di siti di phishing e in blu scuro le richieste per i siti con malware.

4.5 Crimeware

Anche nel primo semestre del 2018 sono state perpetrate numerose infezioni con software criminali («crimeware»). La statistica della figura 6 presenta la distribuzione dei principali software malevoli in Svizzera. Esistono anche malware che, pur essendo rilevanti, non appaiono nelle statistiche, ad esempio il malware e-banking Retefe.

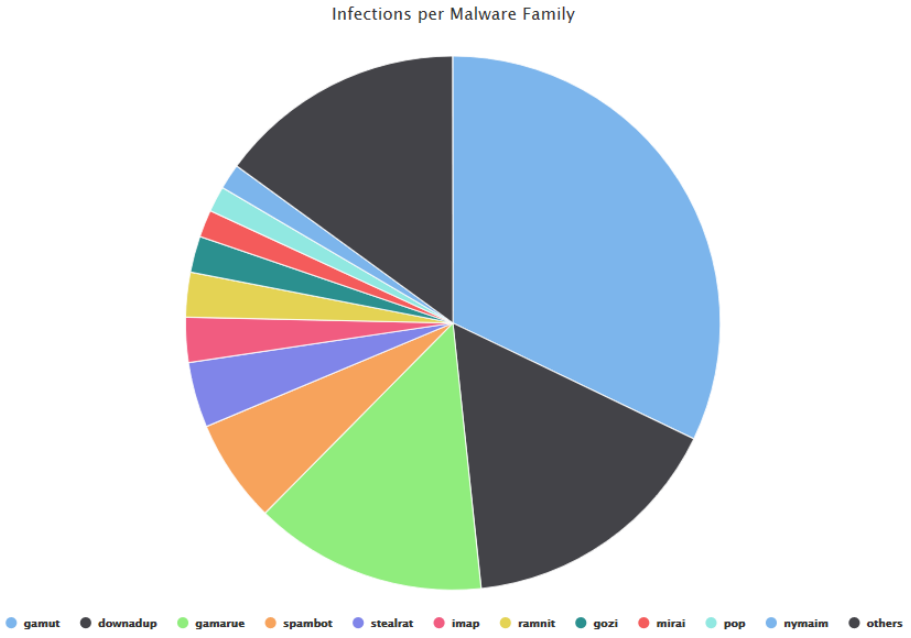


Figura 6: Distribuzione in Svizzera dei malware noti a MELANI al 31 dicembre 2018. I dati aggiornati sono pubblicati all'indirizzo: http://www.govcert.admin.ch/statistics/dronemap/

Per la prima volta da quando esiste questa statistica, il malware Downadup (noto anche come «Conficker») non figura più al primo posto. Per il secondo semestre del 2018 in vetta alla classifica si trova Gamut, responsabile di gran parte dello spam spedito nel mondo. Questa botnet invia spam legati soprattutto alle offerte di lavoro per il reclutamento di «money mule» o agenti finanziari[21]. Al terzo posto si trova Gamarue[22], noto anche come «Andromeda», un downloader in grado di scaricare altri malware. Al quarto e al quinto posto si posizionano rispettivamente Spambot e Stealrat, anch'essi responsabili dell'invio di spam. Stealrat agisce mediante domini, tra i quali si trovano WordPress, Joomla! e Drupal. I messaggi spam sono così inviati tramite server di posta elettronica legittimi, quindi più difficili da filtrare. All'ottavo posto si trova Gozi, il primo trojan bancario. La botnet Mirai, nota per l'attacco al fornitore di servizi Internet Dyn, è rientrata nella top ten ed estromette il cryptominer Monerominer.

4.5.1 Retefe, il più importante trojan bancario in Svizzera

Retefe si conferma uno dei più importanti trojan bancari in Svizzera. Il malware viene inviato per posta elettronica a nome di società o istituzioni conosciute e prende di mira i sistemi Windows e macOS. Nella maggior parte dei casi, viene allegato alle mail un documento Word dannoso, ad esempio una presunta fattura dello shop online, una conferma di invio di un fornitore di pacchi o informazioni dell'Amministrazione federale concernenti la contaminazione dell'acqua potabile. La figura 7 illustra il numero di ondate di spam registrate negli ultimi tre anni.

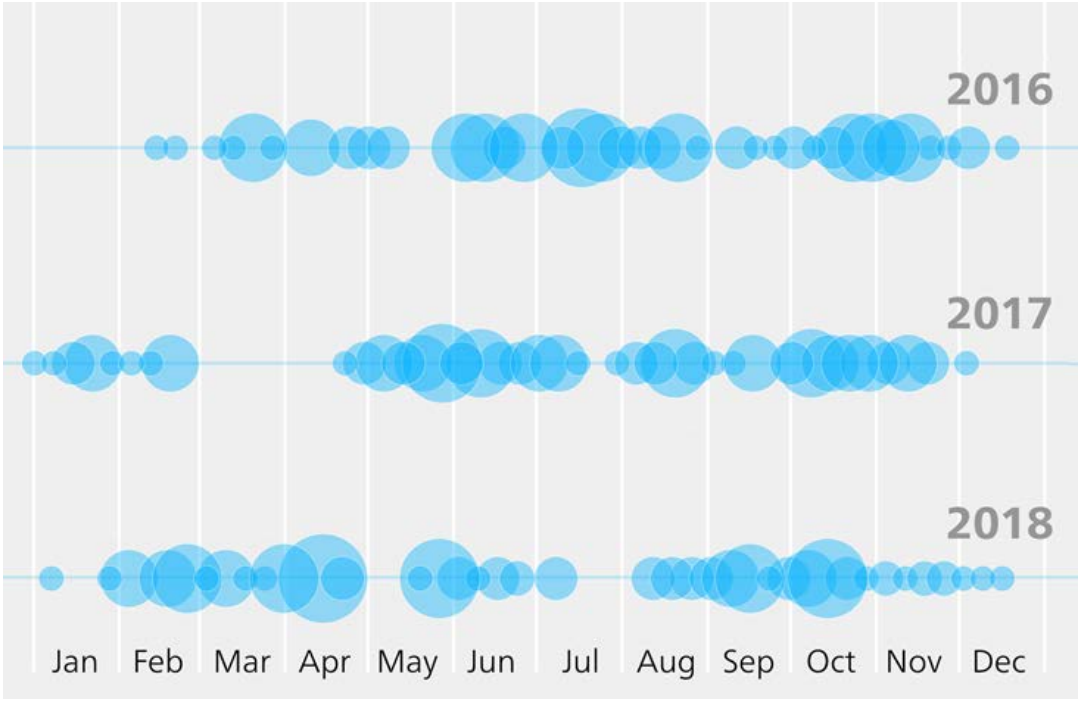


Figura 7: Ondate di Retefe negli ultimi tre anni. I cerchi blu rappresentano il numero delle diverse ondate di spam.

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

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

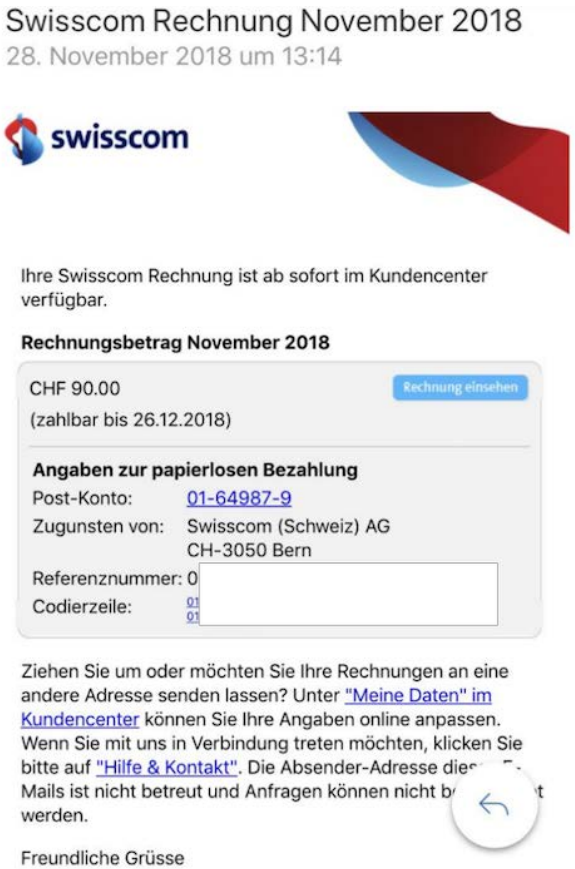
Retefe tenta inoltre di rendere le e-mail più attendibili inserendo nel corpo del messaggio informazioni personali tra cui il numero di telefono o l'indirizzo del destinatario. Questi dati sono stati rubati. Per il momento Retefe prende di mira soltanto clienti privati in Svizzera, nel Liechtenstein e in Norvegia. Le aziende sono meno colpite da Retefe. Da un lato i sistemi di pagamento offline non sono attaccati direttamente, dall'altro Retefe deve modificare le impostazioni di proxy, nonché installare un certificato principale e una porta. Per i computer delle aziende questi diritti dovrebbero essere limitati evitando così simili manipolazioni.

Raccomandazione

Siate particolarmente cauti nell'aprire documenti Word. Normalmente le aziende e le organizzazioni inviano file in formato pdf e non Word negli scambi commerciali (ad es. fatture, offerte ecc.).

4.5.2 Gozi torna attivo

Dopo un lungo periodo contrassegnato da pochi attacchi Gozi in Svizzera, il 28 novembre 2018 è emersa un'ondata di e-mail con una fattura Swisscom contraffatta. Gli hacker hanno abilmente utilizzato metodi di ingegneria sociale.


Swisscom Rechnung November 2018
28. November 2018 um 13:14

swisscom

Ihre Swisscom Rechnung ist ab sofort im Kundencenter verfügbar.

Rechnungsbetrag November 2018

CHF 90.00 Rechnung einsehen
(zahlbar bis 26.12.2018)

Angaben zur papierlosen Bezahlung
Post-Konto: 01-64987-9
Zugunsten von: Swisscom (Schweiz) AG
CH-3050 Bern
Referenznummer: 0
Codierzeile:

Ziehen Sie um oder möchten Sie Ihre Rechnungen an eine andere Adresse senden lassen? Unter "Meine Daten" im Kundencenter können Sie Ihre Angaben online anpassen. Wenn Sie mit uns in Verbindung treten möchten, klicken Sie bitte auf "Hilfe & Kontakt". Die Absender-Adresse dies... Mails ist nicht betreut und Anfragen können nicht b...t werden.

Freundliche Grüsse

Figura 8: Fattura Swisscom contraffatta con un link a un file malevolo

La mail contiene un link a un file ZIP, con uno script Visual Basic offuscato (camuffato) che viene avviato tramite powershell "bitsadmin"[23]. In tal modo il vero e proprio malware è scaricato, memorizzato nel profilo provvisorio dell'utente, quindi avviato.

Oltre alle informazioni sui server del tipo «command and control», la configurazione di Gozi contiene dati necessari all'utilizzo di un algoritmo di generazioni di domini («domain generation algorithm», DGA). Questi nomi di dominio si basano su parole della Costituzione statunitense, scelte casualmente e poi ricomposte[24]. Così possono essere definiti punti di contatto dinamici per i server di controllo se quelli fissi non funzionano più. Nel caso in questione, tuttavia, questa funzione non è stata utilizzata.

Nella sua configurazione Gozi contiene, da un lato, banche da attaccare e, dall'altro, prodotti software che devono essere sorvegliati. Il malware mira anche a software di pagamento offline e prende di mira direttamente pure le aziende.

Raccomandazione

Si raccomanda in particolare alle PMI di utilizzare per i pagamenti dispositivi propri, dedicati con accesso limitato a Internet, sui quali non navigare né scrivere e-mail, di aggiornare il dispositivo e il software installato nonché di memorizzare le password in un apposito software. Nell'autorizzazione dei pagamenti si raccomanda di osservare il principio del doppio controllo e di sbloccarli su un secondo dispositivo, anch'esso protetto. I pagamenti sospetti dovrebbero sempre essere segnalati tempestivamente alla banca.

4.5.3 App bancarie contraffatte

Nell'epoca degli smartphone, le app hanno un ruolo centrale. Per i criminali hanno tuttavia il difetto che, a differenza di un browser standard, sono costruite prevalentemente in modo proprietario. A differenza di quanto avviene per un browser standard, se una app viene abusata l'offerente e lo sviluppatore hanno la possibilità di modificare direttamente il codice e di reagire agli attacchi con opportuni meccanismi di sicurezza. Per i criminali diventa dunque più difficile attaccare una app e manipolarla.

Ecco perché tentano soprattutto di mettere in circolazione app contraffatte piuttosto che manomettere quelle legittime. Proprio in ambito finanziario, molte di queste app contraffatte riescono a farsi strada negli store, ufficiali e non. Le cosiddette «fake app» hanno una struttura piuttosto semplice e, una volta avviate, appaiono i campi di un modulo da compilare con i dati delle carte di credito, il login e le password. Le vittime vengono adescate con nomi e loghi simili a quelli delle banche per indurle a scaricare queste app. I criminali hanno anche altri metodi di ingegneria sociale nel loro repertorio: ad esempio, sostengono che il limite di credito presso la rispettiva banca possa essere aumentato con una app (contraffatta).

Con Google Play Protect Google ha sviluppato un filtro che lo scorso anno è riuscito, per la prima volta, a frenare la diffusione di malware tra i dispositivi Android. Ma le fake app continuano a spuntare.

---

[23] https://docs.microsoft.com/en-us/windows/desktop/bits/bitsadmin-tool (stato: 31 gennaio 2018)

[24] Blog su Gozi: https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature (in inglese; stato: 31 gennaio 2018)

A fine settembre anche Postfinance è stata interessata da una di queste: l'app contraffatta non chiedeva dati di accesso all'e-banking né altre password. Gli hacker avevano puntato ai dati delle carte di credito. Una volta che la vittima li aveva inseriti, appariva un messaggio di ringraziamento e l'app si chiudeva. Al più tardi in quel momento le vittime dovevano insospettirsi e mettersi in contatto con il proprio fornitore di servizi Internet oppure con la società emittente della carta di credito[25].

4.5.4 Ransomware

Oggi le estorsioni commesse mediante software di crittografia, cosiddetti ransomware, sono sicuramente tra gli attacchi più carichi di conseguenze per le PMI, ma anche per le infrastrutture critiche informatizzate, come dimostrano gli esempi illustrati al capitolo 5.3.5 Attualmente i più diffusi sono Ryuk, GandCrab, Dharma e Locky. Nel sito botfrei.de è pubblicata una panoramica di tutti i tipi di ransomware[26].

Ryuk si contraddistingue soprattutto per il suo modus operandi che consiste prima nel raccogliere dati, poi crittografare in modo mirato i sistemi di vittime promettenti in termini di guadagno. Il 12 dicembre 2018 MELANI ha diffuso un'allerta sulle diverse ondate di malspam che avevano in allegato documenti Word infetti[27]. Ryuk si è propagato mediante Emotet, un trojan noto da tempo, che con e-mail fasulle a nome di colleghi, soci d'affari o conoscenti prova, ricorrendo all'ingegneria sociale, a convincere il destinatario ad aprire il documento Word allegato ed eseguire le macro di Office che vi sono contenute. Originariamente conosciuto come trojan dell'e-banking, Emotet è oggi utilizzato soprattutto per inviare spam e scaricare altri malware. In questo caso è stato scaricato il malware Trickbot, che ha cercato di prendere il controllo dei computer infetti. Una volta installato, Trickbot svolgeva un'analisi completa della rete per individuare se il computer facesse parte di un'azienda o di un'organizzazione importante e tentava di propagarsi all'interno di questa rete mediante la nota falla di sicurezza SMB. Il malware continuava a comunicare con il server di controllo e solo quando il bersaglio era ritenuto sufficientemente di alto profilo veniva scaricato il ransomware Ryuk, che crittografava i dati presenti sui computer e sui server della rete aziendale. Si ritiene che, con questo attacco molto mirato, i cibercriminali siano riusciti a estorcere bitcoin per un controvalore di circa 3,7 milioni di dollari americani dal mese di agosto del 2018[28]. Non è noto quanto abbia potuto essere convertito in denaro fisico, né da dove operino gli autori degli attacchi.

---

25 https://www.blick.ch/news/wirtschaft/ueber-1000-opfer-falsche-postfinance-app-in-play-store-gebracht-id8881643.html (stato: 31 gennaio 2019)

26 https://www.botfrei.de/de/ransomware/galerie.html (stato: 31 gennaio 2019)

27 https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/Trojaner_Emotet_greift_Unternehmensnetzwerke_an.html (stato: 31 gennaio 2019)

28 https://derstandard.at/2000096143241/Ryuk-Neue-Ransomware-brachte-Cyberkriminellen-vier-Millionen-Dollar (stato: 31 gennaio 2019)

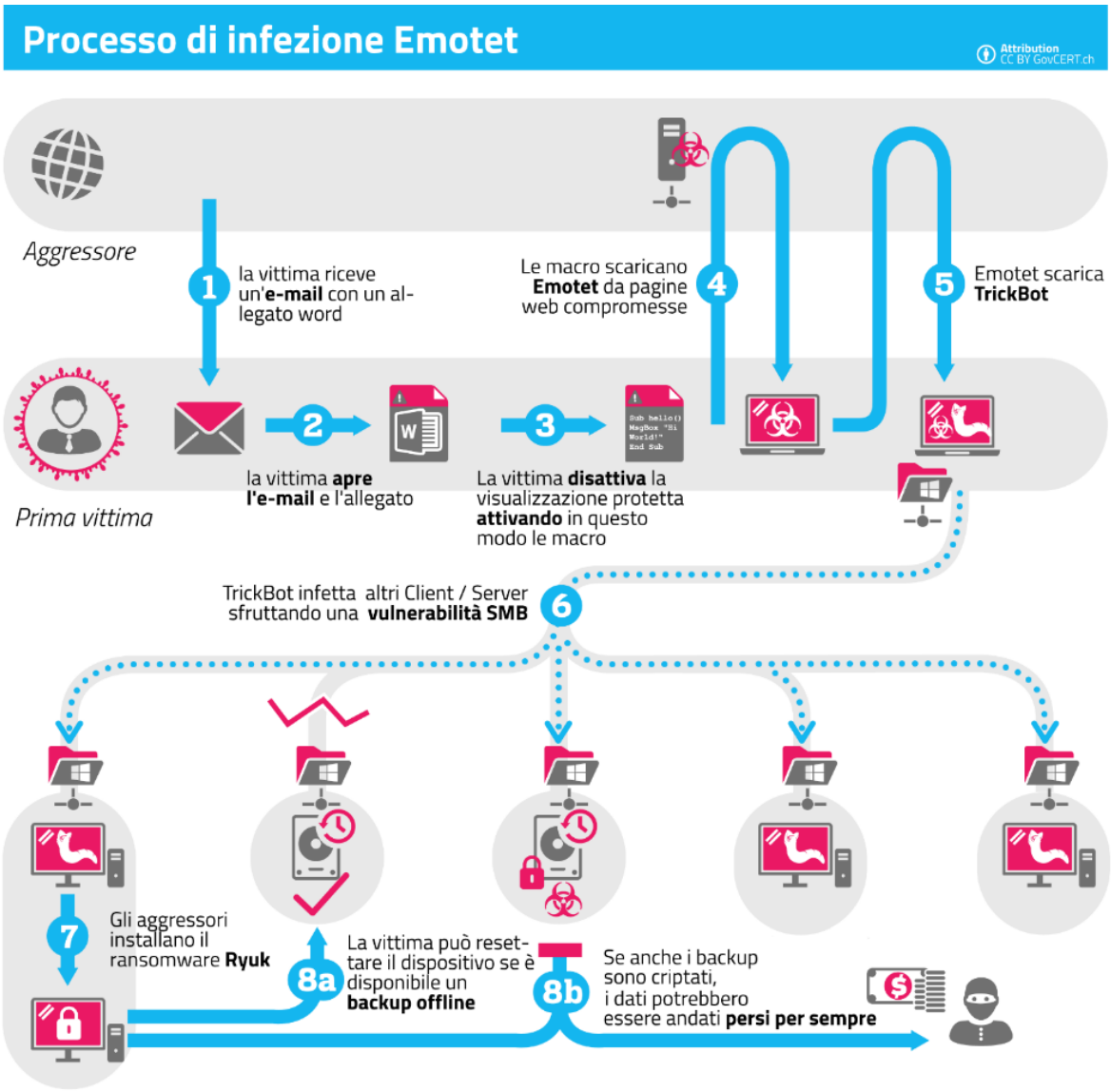


Figura 9: Processo di infezione del malware Emotet

Nel secondo semestre del 2018 sono stati più volte segnalati casi in cui era coinvolto il ransomware GandCrab. Apparso per la prima volta nel mese di gennaio del 2018[29], si contraddistingue soprattutto per la molteplicità di vettori con cui si propaga l'infezione. Inizialmente GandCrab si diffondeva utilizzando le e-mail di spam. Con la versione 4, nell'estate del 2018 gli hacker hanno modificato il modus operandi e per la diffusione sfruttavano siti web sui quali venivano offerte versioni illegali «craccate» di software a pagamento. Spesso si tratta di siti contraffatti, attivati dagli stessi ricattatori e reperiti mediante la ricerca di Google. Nel repertorio dei metodi di diffusione si annoverano anche dossier di candidatura manomessi[30]. Nel mese di agosto del 2018 la società di sicurezza informatica FireEye ha riferito che il ransomware

29 https://blog.comodo.com/comodo-news/gandcrab-the-new-version-of-ransomware/ (stato: 31 gennaio 2019)

30 https://www.heise.de/security/meldung/Erpressungstrojaner-Gandcrab-verbreitet-sich-ueber-gefaelschte-Bewerbungsmails-4154167.html (stato: 31 gennaio 2019)

GandCrab utilizza un exploit-kit su siti web manomessi. Viene inoculato in siti infetti e sfrutta due falle di sicurezza di Windows[31].

Il ransomware Dharma è attivo già dal 2016, ma rimane uno dei trojan di crittografia più pericolosi. I criminali che si celano dietro questo malware pubblicano continuamente nuove varianti con diverse crittografie che non è possibile decriptare. Il ransomware Dharma è salito alla ribalta delle cronache nel secondo semestre del 2018 soprattutto a causa di due vittime che hanno calamitato un forte interesse mediatico: il birrificio scozzese Arran Brewery e un grosso porto marittimo (cfr. anche capitolo 5.3.5).

Nel periodo in esame non sono comunque mancate le buone notizie: il 26 novembre 2018 l'FBI ha reso noto di avere identificato due autori del ransomware SamSam. Si trattava di due cittadini iraniani di 28 e 35 anni, ufficialmente accusati dal Dipartimento della giustizia statunitense. Sembra che i criminali siano riusciti a incassare oltre 6 milioni di dollari statunitensi dalle vittime ricattate che operavano in diversi settori, tra cui anche infrastrutture critiche del sistema sanitario, dei trasporti e dell'amministrazione.

Raccomandazione

Eseguite regolarmente una copia di sicurezza (backup) dei Vostri dati. La copia di sicurezza dovrebbe essere salvata offline, cioè su un supporto esterno, ad esempio un disco rigido esterno. Scollegate il supporto su cui eseguite la copia di sicurezza dal computer subito dopo il processo di backup. In caso contrario, l'attacco di un ransomware cifrerebbe probabilmente anche i dati salvati sul supporto per backup rendendoli inaccessibili.

Segmentate la Vostra rete. Staccate dal resto della rete le unità particolarmente a rischio, ad esempio l'ufficio del personale o il servizio stampa, che devono aprire allegati da mittenti sconosciuti.

INFO

Pagina informativa di MELANI sui ransomware

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

31 https://www.fireeye.com/blog/threat-research/2018/09/fallout-exploit-kit-used-in-malvertising-campaign-to-deliver-gandcrab-ransomware.html (stato: 31 gennaio 2019)

5 La situazione a livello internazionale

5.1 Spionaggio

5.1.1 APT 10

Il 20 dicembre 2018 il Dipartimento della giustizia statunitense (DoJ) ha accusato due cittadini cinesi di essere penetrati illegalmente in diversi sistemi informatici e li ha incriminati per frode telematica e furto d'identità. Sembra che i due hacker siano coinvolti nella campagna di spionaggio informatico APT10. Questa campagna è conosciuta anche come «menuPass», «CVNX», «StonePanda» e «POTASSIUM», i cui primi attacchi a importanti provider di Managed IT Service (MSP) a livello mondiale risalirebbero almeno al 2016 (cfr. anche il rapporto semestrale MELANI 2017/I, cap. 5.1.1[32]). Nel documento pubblicato dal DoJ sono menzionati obiettivi presi di mira in 12 Paesi, tra cui la Svizzera.

Gli MSP sono un obiettivo interessante poiché supportano grandi aziende nella gestione della loro infrastruttura IT e possiedono diritti d'accesso diretti ai sistemi e ai dati dei loro clienti. In questa campagna gli MSP non sono neppure stati il vero e proprio obiettivo, ma sono serviti a ottenere l'accesso alle reti di molte grandi aziende. Tuttavia, il gruppo ha optato per il suddetto metodo solo dal 2016. Infatti, prima gli obiettivi venivano attaccati direttamente. Il gruppo è attivo già dal 2006 e, da allora, è illegalmente penetrato nelle reti informatiche di oltre 45 imprese tecnologiche, del Dipartimento dell'energia statunitense e della NASA. Inoltre, gli hacker sono sospettati di avere sottratto informazioni personali dei membri dell'esercito, compresi i numeri di assicurazione sociale, gli indirizzi e-mail e i dati dello stipendio di 100 000 dipendenti della Marina statunitense.

Il Dipartimento della giustizia statunitense sottolinea il rapporto dei due incriminati con il Ministero della Pubblica sicurezza cinese. Contemporaneamente gli altri quattro Paesi dell'alleanza «Five Eyes»[33] hanno preso ufficialmente posizione a favore delle dichiarazioni del Governo statunitense in merito a un coinvolgimento del Governo cinese nella campagna di spionaggio. Hanno dichiarato di avvalersi delle possibilità di attribuire pubblicamente i ciberattacchi, in particolare qualora la crescita economica globale, la sicurezza nazionale e la stabilità internazionale siano in pericolo. Inoltre, la Cina e tutti gli altri Paesi coinvolti sono stati esortati a rispettare gli impegni assunti con i diversi trattati internazionali.

5.1.2 Sviluppi di APT 28

In questa sede si è già riferito a più riprese del gruppo di spionaggio APT 28, conosciuto anche come «Sofacy» o «Fancy Bear». Si tratta della campagna di attacchi informatici più attiva e più nota al mondo. Anche nel secondo semestre del 2018 il gruppo ha ulteriormente sviluppato le proprie capacità tecniche e ampliato le funzionalità. Spicca soprattutto l'impiego di LoJax, un rootkit UEFI. Come riferito alla fine di settembre del 2018 da ESET, un'azienda che offre soluzioni per la sicurezza informatica, il rootkit è stato utilizzato per compiere operazioni contro

---

[32] Rapporto semestrale MELANI 2017/I, cap. 5.1.1 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2017-1.html (stato: 31 gennaio 2019)

[33] Stati Uniti, Gran Bretagna, Australia, Nuova Zelanda, Canada

organizzazioni nei Balcani e in altre regioni dell'Europa centrale e orientale[34]. I rootkit UEFI sono sofisticati strumenti per preparare attacchi informatici. Sono difficili da rilevare e in grado di persistere anche a fronte di misure di sicurezza informatica drastiche come la reinstallazione del sistema operativo o la sostituzione di un disco rigido. È stata la prima scoperta di un rootkit UEFI in azione.

Anche Sofacy è sospettata di essere responsabile di una funzione che può ostacolare l'analisi di documenti in un ambiente di sandbox automatizzato. Il metodo si basa sulla cosiddetta funzione «AutoClose», con la quale la macro contenuta in un documento Word viene eseguita e il codice dannoso è scaricato solo quando l'utente chiude il documento. Nell'analisi automatica i documenti rimangono normalmente aperti per un determinato periodo e ne è verificato il comportamento, tuttavia non vengono chiusi. Dal momento che il codice dannoso deve essere scaricato da un server esterno solo al momento della chiusura e non è implementato nel documento Word, l'attacco può andare a buon fine solo se il server è effettivamente online in quel momento, altrimenti non causa danni. La campagna si rivolgeva a diversi enti governativi di tutto il mondo. In un caso è stato fatto riferimento all'areo della compagnia Lion-Air precipitato il 29 ottobre 2018 e utilizzato il nome del file «crash list (Lion Air Boeing 737).docx.».

Dell'impiego del software malevolo Zebrocy da parte di Sofacy abbiamo già riferito nell'ultimo rapporto semestrale. Zebrocy è un insieme di downloader, dropper e backdoor. Mentre i downloader e i dropper si occupano delle attività di ricognizione, le backdoor assicurano la persistenza dell'accesso per svolgere le attività di spionaggio sull'obiettivo. Nel periodo in esame sono stati utilizzati nuovi componenti e Zebrocy ha vissuto un forte revival. I nuovi componenti si avvalgono, ad esempio, dei protocolli dei servizi di posta elettronica SMTP e POP3 per estrarre i dati rubati dalla rete della vittima. Nel mese di dicembre del 2018 la società di cibersicurezza PaloAlto[35] ha reso nota una nuova variante di Zebrocy con funzioni praticamente identiche, ma scritta in «Go», un nuovo linguaggio di programmazione per Sofacy. Sinora erano state viste varianti in «AutoIt», «Delphi», «VB.NET», «C#» e «Visual C++». Il motivo non è chiaro. Si presume che la diversità dei linguaggi di programmazione sia volta a ostacolare l'intercettazione.

5.1.3 Attacco mirato all'industria navale e della difesa italiana?

Tra il 9 e il 15 ottobre 2018 sono state inviate e-mail con un predisposto documento Excel ai dipendenti dell'industria navale e della difesa italiana[36]. Secondo la società italiana di sicurezza informatica Yoroi, le e-mail contenevano una richiesta di pezzi di ricambio per motori delle imbarcazioni. Gli hacker chiedevano di sottoporre un'offerta per gli articoli elencati nel file Excel, che i destinatari erano quindi costretti ad aprire. Apparentemente i criminali hanno svolto accurate ricerche preliminari, per far sembrare la richiesta il più autentica possibile, tant'è vero che è arrivata all'ufficio giusto e il linguaggio con cui è stata formulata era chiaro e corretto. Una volta aperto il file, veniva scaricato nel sistema della vittima QuasarRAT, uno strumento di amministrazione remota, con il quale gli autori dell'attacco ottenevano pieno accesso al

---

34 https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/ (stato: 31 gennaio 2019)

35 https://unit42.paloaltonetworks.com/sofacy-creates-new-go-variant-of-zebrocy-tool/ (stato: 31 gennaio 2019)

36 https://securityaffairs.co/wordpress/77195/malware/martymcfly-malware-cyber-espionage.html (stato: 31 gennaio 2019)

sistema ed erano in grado di rubare dati e manomettere i computer. Il codice sorgente di QuasarRAT è pubblico e liberamente disponibile nel servizio online GitHub. Yoroi presume che dietro gli attacchi si celi uno Stato, mentre l'azienda produttrice di software Kaspersky propende per un'origine criminale nella sua analisi. Secondo Kaspersky, la campagna ha una caratura ben più ampia e i documenti sono stati inviati con nomi diversi a imprese di numerosi Paesi, tra cui Germania, Spagna, Bulgaria, India e Romania[37].

5.2 Sistemi di controllo industriali

Nel periodo in esame non si sono sostanzialmente verificati attacchi mirati di vasta portata contro sistemi di gestione dei processi, ma ciò non significa che i gruppi, responsabili di simili attacchi in passato, siano rimasti a guardare. Ad esempio, i servizi di sicurezza ucraini hanno accusato il servizio segreto militare russo GRU di aver sferrato un attacco a un impianto di trattamento delle acque con il malware VPNFilter[38]. Inoltre, nuovi gruppi si sono affacciati sulla scena dei gestori di sistemi di controllo industriali. Stati Uniti, Europa, Medio Oriente e Asia orientale hanno osservato diverse attività. Alcune aziende che offrono soluzioni per la sicurezza informatica[39] le hanno battezzate «RASPITE»[40] o «Leafminer»[41]. Nei prossimi capitoli approfondiamo altri tre esempi di continui tentativi preparatori di ricognizione.

5.2.1 GreyEnergy: evoluzione dell'arsenale di una delle più aggressive minacce nel settore dell'energia

Il malware BlackEnergy è salito alla ribalta delle cronache dopo Natale del 2015: gli hacker sono penetrati nelle stazioni operative dei sistemi di controllo di diversi fornitori ucraini di energia e hanno causato un blackout che si è protratto per diverse ore e ha colpito 220 000 utenti nella regione[42].

Da allora, il servizio di sicurezza slovacco ESET ha osservato un altro framework di malware che, basandosi sull'incidente suesposto, ha battezzato GreyEnergy[43]. Secondo ESET, negli ultimi tre anni la famiglia di malware è stata utilizzata per colpire diversi bersagli in Ucraina e in Polonia. Oltre alla constatazione che la sparizione del malware BlackEnergy coincide con la comparsa di GreyEnergy, ESET li ritiene collegati soprattutto per la stessa struttura modulare, l'esecuzione degli attacchi e la scelta di obiettivi analoghi. Sinora non è stato scoperto un modulo specifico per i sistemi di controllo industriali della famiglia GreyEnergy, tuttavia è stato osservato come gli hacker abbiano preso di mira le stazioni operative di sistemi di controllo secondo una strategia mirata.

---

37 https://ics-cert.kaspersky.com/news/2018/10/22/yoroi/ (stato: 31 gennaio 2019)

38 https://www.theregister.co.uk/2018/07/13/ukraine_vpnfilter_attack/ (stato: 31 gennaio 2019)

39 https://ics-cert.kaspersky.com/news/2018/08/06/raspite/ (stato: 31 gennaio 2019)

40 https://dragos.com/resource/raspite/ (stato: 31 gennaio 2019)

41 https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east (stato: 31 gennaio 2019)

42 Rapporto semestrale MELANI 2015/II, capitolo 5.3.1, 26 aprile 2016 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2015-2.html (stato: 31 gennaio 2019)

43 https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/ (stato: 31 gennaio 2019)

Oltre alla struttura sostanzialmente più moderna di GreyEnergy rispetto al suo presunto predecessore, colpisce l'impiego dei certificati digitali appartenenti ad Advantech, un produttore taiwanese di hardware industriale e dispositivi IoT. Questi certificati, molto probabilmente rubati, sono stati utilizzati per dare una parvenza di attendibilità al proprio malware, aumentando così le probabilità di successo dell'infezione. Lo stesso modus operandi è stato seguito anche con Stuxnet, il primo malware conosciuto contro i processi industriali[44].

GreyEnergy dimostra che gli hacker continuano a svolgere tentativi di ricognizione contro i gestori di infrastrutture critiche. Come dimostrato nel 2015, sono pronti anche a passare, al momento giusto, dal lavoro di ricognizione al sabotaggio.

5.2.2 Shamoon distrugge dati e configurazioni – colpita l'infrastruttura di Saipem

«L'attacco ha messo al tappeto per qualche tempo 300–400 server e circa 100 singole stazioni di lavoro», ha dichiarato all'agenzia Reuters Mauro Piasere, direttore del settore «Digitale e Innovazione» della società petrolifera italiana Saipem[45], che il 10 dicembre 2018 aveva dato notizia di un ciberattacco con un comunicato stampa[46]. Il 12 dicembre Saipem ha poi aggiornato il comunicato[47] precisando che una variante del malware Shamoon aveva colpito server in Medio Oriente, India, Scozia e, in modo limitato, l'Italia. Il ripristino dei sistemi colpiti è avvenuto, in modalità graduale, attraverso l'infrastruttura di backup.

In questo periodo la società di cibersicurezza Chronicle ha analizzato una nuova variante[48] del malware Shamoon, che era stato scaricato su Virustotal, una piattaforma pubblica di analisi di file, da un indirizzo IP italiano. Shamoon è diventato famoso nel 2012 con l'attacco sferrato contro Saudi Aramco, nel corso del quale sono stati distrutti dati di 35 000 sistemi. Quattro anni più tardi una nuova ondata del malware si è abbattuta sulla stessa regione. La sua versione aggiornata si contraddistingue per la sua capacità di sovrascrivere file e il Master Boot Record (MBR), una parte del disco fisso necessario per avviare il sistema, con dati casuali. Saudi Aramco è uno dei maggiori clienti di Saipem e ciò avvalora il sospetto di un legame con i precedenti attacchi compiuti con Shamoon. Non è stato reso noto se la variante di malware analizzata da Chronicle e Palo Alto Networks[49] sia effettivamente entrata in gioco nell'attacco che ha colpito Saipem.

5.2.3 Droni all'aeroporto

I droni hanno forme, dimensioni e funzioni molto diverse. Partono dal semplice giocattolo e, passando per i servizi di consegna, finiscono con l'impiego in attività militari. È evidente che,

---

44 https://www.welivesecurity.com/2010/07/19/win32stuxnet-signed-binaries/, 19 luglio 2010

45 https://www.reuters.com/article/us-cyber-shamoon/saipem-says-shamoon-variant-crippled-hundreds-of-computers-idUSKBN1OB2FA (stato: 31 gennaio 2019)

46 http://www.saipem.com/sites/SAIPEM_en_IT/con-side-dx/Press%20releases/2018/Cyber%20attack.page (stato: 31 gennaio 2019)

47 http://www.saipem.com/sites/SAIPEM_en_IT/con-side-dx/Press%20releases/2018/Cyber%20attack%20update.page (stato: 31 gennaio 2019)

48 https://www.bleepingcomputer.com/news/security/shamoon-disk-wiping-malware-re-emerges-with-a-third-variant/ (stato: 31 gennaio 2019)

49 https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/ (stato: 31 gennaio 2019)

nei prossimi anni, il loro numero e le possibilità che offrono cresceranno notevolmente. L'incidente, avvenuto nei pressi dell'aeroporto inglese di Gatwick, dimostra che cosa possono fare i droni. Il 19 dicembre 2018, proprio all'inizio delle vacanze di Natale, droni comandati da sconosciuti hanno paralizzato l'aeroporto per 36 ore. Complessivamente sono stati avvistati oltre 200 droni. La polizia e anche i militari intervenuti non sono riusciti a trovare gli autori in questo lasso di tempo e a bloccare i droni. Sino a oggi i colpevoli della vicenda di Gatwick sono ancora a piede libero. Nel frattempo, casi di più modesta entità si verificano periodicamente in tutto il mondo. Il 12 dicembre 2018 un Boeing della compagnia aerea messicana Aeromexico è atterrato con il muso notevolmente ammaccato, presumibilmente in seguito all'impatto con un drone. In tutti i casi suesposti non sono emersi indizi di sistemi manomessi, ma il pericolo di questi incidenti aumenta.

Valutazione

Il governo britannico ha tratto le conseguenze dai fatti avvenuti e inasprito la protezione contro i droni. In Svizzera i droni e gli aeromodelli di peso superiore ai 30 chilogrammi necessitano di un'autorizzazione dell'Ufficio federale dell'aviazione civile (UFAC) per volare. L'utilizzo di droni e aeromodelli fino a un peso di 30 chilogrammi è disciplinato nell'ordinanza del DATEC sulle categorie speciali di aeromobili. Ad esempio, l'utilizzo di droni a una distanza inferiore a 5 km dalle piste di un aeroporto o di un eliporto è proibito senza autorizzazione. Tuttavia, queste regole non proteggono da azioni condotte intenzionalmente o se un drone è hackerato da un terzo che ne assume il controllo.

5.3 Attacchi (DDoS, Defacements, Drive-By ecc.)

5.3.1 Lo skimming digitale miete vittime illustri

Nel mese di agosto del 2018 un gruppo di hacker è riuscito a rubare alla compagnia area British Airways i dati di oltre 380 000 clienti. Tra questi si trovavano non solo i nomi e gli indirizzi postali e e-mail, ma anche i dati delle carte di credito e dei conti. Quello che a prima vista sembrava un ennesimo attacco sferrato a una banca dati, si è rivelato una manipolazione del sito web e dell'app di British Airways che gli hacker hanno commesso con il cosiddetto «skimming digitale». Secondo il metodo classico dello skimming, un lettore viene posizionato dai criminali all'interno di un bancomat in modo che la banda magnetica della tessera possa essere letta e memorizzata. Anche lo skimming digitale tenta di carpire i numeri delle carte di credito e le loro caratteristiche di sicurezza, tuttavia non a un bancomat, ma nel processo di pagamento su un sito di e-commerce. Nel caso di British Airways, ad esempio, sono stati rubati solo i dati dei clienti che erano stati immessi nel modulo di pagamento all'atto della prenotazione di un biglietto tra il 21 agosto e il 5 settembre 2018. I dati riguardanti il volo e la destinazione non sono stati colpiti dalla violazione del sistema.

Un altro caso è stato scoperto il 23 giugno 2018: Ticketmaster, rivenditore di biglietti riguardanti eventi di intrattenimento, ha identificato un malware che dal mese di febbraio del 2018 ha consentito a uno sconosciuto di impossessarsi di nominativi dei clienti, indirizzi e-mail, numeri di telefono, dati dei pagamenti e di accesso.

Anche la pagina di Newegg, società britannica di vendite online, in cui gli utenti registrano i dati per i pagamenti è stata colpita allo stesso modo. Il 14 agosto 2018 gli hacker hanno inoculato nel sito web 15 righe del codice malevolo che non è stato scoperto fino al 18 settembre

2018, quindi per più di un mese. Lo script dannoso installato ha inviato i dati delle carte di credito dei clienti a un server controllato dai cibercriminali.

I siti di e-commerce sono presi di mira dai pirati informatici sin dagli albori di Internet. Il motivo è relativamente semplice: se un hacker vuole carpire dati validi riguardanti carte di credito, gli shop online sono la sede ideale. Già nel 2000 la scoperta di una vulnerabilità nell'allora diffuso Cart32, software dei server Microsoft per l'e-commerce, ha consentito ai pirati informatici di entrare come amministratori nell'applicazione, riuscendo così a estrapolare i dati delle carte di credito e a eseguire comandi sul server di hosting. Nel 2011 i criminali si sono concentrati soprattutto sulle vulnerabilità del software OSCommerce. Anche in Svizzera si sono allora verificati numerosi casi di siti web compromessi, il che ha indotto MELANI a diffondere un'allerta[50].

Dal mese di marzo del 2016 RiskIQ, un'azienda che offre soluzioni per la sicurezza informatica, osserva le diverse campagne con infrastrutture di attacco sempre nuove[51] e le ha raggruppate sotto l'ombrello di Magecart, che riunisce almeno sette gruppi accusati di introdurre skimmer digitali per clonare carte di credito nei siti di e-commerce compromessi. A tal fine vengono sfruttate soprattutto le vulnerabilità presenti nelle estensioni, ossia moduli che consentono di aggiungere funzionalità, del software Magento. Questo software degli shop online è stato pubblicato nel 2008 come piattaforma open source per l'e-commerce. Willem de Groot, esperto olandese di sicurezza, ha identificato falle Zero-Day in almeno due estensioni di Magento e ha chiesto aiuto per cercarne altre nelle restanti 18 estensioni. Ma questi pirati informatici si interessano anche a Powerfront CMS e OpenCart, due software per l'e-commerce[52].

5.3.2 Rischi legati ai VPN: l'esempio di Hola VPN

Una rete virtuale privata (VPN, «virtual private network) è un canale di comunicazione criptato che consente di stabilire una connessione tra due computer distanti tramite Internet. Per molti utenti, utilizzare una rete VPN permette di aumentare il livello di confidenzialità delle sue attività online. Tuttavia, non tutte le VPN sono uguali e spetta all'utente assicurarsi che quella che utilizza sia affidabile e rispetti determinati standard di sicurezza. Nemmeno un fornitore di VPN è immune da un attacco che potrebbe compromettere la sicurezza dei suoi utenti. È quanto sembra sia accaduto nel luglio del 2018, quando MyEtherWallet (MEW), un'interfaccia molto popolare di gestione di portafogli Ethereum (che contiene criptovalute Ether), ha informato i suoi clienti che correvano un rischio con l'uso dell'estensione Chrome di VPN Hola. In effetti, secondo MEW, il 9 luglio 2018 il funzionamento di Hola è stato compromesso per 5 ore. Durante questo lasso di tempo gli utenti dei servizi MEW hanno rischiato di farsi rubare i loro averi virtuali. In un comunicato stampa, Hola ha ammesso l'incidente e precisato che il conto della ditta su Google Chrome Store era stato compromesso per proporre una versione modificata dell'estensione per Google Chrome e raccogliere i dati degli utenti che si collegavano a loro conto MEW. Dopo questa scoperta, la ditta ha reso più sicuro il suo conto su Google Chrome Store e ha ritirato l'estensione fraudolenta.

---

50 https://www.computerworld.ch/business/politik/melani-warnt-schweizer-webshop-betreiber-1321089.html (stato: 31 gennaio 2019)

51 https://www.riskiq.com/blog/external-threat-management/inside-magecart/ (stato: 31 gennaio 2019)

52 https://www.riskiq.com/blog/labs/magecart-keylogger-injection/ (stato: 31 gennaio 2019)

Raccomandazione:

Raccomandazioni di MELANI per l'utilizzo di reti VPN:
https://www.melani.admin.ch/melani/it/home/themen/vpn.html

5.3.3 Banche attaccate tramite un accesso fisico alla rete

A dicembre, il fornitore di soluzioni di sicurezza Kasperky ha pubblicato i risultati di una serie di ciberincidenti che hanno colpito diverse banche in Europa dell'Est. Il punto di ingresso nella rete della ditta è particolarmente interessante poiché i criminali hanno collegato direttamente i propri dispositivi alla rete. A differenza di numerosi attacchi sferrati a distanza, ad esempio tramite l'invio d'e-mail infette o l'hackeraggio di un server vulnerabile, in questo caso i criminali hanno avuto bisogno di un accesso fisico ai locali della ditta. Dopo essere entrati sul sito spacciandosi ad esempio per corrieri o persone in cerca di lavoro hanno collegato i loro dispositivi alla rete. A seconda dei casi, si è trattato di piccoli computer portatili, microcomputer Raspberry Pi o Bash Bunny, uno strumento di ingresso che utilizza la porta USB. Una volta stabilito il primo contatto, gli hacker hanno lanciato una fase di riconoscimento che mirava in particolare a ottenere identificatori e individuare dei terminali dai quali erano effettuati i versamenti. Dopodiché, gli aggressori hanno cercato di garantirsi un accesso remoto duraturo su questi terminali.

Questo tipo di attacco ci ricorda quanto sia importante prevedere una strategia di sicurezza globale che non si limiti a provvedimenti tecnici, ma che integri anche provvedimenti fisici o sul piano organizzativo. Il controllo degli accessi ai locali è quindi fondamentale: i punti di ingresso alla rete (dispositivi, porte Ethernet) dovrebbero essere non soltanto documentati e sorvegliati, ma anche disattivati se non sussiste la necessità di utilizzarli.

5.3.4 Lazarus, un attore sempre molto attivo

Il gruppo Lazarus è noto per aver attaccato i sistemi di diverse banche, tra cui quelli della banca centrale del Bangladesh nel 2016. Secondo molti esperti, Lazarus è legato al regime nordcoreano. Il gruppo è anche sospettato in un caso che ha colpito la banca cilena Redbanc a fine dicembre 2018. La società Flashpoint afferma in effetti che il malware utilizzato (PowerRatankba) fa parte dell'arsenale di Lazarus. Il metodo usato per installare il codice dannoso nelle reti della ditta è particolarmente interessante. Gli aggressori si sono spacciati per un reclutatore e hanno contattato un impiegato della banca tramite le reti sociali per proporgli un colloquio di lavoro tramite Skype. Durante il colloquio alla vittima è stato chiesto di scaricare una sedicente applicazione utile ai fini del processo di assunzione. In realtà si trattava di un file dannoso. Stando alle informazioni disponibili, l'incidente è stato tuttavia rilevato per tempo e non ha avuto ripercussioni sull'infrastruttura o sulle attività della banca.

Già nel mese di ottobre lo US-CERT ha pubblicato delle informazioni sulle attività di Hidden Cobra che, dal 2016, ha preso di mira banche asiatiche e africane nel quadro di una campagna di «FastCash» allo scopo di autorizzare contemporaneamente grandi quantità di contanti dai distributori automatici. Un complice recuperava poi il denaro erogato dalla macchina. In un caso del 2017 in particolare, sono stati registrati prelievi in oltre 30 Paesi che sarebbero stati effettuati in contemporanea. Per alcuni esperti, tra cui la società di soluzioni di sicurezza Symantec, che ha pubblicato la sua analisi di questi casi, dietro Hidden Cobra si celerebbe il

gruppo Lazarus. Symantec descrive dettagliatamente il modus operandi degli aggressori. Dopo una manomissione iniziale, i server utilizzati per gestire i distributori automatici verrebbero infettati da un trojan specifico (Trojan.Fastcash), programmato per produrre richieste fraudolente di transazione.

È oramai risaputo anche che Lazarus si interessa da vicino al mercato delle criptovalute per diversificare le sue fonti di guadagno. Secondo un'analisi di Kaspersky pubblicata ad agosto, il gruppo è responsabile di un attacco contro una piattaforma di scambio di criptovalute con sede in Asia. Nella fattispecie, si tratta di un'applicazione terza di trading scaricata da un impiegato della ditta che è stata utilizzata come punto di ingresso. Il codice dannoso era generato in seguito sotto forma di aggiornamento dell'applicazione. Fatto particolarmente peculiare in questo caso è l'esistenza di versioni che sono state adeguate al sistema operativo preso di mira. Se nel passato Lazarus ha spesso preso di mira i sistemi Windows, sembra la prima volta che il gruppo mette a punto un codice dannoso specifico per i sistemi mac os.

5.3.5 Ransomware

Quando si parla di malware di crittografia (cosiddetti «ransomware») si pensa prima di tutto a dati distrutti e all'auspicabile funzionamento del backup. Ma nell'attività di prevenzione non si dovrebbe dimenticare la perdita di produttività causata da questo malware fino a quando il backup non sarà eseguito e tutti i sistemi torneranno a funzionare in modo ineccepibile. Le ripercussioni sono particolarmente gravi quando gli attacchi colpiscono interi impianti produttivi. Nel semestre in esame molti di questi casi sono finiti in prima pagina.

Nel mese di agosto del 2018 è stato colpito il produttore taiwanese di microchip TSMC (Taiwan Semiconductor Manufacturing Company). Anche in questo caso il malware di crittografia utilizzato ha costretto la società a fermare la produzione in diversi stabilimenti. TSMC è il maggiore produttore mondiale di semiconduttori e processori e, in particolare, fornisce alla Apple i processori per i suoi iPhone. La causa è stata identificata in una variante del malware WannaCry, salito alla ribalta delle cronache nel mese di maggio del 2017 con le sue pesanti conseguenze a livello mondiale. In realtà, la falla individuata nel protocollo SMB di Windows responsabile della diffusione del malware era già stata chiusa nel mese di marzo del 2017, ma proprio per i sistemi di comando è talora difficile attuare una gestione degli aggiornamenti di sicurezza, cosiddetta «patch management», in tempi brevi. I computer colpiti dei «sistemi di manipolazione dei materiali» funzionavano su sistemi Windows 7 privi di patch di sicurezza. Il malware è stato inoculato mediante un nuovo software da installare, per il quale si è tralasciato di eseguire un controllo antivirus.

Nel secondo semestre del 2018 due porti hanno dovuto lottare contro ciberattacchi: il 20 settembre 2018 il porto di Barcellona ha denunciato un attacco compiuto con ransomware all'infrastruttura di sicurezza. Il tipo di ransomware utilizzato non è stato reso noto. L'attività marittima ha potuto essere mantenuta grazie alle misure preventive adottate per questi eventi. Una settimana più tardi, il 27 settembre 2018, un ransomware ha danneggiato il porto di San Diego. Anche qui i servizi portuali non sono stati interrotti e i dipendenti hanno potuto continuare a lavorare, tuttavia l'attacco ha limitato determinate funzioni e l'accesso ai dati.

Il 21 novembre 2018 l'azienda tedesca di ingegneria meccanica KraussMaffei è stata oggetto di un attacco ai suoi sistemi informatici sotto forma di ransomware. KraussMaffei si annovera tra i leader mondiali nella fornitura di macchine per la produzione di materie plastiche e gomma. All'inizio, l'attacco ha impedito l'avvio dei macchinari necessari per il comando di alcuni processi nella produzione e nel montaggio. Secondo diversi rapporti, la produzione ha subito rallentamenti. Grazie al backup, l'azienda è riuscita a far ripartire importanti sistemi,

tuttavia dovrà lottare ancora a lungo per rimediare agli effetti dell'attacco. Nel mese di gennaio del 2019 un portavoce ha confermato che solo tre quarti dei sistemi rilevanti per l'operatività sono tornati a funzionare normalmente.[53] Sul tipo di ransomware impiegato non sono state fornite informazioni, né sono stati comunicati l'ammontare del riscatto e il suo eventuale pagamento.

Valutazione/Raccomandazione

Una porta d'ingresso particolarmente amata per introdurre malware è rappresentata dagli uffici del personale delle aziende. Le candidature contengono di norma documenti di ogni tipo che devono essere aperti. Nel secondo semestre del 2018 questo tipo di attacco è stato sferrato più spesso nella forma del ransomware. Ma anche gli eventi societari o i comunicati stampa offrono buone possibilità di propagare malware.

Nel frattempo i cibercriminali hanno scoperto che anche gli attacchi ai dispositivi mobili sono redditizi, di conseguenza l'attività dei ransomware mobile continua ad aumentare. Il ransomware più comune utilizzato per colpire apparecchi Android e altri dispositivi mobili è la variante Locker che, anziché codificare file, blocca l'intero dispositivo. Con il diffondersi dei dispositivi IoT si aprirà certamente un nuovo campo di attività per i criminali.

Una misura decisiva che consente alle imprese industriali di proteggersi dai ciberattacchi è la separazione delle reti operative dalle reti IT. In tal modo, anche se l'infrastruttura informatica viene attaccata, i sistemi continuano a funzionare senza problemi. Tuttavia, per una migliore fruibilità le reti sono spesso collegate direttamente tra loro, ad esempio per semplificare l'invio dei comandi ai macchinari.

5.4 Fughe di dati

5.4.1 La piattaforma Ariane del Ministero francese degli affari esteri era stata attaccata

Il 13 dicembre il Ministero francese degli affari esteri comunicava che la sua piattaforma Ariane era stata attaccata e che dati privati erano stati rubati. Dal 2010, il servizio Ariane consente ai cittadini francesi che prevedono un viaggio all'estero di iscriversi online per ricevere raccomandazioni di sicurezza sul Paese in cui si recheranno. Se necessario, le persone iscritte vengono contattate direttamente, così come le persone di contatto indicate. La fuga di dati riguarda precisamente i nomi, i numeri di telefono e gli indirizzi e-mail delle persone indicate come contatti dal titolare dell'account. Il ministero ha precisato che i dati sottratti non sono considerati sensibili, ma si può tuttavia presumere che siano utilizzati ad esempio per l'invio di e-mail mirate o compiere truffe. Le persone coinvolte, tra le quali figurano anche cittadini svizzeri, sono stati informate tramite e-mail. Alcuni destinatari dell'e-mail, che ignoravano che i loro dati figuravano su questa piattaforma hanno peraltro avuto il sospetto che si trattasse di un e-mail di phishing.

[53] https://www.zeit.de/2019/03/datenschutz-cyberangriffe-unternehmen-digitalisierung-risiken-datendiebstahl-hacker (stato: 31 gennaio 2019)

5.4.2 Falla della funzione «view as» di Facebook

Il 28 settembre Facebook rivelava i dettagli di ciò che potrebbe rivelarsi come l'incidente di sicurezza più importante nella storia dell'applicazione. La falla ha interessato la funzionalità «View as» che consente agli utenti di scegliere come rendere visibile il proprio profilo agli altri utenti. Come misura di sicurezza, i 50 milioni di utenti coinvolti sono stati disconnessi dai propri account. Hanno dovuto effettuare un nuovo login anche i 40 milioni di utenti che hanno utilizzato la funzionalità vulnerabile. Il servizio «view as» e' stato sospeso. Lo sfruttamento di questa falla avrebbe permesso agli aggressori di prendere possesso del pulsante che consente agli utenti di rimanere connessi ai propri profili durante varie sessioni. Gli hacker hanno così potuto avere un accesso completo agli account delle loro vittime, ma anche a qualsiasi altro servizio che utilizza Facebook per l'identificazione (autenticazione unica). Questa prassi oramai molto diffusa consiste nell'utilizzare un'identificazione a un servizio considerato sicuro per connettersi a diversi altri servizi ed evitare così di dover connettersi separatamente ogni volta. L'incidente dimostra che la prassi può anche essere un rischio per la sicurezza. Il danno è quindi difficile da quantificare con precisione poiché non sono soltanto gli account Facebook ad essere interessati.

5.4.3 Fuga di dati medici a Singapore

A luglio sono stati resi noti i dettagli di un massiccio attacco nel settore della sanità a Singapore. Sono stati sottratti i dati di 1,5 milioni di persone che tra inizio maggio e inizio luglio 2018 si sono recate in una struttura che fa parte del SingHealth, il maggiore gruppo di strutture mediche del Paese. Sono inoltre state rubate informazioni sulle ricette mediche di 150 000 pazienti. Tra le vittime figura il primo ministro Lee Hsien Loong che secondo le autorità è stato preso di mira di proposito.

5.4.4 Falla del portale online di Movistar

Anche la società spagnola di telecomunicazione Telefonica ha scoperto una falla importante nel 2018. L'incidente è stato reso pubblico dall'organizzazione di tutela dei consumatori FACUA nel mese di luglio. I dati dei clienti dell'operatore Movistar sono stati accessibili a terzi non autorizzati. Una falla nella programmazione del portale online ha in effetti permesso a chiunque disponesse di un conto Movistar di accedere a nomi, indirizzi, numeri di telefono di tutti gli altri utenti. La ha poi risolto il problema, ma non è stato possibile se malintenzionati abbiano avuto modo di raccogliere dati personali.

5.4.5 La catena di alberghi Starwood vittima di una fuga per un periodo prolungato

Il 30 novembre 2018 Marriott ha comunicato che un accesso non autorizzato ha esposto i dati di 500 milioni di clienti degli alberghi del suo gruppo Starwood. Nel gennaio 2019 la società ha affermato che la fuga di dati ha interessato non più di 383 milioni di registrazioni singole. Oltre ai dati personali come indirizzi e numeri di telefono, in alcuni casi la fuga ha riguardato dati più problematici come il numero di passaporto e dati concernenti le carte di credito. Sebbene fossero criptati, Marriott non può escludere che gli aggressori siano entrati in possesso anche delle chiavi che consentono di leggere questi dati. Gli hacker avrebbero avuto accesso ai dati dal 2014 al settembre 2018, quando è stata scoperta la fuga di dati.

Starwood, marchio acquistato da Marriott nel 2016, comprende oltre 1200 alberghi in circa 100 Paesi. La fuga comunicata nel mese di novembre è singolare per il numero di persone

interessate e la durata dell'accesso abusivo, ma anche per la natura stessa dei dati raccolti. Se le informazioni personali, i dati relativi alle carte di credito e il numero di passaporto offrono numerose possibilità per commettere frodi e furti d'identità, probabilmente chi svolge operazioni di spionaggio è particolarmente interessato a sapere in quali alberghi risiedono alcune vittime. In passato, diverse campagne sofisticate di ciberspionaggio hanno colpito alberghi intrufolandosi ad esempio nelle reti wi-fi. Già nel 2014 MELANI rendeva attenti su questa possibilità portando ad esempio la campagna Darkhotel[54], con la quale un gruppo di aggressori avrebbe preso di mira le reti wireless di grandi alberghi per spiare uomini d'affari in viaggio. Tuttavia, prima di organizzare un'operazione di questo tipo, occorre sapere quando e in quale albergo si troverà la vittima designata. La fuga presso Starwood ha potenzialmente servito questo tipo di informazioni su un piatto d'argento. Anche se si ignora chi abbia ordinato l'attacco e quale fosse l'obiettivo, non si può escludere che queste informazioni siano state utilizzate per preparare un'aggressione con mezzi informatici o fisici. È possibile che le informazioni necessarie siano state acquisite da terzi e non dagli hacker stessi.

5.5 Misure preventive

5.5.1 Lotta contro i truffatori del falso supporto informatico

Quando arriva una telefonata inaspettata e l'interlocutore all'altro capo del filo si presenta come dipendente di Microsoft, potrebbe trattarsi di un truffatore. Lo stesso vale per i messaggi che appaiono improvvisamente durante la navigazione, nei quali si sostiene che il computer è a rischio o, addirittura, infetto, e si raccomanda di telefonare a un dato numero. Con questo stratagemma i criminali cercano di ottenere l'accesso ai computer in remoto e di procurarsi, oltre ai dati che vi sono contenuti, anche un po' di denaro, poiché fatturano le loro «prestazioni di supporto» e vendono licenze fittizie. Questa tipologia di attacco continua a mietere vittime anche in Svizzera[55]. Gli autori dissimulano spesso il loro numero e riescono addirittura a far comparire numeri svizzeri sul display della vittima. I numeri svizzeri che appaiono nei popup sono stati solitamente assegnati tramite operatori telefonici VoIP esteri[56].

Dal momento che, nella maggior parte dei casi, i truffatori si spacciano per collaboratori di Microsoft e Windows rimane il sistema operativo più diffuso, anche Microsoft ha tutto l'interesse a spuntare loro le armi e collabora attivamente con le autorità di perseguimento penale[57].

---

54 MELANI rapporto semestrale 2/2014 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/halbjahresbericht-2014-2.html (stato: 31 gennaio 2019)

55 MELANI mette in guardia contro questo modus operandi sin dal 2011: https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/chiamate-di-truffatori--che-si-fanno-passare-per-il-servizio-di-.html; dal momento che la tendenza a compiere truffe di questo tipo persiste, continua a figurare tra i «pericoli attuali»: https://www.melani.admin.ch/melani/it/home/themen/fake_support.html (stato: 31 gennaio 2019)

56 Nell'ambito dell'attuale revisione parziale della legge sulle telecomunicazioni (LTC) si intende attribuire alla Segreteria di Stato dell'economia SECO le competenze per bloccare rapidamente questi numeri.

57 https://blogs.microsoft.com/on-the-issues/2018/11/29/new-breakthroughs-in-combatting-tech-support-scams/; https://www.zdnet.com/article/after-microsoft-complaints-indian-police-arrest-tech-support-scammers-at-26-call-centers/ (stato: 31 gennaio 2019)

Le vittime del falso supporto tecnico possono sporgere denuncia alla polizia locale e informare direttamente Microsoft[58].

I mandanti di questa truffa e i gestori delle infrastrutture sono distribuiti in tutto il mondo[59], ma le tracce delle chiamate conducono regolarmente a call center in India. Lo scorso autunno la polizia indiana ha eseguito perquisizioni in 26 call center di Nuova Delhi e ha fermato più di 60 persone[60]. Non è ancora dato sapere se questi arresti porteranno a una diminuzione duratura del fenomeno. È tuttavia rassicurante che l'attività di perseguimento penale a livello internazionale riscuota sempre più successi e le organizzazioni criminali che agiscono su scala globale non possono sperare di rimanere impunite.

5.5.2 Necessario un freno alla falsificazione dei numeri di chiamata

Il 1° ottobre 2018 l'autorità per le telecomunicazioni britanniche OfCom ha posto in vigore la versione riveduta delle condizioni generali per gli operatori telefonici[61], nelle quali viene sancito l'obbligo per gli operatori di mettere gratuitamente a disposizione la visualizzazione dei numeri di chiamata e di garantire che il numero visualizzato appartenga effettivamente all'autore della telefonata. Le telefonate provenienti da numeri falsificati devono essere bloccate. Questa misura intende tutelare meglio i consumatori da telefonate fraudolente o comunque moleste.

La possibilità di attuare queste disposizioni in modo opportuno è controversa. In Svizzera la legge sulle telecomunicazioni è in fase di revisione. Il messaggio del Consiglio federale[62] illustra la problematica della falsificazione dell'identificativo di chi chiama e spiega che l'introduzione di una procedura efficace per verificare i numeri su scala globale potrebbe durare molti anni nonostante gli sforzi in atto a livello internazionale. È comunque previsto di estendere anche alle chiamate pubblicitarie indesiderate l'obbligo legale dei fornitori di servizi di telecomunicazione di lottare direttamente contro lo spamming. Al riguardo la Svizzera sarebbe disposta a prescrivere e attuare misure a livello di ordinanza non appena lo stato della tecnica lo consenta.

5.5.3 Operazione concertata contro gli autori di Voice Phishing

Un gruppo attivo a livello internazionale è sospettato di essersi impossessato di dati di e-banking mediante e-mail di spam e telefonate e di averli utilizzato in modo illecito («Voice Phishing»). Tra le vittime si annoverano anche clienti di istituti finanziari in Svizzera.

Grazie alla collaborazione con l'Olanda per mezzo dell'assistenza giudiziaria, i presunti colpevoli sono stati identificati e la loro base operativa è stata localizzata nell'area metropolitana di Rotterdam. Con il sostegno delle autorità di perseguimento penale olandesi, dell'Ufficio fede-

---

58 Il modulo di segnalazione di Microsoft è pubblicato a questo indirizzo: https://www.microsoft.com/de-ch/concern/scam

59 Tra l'altro in Germania e in Inghilterra: https://winfuture.de/news,96690.html; https://www.t-online.de/digital/sicherheit/id_81548210/trickbetrueger-mit-microsoft-masche-verhaftet.html (stato: 31 gennaio 2019)

60 https://www.nytimes.com/2018/11/28/technology/scams-india-call-center-raids.html (stato: 31 gennaio 2019)

61 https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/new-rules-protect-consumers

62 https://www.admin.ch/opc/de/federal-gazette/2017/6559.pdf, pag. 5620 seg. e pag. 5635 seg. (stato: 31 gennaio 2019)

rale di polizia (fedpol) e grazie al coordinamento con Eurojust, l'autorità di cooperazione giudiziaria dell'Unione europea, il 17 luglio 2018 è stata condotta un'operazione concertata in Olanda, durante la quale sono state arrestate due persone e svolte perquisizioni. Per il presunto responsabile delle telefonate di phishing in Svizzera è stata chiesta l'estradizione. L'altra persona sarà perseguita nell'ambito di un procedimento penale olandese[63].

Valutazione

Come dimostra il successo dell'operazione concertata in Olanda, il perseguimento penale della cibercriminalità deve essere affrontato a livello internazionale.

5.5.4 Gli Internet provider tagliano i collegamenti ai dirottatori di rete

Il Border Gateway Protocol (BGP) è il protocollo di istradamento o «routing» utilizzato in Internet e collega tra loro le singole reti, cosiddette sistemi autonomi. A ognuno di questi sistemi autonomi appartengono indirizzi IP e l'insieme dei sistemi autonomi crea la rete di Internet. Con «dirottamento BGP» (in inglese «BGP Hijacking») si intende l'acquisizione illegittima di indirizzi IP da parte di gestori di un sistema autonomo mediante la manomissione di tabelle di routing per intercettare il traffico di transito.

Una società di hosting portoghese ha dato più volte nell'occhio con queste acquisizioni illegittime. È sospettata di avere noleggiato i sottratti indirizzi IP soprattutto a mittenti di spam, dal momento che i loro indirizzi sono inseriti generalmente in fretta nelle «block list», ossia gli elenchi di indirizzi IP fonte di spam, e hanno bisogno di indirizzi sempre nuovi per poter consegnare le loro e-mail. Si presume che negli ultimi anni siano stati immessi complessivamente 130 percorsi falsi, quindi quasi 225 000 indirizzi IP sono stati utilizzati abusivamente. Questa fattispecie è stata trattata in diverse mailing list, dopo di che i fornitori di connettività Internet e i punti di scambio Internet hanno convenuto di bloccare tutti i collegamenti al sistema autonomo di questa azienda[64].

Valutazione

Si può discutere se un simile procedimento sia da considerare una forma di autodisciplina o piuttosto un'azione di giustizia privata. A conti fatti, questa prima messa al bando può essere vista come un avvertimento a tutti i gestori di rete affinché le loro attività in Internet si attengano a determinate regole, anche in assenza di leggi formali ed eseguibili. In particolare, chi manomette l'infrastruttura di base deve affrontare una comunità globale che non approva queste azioni e può adottare contromisure comuni.

63 https://www.bundesanwaltschaft.ch/mpc/de/home/medien/archiv-medienmitteilungen/news-seite.msg-id-71647.html (stato: 31 gennaio 2019)

64 https://www.bleepingcomputer.com/news/security/internet-transit-providers-disconnect-infamous-bgp-hijack-factory/ (stato: 31 gennaio 2019)

6 Tendenze e prospettive

6.1 La manipolazione, un effetto della circolazione dell'informazione

Da quando l'informazione circola tra le persone e consente di modificare i propri comportamenti od opinioni, esistono anche la disinformazione e la manipolazione della stessa informazione. Già nel IV secolo a.C. Sun Tzu descriveva questi metodi ne «L'arte della guerra». Oggi, la nostra società iperconnessa offre potenzialità molto vaste in termini di trasmissione dell'informazione e delle sue conseguenze, ovvero la manipolazione dell'informazione. In un contesto in cui l'attenzione è presente sul piano sociale, mediatico e politico, il dibattito risulta a volte poco chiaro e diventa difficile districarsi tra fake news, junk news, propaganda e altri tentativi di influenzare l'opinione pubblica. In questo anno elettorale l'interesse per queste tematiche non scemerà. Esempi che arrivano dall'estero dimostrano come il dibattito che precede un'elezione si presti facilmente a manipolazioni dell'informazione, intese come diffusione massiccia e organizzata di informazioni false, distorte o non destinate a essere divulgate pubblicamente (dati personali o classificati in particolare).

6.1.1 Un contesto sociale e tecnologico favorevole

Se le campagne di manipolazione dell'informazione fanno leva su caratteristiche proprie della natura umana, come determinati mezzi cognitivi, esse trovano in determinate tendenze attuali terreno fertile.

I media classici sono sopraffatti dai media online e dalle reti sociali, che diventano la fonte di informazione principale per molte persone[65]. Ognuno di noi può diffondere informazioni senza doversi preoccupare del rispetto di qualsiasi standard di qualità giornalistico. Le stesse reti sociali hanno peraltro aperto prospettive inedite in termini di monitoraggio della popolazione. È possibile inviare un messaggio preciso a un sottogruppo della popolazione noto per essere particolarmente ricettivo a un certo tipo di informazione. Le reti sociali e Internet non rappresentano soltanto un vantaggio per prendere di mira determinate fasce di utenti, ma permettono anche di moltiplicare la diffusione di un'informazione per utilizzare bot. Sui social network una preponderanza può essere raggiunta anche da un piccolo numero di attori.

Le informazioni manipolate circolano più rapidamente rispetto a quelle vere[66]. Il fatto di essere eclatanti, superficiali e forse anche divertenti aumenta la loro probabilità di essere condivise. Oltre agli utenti medi, ci si può imbattere anche in attori che fungono consapevolmente da tramite per diffondere informazioni manipolate e a volte si premurano addirittura di dare a queste informazioni un'apparenza di veridicità pubblicandole su blog o giornali online.

6.1.2 Esempi eloquenti

Le operazioni di manipolazione messe a punto negli ultimi anni sono state effettuate in contesti specifici. Sono state particolarmente prese di mira le campagne che precedono un'elezione o

---

65 Secondo Reuters Digital News Report 2016, le reti sociali sono oramai una fonte di informazione per il 62 per cento degli adulti americani e il 48 per cento degli europei (stato: 31 gennaio 2019).

66 Cfr. in particolare uno studio del M.I.T.: http://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308 (stato: 31 gennaio 2019)

una votazione popolare in contesti molto tesi. L'esempio più eloquente e caratteristico in questa categoria è sicuramente dato dalle elezioni presidenziali americane del 2016. In un contesto già fortemente conflittuale erano stati resi pubblici i contenuti degli account di posta elettronica di personalità e organizzazioni politiche. Il 7 ottobre 2016 le autorità americane avevano quindi accusato il governo russo di avere tentato di destabilizzare le elezioni presidenziali. Nel mese di febbraio 2018, in un documento di rinvio a giudizio[67], il team del procuratore speciale Müller ha fornito dettagli su un altro aspetto dell'operazione sotto accusa: la creazione e la diffusione sistematica di false notizie da parte dell'«Internet Research Agency», con sede a San Pietroburgo. Sembra che l'obiettivo fosse quello di minare innanzitutto la fiducia nelle istituzioni democratiche, rafforzare le linee di frattura della società americana e radicalizzare gli elettori. Le informazioni completamente inventate concernenti temi controversi (armi da fuoco, razzismo ecc.) dovevano sembrare provenire dagli Stati Uniti e spesso erano supportate da simpatizzanti o gruppi locali. Le reti sociali, in particolare Facebook, hanno svolto un ruolo decisivo nella diffusione di queste informazioni. Nemmeno l'Europa è stata risparmiata da questo tipo di operazioni. Infatti, anche durante la campagna elettorale francese del 2017 sono state diffuse false informazioni, tra cui la sedicente esistenza di un conto offshore dell'attuale presidente francese Emmanuel Macron. Poco prima delle elezioni sono inoltre stati pubblicati documenti provenienti dai conti piratati di stretti collaboratori di Macron. Sebbene alcuni esperti puntino il dito contro la Russia, ufficialmente le autorità francesi non hanno accusato nessuno. Tuttavia, le operazioni di manipolazione dell'informazione possono anche prendere di mira le votazioni, ad esempio in occasione di referendum. Vi sono ad esempio sospetti d'ingerenza russa nel voto che ha decretato l'uscita del Regno Unito dall'Unione europea (Brexit) e in quello sull'indipedenza della Catalogna.

6.1.3 Prospettive in Svizzera

È difficile immaginare che in Svizzera venga compiuta un'operazione come quelle che hanno colpito le elezioni americane e francesi. Innanzitutto il ruolo strategico del nostro Paese non è paragonabile. Fatto ancora più importante, le elezioni a livello federale non si prestano a questo tipo di azioni, per ragioni legate alla cultura politica e al sistema proporzionale, in particolare. Le battaglie politiche più aspre che sfociano in una maggiore polarizzazione della società si verificano spesso in occasione di referendum o iniziative popolari che vertono sull'immigrazione o più in generale sull'indipendenza dall'Unione europea. Da questo punto di vista, il sistema svizzero di democrazia diretta potrebbe prestarsi a tentativi di destabilizzazione. Inoltre, alcune operazioni di manipolazione dell'informazione sono avvenute dopo singoli eventi, che difficilmente possono essere previsti in anticipo. Ad esempio, secondo alcuni esperti, la distruzione del volo MH17 della Malaysia Airlines avrebbe scatenato una vasta campagna di disinformazione da parte della Russia, che è stata accusata di avere distrutto il velivolo. Lo stesso vale per l'avvelenamento in Inghilterra dell'agente russo Skripal. Qualsiasi Paese può quindi essere coinvolto da operazioni di questo tipo quando è direttamente interessato suo malgrado da un fatto dal quale un altro Stato può trarre beneficio. Alla luce di quanto precede, non si può affermare che il nostro Paese sia fuori dalla portata di questo tipo di minacce. E il potenziale danno che queste campagne possono arrecare non deve essere sottovalutato. In alcuni casi il dubbio sulla legittimità del risultato di una votazione potrebbe in effetti nuocere pesantemente sul buon funzionamento del dibattito politico svizzero e sulla fiducia nelle istituzioni.

[67] https://www.justice.gov/file/1035477/download (stato: 31 gennaio 2019)

6.1.4 Possibili risposte

Prima di attuare misure che possano contrastare eventuali operazioni di manipolazione dell'informazione occorre definire le prossime tappe. Innanzitutto è necessario chiarire il dibattito e i concetti in gioco. Il termine «fake news» è ad esempio molto vago e riunisce numerose realtà. Si tratta quindi di definire il problema e, su questa base, decidere ciò che è accettabile in una democrazia e ciò che non lo è. Non si può infatti mettere nella stessa categoria le informazioni errate o la diffusione di dicerie dovute a giornalismo di qualità scadente più che all'intenzione di nuocere e una campagna di disinformazione orchestrata dall'estero con l'intento di influenzare l'opinione pubblica. In secondo luogo, occorre sviluppare la capacità di fare questa distinzione. Quali sono gli indizi che permettono di capire se una campagna è portata avanti con l'intento di nuocere? In questo contesto è necessaria un'intensa collaborazione con gli attori privati (gestori di contenuto, fornitori di servizi Internet) e i partner internazionali che si occupano anche di queste tematiche. In un contesto simile, verranno monitorati con attenzione eventi chiave, come ad esempio votazioni su temi cruciali. Anche le misure previste dovranno essere definite in stretta collaborazione con gli attori privati che hanno la possibilità di agire e di individuare i contenuti problematici. Il lavoro preliminare è fondamentale, poiché una definizione troppo ampia del problema che si cerca di affrontare rischierebbe di essere interpretata come un tentativo di censura. Al di là delle misure che potranno essere adottate sul piano tecnico, o addirittura legale (in particolare in ambito penale), occorre sensibilizzare l'opinione pubblica. Le misure di sensibilizzazione e di educazione politica a tutti i livelli sono la base per la protezione di società, gruppi e individui dagli effetti manipolatori delle operazioni di influenza. A tal fine sono indispensabili istituzioni funzionanti della società civile. Il successo di una campagna di manipolazione dell'informazione si basa in effetti sul modo in cui questa informazione viene recepita ed eventualmente diffusa dagli utenti. Migliorare le competenze mediatiche e tecnologiche può quindi permettere di limitare l'impatto di una campagna di disinformazione. Tra queste competenze rientrano ad esempio la capacità di verificare le fonti di un'informazione o l'attendibilità di un sito Internet. Occorre però anche (e soprattutto) sviluppare uno sguardo critico nei confronti dell'informazione in generale.

6.2 Sviluppi normativi

Chi disciplina Internet? Per lungo tempo numerosi Paesi hanno ignorato o irriso questo nuovo strumento e i suoi utenti. La società civile utilizzava Internet in qualunque modo proposto e possibile. Le aziende facevano altrettanto. Gli attori di Internet, in particolare le società di telecomunicazioni che approntano linee e collegamenti e anche l'industria dei nomi di dominio, prevalentemente si autoregolamentavano. Gli obiettivi erano diffusione e crescita. Il controllo degli utenti e il monitoraggio delle loro azioni non rivestivano un ruolo essenziale. Infatti Internet era un mondo libero, in cui tutti potevano esprimere la loro opinione senza restrizioni. Ma i tempi in cui Internet era utilizzato soltanto per scambiare informazioni sono ormai lontani. Nel frattempo la connessione in rete pervade tutti gli ambiti dell'esistenza umana e vivere senza Internet è quasi inimmaginabile. Molti e importanti processi economici e sociali non possono prescindere da questo strumento, che deve dunque essere affidabile e sicuro. La sicurezza è, per tradizione, un compito sovrano, pertanto numerose autorità cercano di assumere questa responsabilità anche relativamente a Internet e di recuperare le occasioni perdute di regolamentarlo. Tuttavia, l'approccio geograficamente circoscritto delle legislazioni nazionali esplica solo un effetto limitato e i diversi Paesi devono considerare la dimensione globale di Internet.

Una regolamentazione globale da parte degli Stati appare poco realistica, sebbene l'ONU abbia già convocato diversi gruppi di esperti («United Nations Group of Government Experts»,

UN GGE) per discutere i rischi e le misure volte a garantire la sicurezza internazionale e la pace nell'ambito di Internet. Il processo richiede tuttavia tempi lunghi e dall'ultimo incontro di esperti tenutosi nel 2017 non è emerso alcun risultato consensuale. Ciò riflette, tra l'altro, le crescenti tensioni politiche, che si ripercuotono in tutti gli ambiti della cooperazione internazionale. Una soluzione multilaterale, che raccolga il consenso di tutti i Paesi del mondo, potrebbe dunque farsi attendere ancora a lungo.

Ma non tutti vogliono o possono attendere. Il processo di digitalizzazione prosegue mentre sale sensibilmente la pressione da parte dei più disparati attori di Internet, non più soltanto qualche gestore dell'infrastruttura, bensì tutti gli offerenti e gli utenti. Alcuni Stati tentano di disciplinare e controllare Internet almeno sul proprio territorio, per esempio imponendo agli offerenti esteri di piattaforme prescrizioni in materia di protezione dei dati e cancellazione di determinati contenuti, censurando informazioni o isolando il proprio segmento di Internet. Al lato opposto si collocano le grandi multinazionali (Google, Facebook, Microsoft ecc.), che vogliono mantenere immutata la rete mondiale (e anche il mercato globale) e non desiderano essere alla mercé dei conflitti geopolitici. Si aggiungono i rappresentanti della società civile, che si contrappongono allo straripante potere statale e anche alla brama di profitti delle imprese.

Alcune regole occorrono dunque anche in Internet, spesso designato come «vuoto giuridico». Dal momento che gli Stati non offrono una certezza del diritto globale, sempre più attori privati si apprestano a colmare il vuoto e propongono regole di condotta o rilasciano dichiarazioni sui principi che reggono il loro operato. Spesso queste iniziative provengono dall'industria delle TIC nella sua accezione più ampia oppure da organismi multi-stakeholder.

I tre esempi seguenti mostrano gli sforzi di rendere Internet e l'utilizzo delle TIC prevedibili, attendibili e più sicuri:

6.2.1 Global Commission on the Stability of Cyberspace (GCSC)[68]

La Global Commission on the Stability of Cyberspace (GCSC) riunisce personalità di spicco di governi, imprese, mondo della tecnologia e società civile provenienti dalle più disparate regioni geografiche. La sua missione è promuovere la pace, la sicurezza e la stabilità in ambito internazionale, proponendo norme e iniziative volte a una condotta responsabile degli attori statali e non statali nel ciberspazio.

6.2.2 CiberSecurity Tech Accord[69]

Il CiberSecurity Tech Accord è stato sottoscritto sinora da un'ottantina di imprese IT[70], che riconoscono i seguenti principi per migliorare la sicurezza, la stabilità e la resilienza del ciberspazio:

- difesa e protezione: ogni utente deve essere protetto da eventuali attacchi in tutto il mondo, indipendentemente dalla sua provenienza;
- attacchi banditi: i governi non saranno aiutati a lanciare attacchi contro cittadini innocenti o imprese e sarà altresì impedito che vengano manomessi prodotti o servizi;

---

68 https://cyberstability.org/ (stato: 31 gennaio 2019)

69 https://cybertechaccord.org/ (stato: 31 gennaio 2019)

70 https://cybertechaccord.org/about/ (stato: 31 gennaio 2019)

- potenziamento delle risorse: le capacità di autoprotezione devono essere migliorate presso gli sviluppatori e gli utenti;
- azione collettiva: occorre migliorare ulteriormente la cooperazione tecnica e la comunicazione concertata di falle di sicurezza nonché lottare contro la diffusione di malware.

6.2.3 Appello di Parigi per la fiducia e la sicurezza nel ciberspazio[71]

Oltre 400 organizzazioni, imprese e Stati hanno sottoscritto l'Appello di Parigi per la fiducia e la sicurezza nel ciberspazio, che vuole promuovere l'elaborazione di basi comuni per la sicurezza in Internet. I sostenitori dell'Appello di Parigi si impegnano a collaborare con i seguenti obiettivi:

- migliorare la prevenzione e la resilienza di fronte ad attività online malevoli;
- proteggere l'accessibilità e la funzionalità di Internet;
- prevenire congiuntamente ingerenze nelle consultazioni elettorali;
- contrastare insieme l'inosservanza della proprietà intellettuale in Internet;
- impedire la diffusione di malware e di tecnologie malevoli di Internet;
- migliorare la sicurezza dei prodotti e dei servizi digitali nonché la generale «ciberigiene», ovvero abitudini di condotta che possono vanificare i più comuni tentativi di attacco;
- adottare misure contro i «cibersoldati» e le attività offensive di attori non statali;
- riunire gli sforzi per migliorare gli standard internazionali di riferimento.

[71] https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-france-et-la-cybersecurite/article/cybersecurite-appel-de-paris-du-12-novembre-2018-pour-la-confiance-et-la (stato: 31 gennaio 2019)

7 Politica, ricerca, policy

7.1 Svizzera: interventi parlamentari

Intervento	Numero	Titolo	Depositato da	Depositato il	CN/CS	Dip.	Stato delle deliberazioni e link
Mo.	18.4387	Nel 2019 Consiglio federale e DDPS attribuiscono massima priorità alla cibersicurezza	Guggger Niklaus-Samuel	14.12.2018	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184387
Mo.	18.4051	Ciberprotezione e ciberdifesa. A che punto siamo oggi?	Golay Roger	28.09.2018	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184051
Mo.	18.4000	Partecipazione della Svizzera al Centro di eccellenza di cyberdifesa cooperativa della NATO a Tallinn	Fridez Pierre-Alain	28.09.2018	CN	DDPS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184000
Mo.	18.4375	Voto elettronico. Per un impegno rapido e determinato a favore di un sistema gestito dall'autorità pubblica e open source	Sommaruga Carlo	14.12.2018	CN	CAF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184375
Po.	18.4346	Portali di comparazione più onesti. Le commissioni palesi e quelle nascoste dei servizi di comparazione devono essere indicate	Reimann Lukas	14.12.2018	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184346
Ip.	18.4230	WiFi gratuito alle FFS. Il minimo nell'era della Svizzera digitale	Tornare Manuel	13.12.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184230
Ip.	18.4178	Per uno «smart farming» realizzabile	Page Pierre-André	12.12.2018	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184178
Ip.	18.4121	Sempre più bambini vengono abbordati da estranei in Internet. Come interviene il Consiglio federale?	Frei Yvonne	29.11.2018	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184121
Po.	18.4004	Adeguare la legge concernente i viaggi "tutto compreso" all'attuale realtà di consumo	Birrer-Heimo Prisca	28.09.2018	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184004
Po.	18.3858	Limitare il consumo di pornografia in Internet da parte di bambini e giovani	Nordmann Roger	26.09.2018	CN	DFI	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183858
Mo.	18.3856	Maggiore considerazione per la salute nella telefonia mobile (1)	Estermann Yvette	26.09.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183856
Mo.	18.3855	Maggiore considerazione per la salute nella telefonia mobile (2)	Estermann Yvette	26.09.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183855
Ip.	18.3800	Come prevenire l'analfabetismo visivo?	Fehlmann Rielle Laurence	20.09.2018	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183800
Dom.	18.5450	Hat das Radio eine Zukunft?	Wasserfallen Flavia	12.09.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185450
Ip.	18.4404	Strategia Svizzera digitale. Semplificare il processo di consultazione delle imprese	Derder Fathi	14.12.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184404

Mo.	18.4037	Creare un centro di competenza per l'intelligenza artificiale nell'Amministrazione federale	Bendahan Samuel	28.09.2018	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184037
Mo.	18.3788	Licenze di circolazione e di condurre digitali	Grüter Franz	19.09.2018	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183788
Dom.	18.5478	Stratégie Suisse numérique. Le pilotage politique permettra-t-il une mise en oeuvre rapide du plan d'action?	Derder Fathi	12.09.2018	CN	DATEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185478
Dom.	18.5476	Stratégie Suisse numérique. Associer les entreprises fondées sur la science et spécialisées dans le numérique au plan d'action	Derder Fathi	12.09.2018	CN	DATEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185476
Mo.	18.3958	Rilevazione unica dei dati da parte dello Stato	Müller-Altermatt Stefan	27.09.2018	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183958
Ip.	18.3853	La discutibile esternalizzazione informatica penalizza i collaboratori più anziani che lavorano da molti anni in Confederazione	Gyse Barbara	26.09.2018	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183853
Po.	18.3783	Incremento dell'efficienza nella Confederazione grazie all'automazione intelligente dei processi amministrativi	Gruppo liberale radicale Dobler Marcel	19.09.2018	CN	DFF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183783
Ip.	18.4299	Il potenziale dei software open source nel sistema educativo svizzero	Quadranti Rosmarie	14.12.2018	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184299
Ip.	18.4197	Sicurezza informatica delle infrastrutture critiche. Quali sono i mezzi e le misure adottati dal Consiglio federale?	Wasserfallen Christian	12.12.2018	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184197
Mo.	18.4276	Semplificare lo scambio di informazioni mediante la creazione di interfacce elettroniche all'interno dell'Amministrazione federale	Vonlanthen Beat	13.12.2018	CS	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184276
Ip.	18.4235	Svizzera lontana dai primi nella classifica della sanità digitale. Quali misure prevede il Consiglio federale?	Graf-Litscher Edith	13.12.2018	CN	DFI	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184235

7.2 Lo sviluppo delle basi giuridiche per la tecnologia blockchain

Oggi tutti parlano della blockchain, ammaliati in particolare dallo sviluppo delle criptovalute e dal mondo della «Crypto Valley» svizzera. Ha tuttavia sollevato diversi interrogativi il modo in cui il sistema giuridico svizzero possa disciplinare la tecnologia soggiacente e creare la necessaria certezza del diritto per l'economia, requisito imprescindibile per la promozione e lo sviluppo.

Per trovare risposte, nel mese di gennaio del 2018 la Segreteria di Stato per le questioni finanziarie (SFI) ha costituito un gruppo di lavoro dedicato alla tecnologia blockchain e alle «Initial Coin Offering» (ICO). La tecnologia blockchain non interessa soltanto la legislazione in materia di mercati finanziari, ma anche altri ambiti giuridici, tra cui il Codice civile e il Codice delle obbligazioni, pertanto nel gruppo di lavoro intervengono pure l'Ufficio federale di giustizia (UFG) e l'Autorità federale di vigilanza sui mercati finanziari (FINMA) insieme a esponenti del

settore finanziario. I lavori sono volti ad aumentare la certezza del diritto, salvaguardare l'integrità della piazza finanziaria e garantire una regolamentazione tecnologicamente neutrale.

Nel mese di agosto del 2018 il gruppo di lavoro ha consultato anche rappresentanti del settore finanziario e fintech offrendo loro la possibilità di esprimere un parere in merito al suo operato e all'orientamento da dare alle raccomandazioni. Oltre alle questioni di carattere generale tra cui l'accesso ai conti bancari per le imprese fintech, dalla consultazione sono emersi interrogativi riguardanti anche la legislazione civile, la lotta contro il riciclaggio di denaro e il finanziamento del terrorismo nonché la legislazione sui mercati finanziari. In particolare è stata individuata una potenziale necessità d'intervento per quanto riguarda la qualifica e il trasferimento dei token sotto l'aspetto del diritto civile, il loro trattamento secondo la normativa in materia di insolvenza e la creazione di nuove possibilità nel settore delle infrastrutture dei mercati finanziari.

Alla metà di dicembre del 2018 il Consiglio federale ha adottato il rapporto sulle basi giuridiche per le tecnologie di registro distribuito e blockchain in Svizzera, elaborato dal gruppo di lavoro che si è occupato di tecnologia blockchain e di ICO, e ha deciso di rinunciare a una legge specifica concernente la tecnologia blockchain. Dal rapporto emerge che il quadro giuridico svizzero è in grado di gestire le nuove tecnologie, tuttavia sono necessari alcuni adeguamenti mirati a livello legislativo. Il Consiglio federale ha incaricato il Dipartimento federale delle finanze (DFF) e il Dipartimento federale di giustizia e polizia (DFGP) di elaborare un progetto, da porre in consultazione nel 2019, che disciplini i seguenti aspetti:

- rafforzare la certezza giuridica nel diritto civile per il trasferimento di diritti attraverso iscrizioni in registri digitali;
- precisare, nella normativa in materia d'insolvenza, la rivendicazione fallimentare di beni basati sui principi della crittografia e verificare la possibilità di rivendicare dati non patrimoniali;
- elaborare, nelle leggi sui mercati finanziari, un nuovo strumento flessibile di autorizzazione per le infrastrutture del mercato finanziario basate sulla tecnologia blockchain;
- adeguare, nella legislazione sulle banche, le disposizioni in materia d'insolvenza delle banche tenendo conto degli adeguamenti della normativa generale in materia d'insolvenza, e
- integrare in modo più esplicito, nella legislazione sul riciclaggio di denaro, la prassi vigente per l'assoggettamento alla legge sul riciclaggio di denaro delle piattaforme di negoziazione decentralizzate.

In sintesi, il Consiglio federale si prefigge di creare le migliori condizioni quadro possibili affinché la Svizzera si posizioni come polo di riferimento per le imprese tecnofinanziarie e per quelle attive nella blockchain. Inoltre, intende combattere sistematicamente gli abusi e preservare l'integrità e la buona reputazione della piazza finanziaria ed economica del nostro Paese.

Nel contempo, il Consiglio federale ha pubblicato un rapporto elaborato dal gruppo di coordinamento interdipartimentale per la lotta contro il riciclaggio di denaro e il finanziamento del terrorismo (GCRF) e incentrato sui rischi di riciclaggio di denaro e di finanziamento del terrorismo cui sono esposti i «criptoasset» e il «crowdfunding». Il rapporto constata che i beni basati sui principi della crittografia rappresentano un rischio nell'ambito del riciclaggio di denaro e del finanziamento del terrorismo. Tuttavia, a causa dell'esiguo numero di casi, in Svizzera non è possibile stabilire con esattezza il rischio concreto. Occorrerà cercare di ottenere ulteriori miglioramenti in questo ambito soprattutto attraverso misure concertate sul piano internazionale.

Il DFF è stato invece incaricato di esaminare se è il caso di adeguare la legislazione sul riciclaggio di denaro in relazione a determinate forme di «crowdfunding».

Sarà il futuro a dimostrare se queste misure saranno sufficienti per garantire in via continuativa l'attrattiva della piazza economica per la tecnologia blockchain e del radicamento della «crypto valley» della Svizzera. La neocostituita Swiss Blockchain Federation, sotto la direzione di Heinz Tännler, consigliere di Stato del Cantone di Zugo, si prefigge di consolidare e aumentare l'attrattiva e la capacità concorrenziale della piazza economica elvetica nell'ambito della tecnologia blockchain, di interconnettere importanti attori e rafforzare l'ecosistema della blockchain in Svizzera.

Tale compito appare essenziale, poiché il Liechtenstein sta diventando un polo d'attrazione con una legge concernente la tecnologia blockchain che dovrebbe entrare in vigore nell'estate del 2019. Queste condizioni quadro richiamano anche le aziende provenienti dalla «crypto valley» svizzera.

Il Principato del Liechtenstein osserva che, a causa dell'elevata densità normativa sul mercato finanziario, le imprese innovative esauriscono ripetutamente i margini di manovra concessi dalla legislazione. Dal punto di vista statale il capo del Governo del Liechtenstein, Adrian Hasler, giudica importante che a queste imprese sia fatta chiarezza in merito a opportunità e limiti. Inoltre, è chiaro che il potenziale della tecnologia blockchain non si limita al settore dei servizi finanziari: un ventaglio molto più ampio di valori patrimoniali può essere rappresentato digitalmente e messo a disposizione per ogni servizio immaginabile. Il Liechtenstein ha optato per una legge concernente la tecnologia blockchain poiché i campi di applicazione della «token economy» riguardano l'intera economia e rappresentano un ulteriore passo avanti verso la digitalizzazione. Con il «token» come nuovo elemento giuridico, il Liechtenstein crea dunque uno strumento che consente di raffigurare in modo digitale qualunque diritto del mondo analogico. Ma la nuova legge disciplinerà anche i limiti e le attività da proteggere per limitare il rischio di abusi.

Questo approccio crea sicurezza e rappresenta un'importante base per l'innovazione e gli investimenti.

Informazioni

INFO

Rapporto «Basi giuridiche per le tecnologie di registro distribuito e blockchain in Svizzera»

https://www.sif.admin.ch/dam/sif/it/dokumente/Fokus/Bericht-Blockchain.pdf.download.pdf/Rapporto%20Blockchain.pdf

Rapporto elaborato dal gruppo di coordinamento interdipartimentale per la lotta contro il riciclaggio di denaro e il finanziamento del terrorismo sui rischi di riciclaggio di denaro e di finanziamento del terrorismo cui sono esposti i «criptoasset» e il «crowdfunding» (disponibile solo in tedesco e francese):

https://www.newsd.admin.ch/newsd/message/attachments/56167.pdf

Guida pratica della FINMA per il trattamento delle richieste inerenti all'assoggettamento in riferimento alle initial coin offering (ICO):

file:///C:/Users/admin/Downloads/20180216%20mm%20ico%20weglei-tung.pdf

Rapporto del Governo del Liechtenstein sui risultati della consultazione concernente una nuova legge sui sistemi di transazioni basati su tecnologie fidate (legge sulla blockchain; legge sulle tecnologie fidate):

https://www.llv.li/files/srk/vnb-blockchain-gesetz.pdf

8 Prodotti MELANI pubblicati

8.1 Blog GovCERT.ch

8.1.1 Ingegneria inversa su Retefe

Circa un anno fa abbiamo pubblicato il post «The Retefe Saga», dedicato al noto trojan bancario. Da allora la situazione non è mutata, se non per l'aumento di malspam osservato verso fine anno. Desideriamo cogliere l'occasione per mostrarvi il processo di reverse-engineering sul malware Retefe.

➔ https://www.govcert.ch/blog/35/reversing-retefe

8.2 Bollettini d'informazione MELANI

8.2.1 Telefonate fraudolente alle imprese di nuovo in aumento

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

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

8.2.2 Attacchi di phishing contro strumenti di condivisione di dati e piattaforme di collaborazione online

02.10.2018 – Oggigiorno molte aziende consentono ai propri dipendenti di condividere documenti e persino di accedere a intere suite per l'ufficio online. Talvolta è sufficiente una semplice password per accedere, oltre che ad un account di posta elettronica, anche a molti altri documenti. Non è quindi sorprendente che i dati d'accesso siano obiettivi privilegiati per gli attacchi di phishing. Un conto compromesso viene poi molto spesso sfruttato come vettore per attaccare altri dipendenti.

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

8.2.3 Chi utilizza la stessa password più volte agevola i cibercriminali

08.11.2018 – Il 27° rapporto semestrale della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), pubblicato l'8 novembre 2018, presenta i maggiori incidenti informatici avvenuti in Svizzera e all'estero nel primo semestre del 2018. Il rapporto è incentrato sulle vulnerabilità dell'hardware, ma spiega anche l'attacco malware mirato che ha sfruttato in modo indebito il nome del Laboratorio Spiez, diverse fughe di dati e la problematica data dall'utilizzo multiplo di una password.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/melani-halbjahresbericht-1-2018.html

8.2.4 Il trojan Emotet attacca le reti aziendali

12.12.2018 – Attualmente MELANI osserva diverse ondate di e-mail con documenti Word infetti in allegato. Si tratta di un trojan ormai noto da tempo, Emotet (anche detto Heodo). Originariamente conosciuto come trojan e-banking, oggi Emotet viene utilizzato soprattutto per l'invio di spam e per scaricare altri malware. Emotet prova – con e-mail fasulle a nome di collaboratori, soci d'affari o conoscenti – tramite ingegneria sociale cioè, a convincere il destinatario ad aprire un documento Word e ad attivare le macro Office in esso contenute.

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

8.3 Liste di controllo e guide

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

9 Glossario

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

	terminata azione alla ricezione di un comando. I cosiddetti malicious bot possono pilotare a distanza i computer compromessi e indurli a eseguire qualsiasi azione.
Brute Force	Metodo di risoluzione di problemi nei settori dell'informatica, della crittologia e della teoria dei giochi, fondato sulla sperimentazione di tutti i casi possibili.
CEO-Fraud	Si parla di «CEO Fraud» (truffa del CEO) nel caso di usurpazione dell'identità di un dirigente d'azienda e quando a suo nome si richiede al servizio competente (servizio finanziario, contabilità) di effettuare un versamento su un conto generalmente all'estero.
Command & Control Server	La maggior parte dei bot possono essere sorvegliati da un botmaster e ricevere comandi attraverso un canale di comunicazione. Tale canale di comunicazione è denominato Command and Control Server.
CPU / Processore	«Central Processing Unit»/processore: unità centrale di un computer, contiene i circuiti logici necessari al funzionamento di un programma per computer.
Cryptomining	Con il mining vengono creati nuovi blocchi che si aggiungono alla blockchain. Il procedimento richiede calcoli molto complessi, pertanto viene retribuito.
Defacement	Deturpamento di pagine web.
Domain Name System	Domain Name System. Con l'ausilio del DNS, Internet e i suoi servizi sono di agevole utilizzazione, in quanto gli utenti al posto dell'indirizzo IP, possono utilizzare un vocabolo (ad es. www.melani.admin.ch).
Downloader	Programma che scarica e installa una o più istanze di malware.
Exploit-Kit	Kit che consente a criminali di generare programmi, script o righe di codice mediante i quali è possibile sfruttare le vulnerabilità dei sistemi di computer.
Global Positioning System (GPS)	Il Global Positioning System (GPS), ufficialmente NAVSTAR GPS, è un sistema globale di navigazione satellitare per la determinazione della posizione e la misura del tempo.
Infezione da «drive-by-download»	Infezione del computer mediante malware unicamente attraverso la consultazione di una pagina web. Le pagine web interessate contengono nella maggior parte dei casi offerte serie, ma sono state dapprima compresse allo

	scopo di diffondere il malware. L'infezione avviene perlopiù per il tramite dell'utilizzo di exploit che sfruttano le lacune nel sistema di sicurezza lasciate scoperte dal visitatore.
Internet delle cose	L'espressione «Internet delle cose» indica che nel mondo digitale il computer è integrato in misura crescente da «oggetti intelligenti», ossia dall'applicazione dell'intelligenza digitale agli oggetti reali.
Javascript	Un linguaggio di script orientato sugli oggetti per lo sviluppo di applicazioni. Gli JavaScripts sono elementi di programma integrati nel codice HTML, che consentono determinate funzioni nel browser di Internet. Né può essere un esempio il controllo dei dati immessi dall'utente in un modulo web. È così possibile verificare se tutti i caratteri immessi alla richiesta di un numero telefonico corrispondono effettivamente a delle cifre. Come gli ActiveX Controls, gli JavaScripts sono eseguiti sul computer del visitatore di pagine Internet. Oltre a funzioni utili, è però anche possibile programmare funzioni nocive. Diversamente dagli ActiveX Controls, gli JavaScripts sono supportati da tutti i browser.
Malware	Termine generico per software che esegue funzioni nocive su un computer. Rientrano tra l'altro in questo gruppo i virus, vermi informatici, cavalli di Troia, nonché le Logic Bombs.
Metadati	I metadati o metainformazioni sono dati che contengono informazioni su altri dati.
MITM	Attacco Man-in-the-Middle. Attacco nel corso del quale l'aggressore si insinua inosservato su un canale di comunicazione tra due partner, in modo da essere in grado di seguire o di modificare lo scambio di dati.
mobileTAN	mobileTAN (mTAN, Mobile Transaction Number) è la procedura che include il canale di trasmissione SMS. Dopo l'invio di un ordine di bonifico compilato, il cliente dell'online banking riceve dalla banca per SMS, sul proprio cellulare, un TAN unico da utilizzare esclusivamente per la transazione in questione.
P2P	Peer to Peer Un'architettura di rete nel cui ambito i sistemi partecipanti possono assumere le medesime funzioni (diversamente dalle architetture cliente-server). Il P2P è sovente utilizzato per lo scambio di dati.

Patch	Un software che sostituisce le componenti di un programma affette da errori, sopprimendo così per esempio una lacuna di sicurezza.
Phishing	Nel caso del phishing i truffatori tentano di accedere ai dati confidenziali di ignari utenti di Internet. Si può trattare per esempio di informazioni sui conti di offerenti di aste online (ad es. eBay) o di dati di accesso a servizi bancari via Internet. I truffatori sfruttano la buona fede e la disponibilità delle loro vittime inviando loro e-mail nei quali l'indirizzo del mittente è falsificato.
Protocollo SMB	Server Message Block (SMB): protocollo per la condivisione in rete di file, stampanti e server in reti di computer.
Proxy	Interfaccia di comunicazione in una rete che funge da intermediario che riceve le richieste da un lato per poi effettuare il collegamento dall'altro lato con il proprio indirizzo.
Remote Administration Tool	Il software di manutenzione a distanza (in inglese: Remote Administration Tool) costituisce un'applicazione nell'ambito del concetto di manutenzione a distanza di qualsiasi computer o sistema di computer.
Router	Apparecchiature del settore delle reti di computer, della telecomunicazione o anche di Internet che collegano o separano più reti di computer. I router sono ad esempio utilizzati nelle reti domestiche per effettuare il collegamento tra la rete interna e Internet.
Script PowerShell	PowerShell è un framework multipiattaforma di Microsoft che consente di automatizzare, configurare e gestire sistemi ed è composto da un interprete a riga di comando (shell) e da un linguaggio di scripting.
Servizi di e-currency	Valore monetario sotto forma di credito nei confronti dell'ente emittente, salvato su un supporto dati e rilasciato dietro riscossione di una somma di denaro, il cui valore non è inferiore al valore monetario emesso e che viene accettato come mezzo di pagamento da aziende diverse dall'ente emittente.
Sistemi industriali di controllo (ICS)	I sistemi di controllo e di comando constano di una o più apparecchiature che guidano, regolano e/o sorvegliano il comportamento di altre apparecchiature o sistemi. Nella produzione industriale il concetto di «sistemi industriali di controllo» (inglese: Industrial Control Systems, ICS) è corrente.

Smartphone	Lo smartphone è un telefono mobile che mette a disposizione una maggiore funzionalità di computer di quella di un telefono mobile progredito usuale.
SMS	Short Message Service Servizio per l'invio di messaggi brevi (160 caratteri al massimo) agli utenti di telefonia mobile.
Social Engineering	Gli attacchi di social engineering sfruttano la disponibilità, la buona fede e l'insicurezza delle persone per accedere per esempio a dati confidenziali o per indurre le vittime a effettuare determinate operazioni.
Spam	Il termine spam designa l'invio non sollecitato e automatizzato di pubblicità di massa, definizione nella quale rientrano anche le e-mail di spam. Si designa come spammer l'autore di queste comunicazioni mentre l'invio come tale è denominato spamming.
Spearphishing mail	Attacco mirato di phishing. Si fa ad esempio credere alla vittima di comunicare tramite e-mail con una persona di fiducia.
Take down	Take down (rimozione) è un'espressione utilizzata quando un provider ritira un sito dalla rete a causa della presenza di contenuti fraudolenti.
Top-Level-Domains	Ogni nome di dominio in Internet consta di una successione di serie di caratteri separati da un punto. La designazione Level-Domain si riferisce all'ultimo nome di questa successione e costituisce il livello più elevato della risoluzione del nome. Se ad esempio il nome completo di dominio di un computer, rispettivamente di un sito web, è de.example.com, l'elemento a destra (com) rappresenta il Top-Level-Domain di questo nome.
Transmission Control Protocol / Internet Protocol (TCP/IP)	Famiglia di protocolli di rete anche designata come famiglia di protocolli Internet a causa della sua grande importanza per Internet.
UDP	«User Datagram Protocol»: protocollo di rete molto semplice, senza connessione, che trasporta datagrammi della famiglia di protocolli Internet.
USB	Universal Serial Bus, Bus seriale che (per il tramite di corrispondenti interfacce) consente il raccordo di periferiche come tastiera, mouse, supporti esterni di dati, stampante ecc. Al momento del raccordo o della disgiunzione di un dispositivo USB il computer non deve essere riavviato. I nuovi dispositivi sono per lo più riconosciuti e

	configurati automaticamente (a dipendenza però del sistema operativo).
Verme informatico	Diversamente dai virus, i vermi informatici non necessitano di un programma ospite per diffondersi. Essi sfruttano piuttosto le lacune di sicurezza o gli errori di configurazione del sistema operativo o delle applicazioni per diffondersi autonomamente da un computer all'altro.
WLAN	L'abbreviazione WLAN (o Wireless Local Area Network) significa rete locale senza fili.
Zero-Day	Exploit che appare il giorno stesso in cui la lacuna di sicurezza è resa nota al pubblico.
ZIP-Datei	Zip è un algoritmo e un formato di file per la compressione dei file, destinato a ridurre lo spazio di memorizzazione dei file per l'archiviazione e la trasmissione.