Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

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

SICUREZZA DELLE INFORMA-ZIONI

LA SITUAZIONE IN SVIZZERA E A LIVELLO INTERNAZIONALE

Rapporto semestrale 2016/I (gennaio – giugno)

28 OTTOBRE 2016

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

1 Indice / Contenuto

2 Editoriale

Martin Sibler, in Swiss Re dal 2001, ha lavorato in diversi settori della sicurezza dell'informazione

Care lettrici, cari lettori,

nel settore assicurativo l'informazione rappresenta un elemento di cruciale importanza nella catena del valore. Per valutare i rischi da assicurare, infatti, oltre a formule matematiche occorrono informazioni storiche sull'evento che consentano di calcolare la probabilità che esso si verifichi (si pensi ad es. a un uragano in Florida). Per queste analisi si utilizzano spesso anche vari dati di clienti (come ad es. la posizione degli stabili da assicurare) di cui deve essere garantita l'integrità, la riservatezza e la disponibilità. La disponibilità delle informazioni giuste al momento giusto permette di comprendere meglio il rischio e, in un certo qual modo, di prevederlo.

Nella valutazione dei cyber-rischi si parte da una situazione analoga, tuttavia esistono diversi fattori dinamici che ne rendono più difficoltosa la stima. Da un lato, le informazioni sugli eventi precedenti sono poco esaustive; dall'altro, spesso, queste informazioni non sono più pertinenti poiché nel frattempo la tecnologia e la natura degli attacchi sono cambiati. Per gli uragani, le condizioni generali sono sempre pressappoco le stesse: cambiano la forza del vento e il tragitto della devastazione, però esistono diverse registrazioni che possono aiutare nell'analisi. In un evento del cyberspazio a cambiare non sono solo la forza del vento e il tragitto, ma anche il fenomeno stesso: al posto di un uragano può verificarsi improvvisamente un terremoto. Il paragone zoppica un po', tuttavia evidenzia con chiarezza come i cyber-rischi costringano a rapportarsi con l'imprevisto, poiché le informazioni sugli attacchi sferrati dagli hacker negli ultimi 20 anni possono contribuire solo in misura limitata a valutare la situazione di minaccia.

Per questo motivo la cyber intelligence, ossia lo scambio tempestivo di informazioni sugli attacchi attuali, è particolarmente utile per comprendere se bisogna difendersi da un uragano o da un terremoto. In questo ambito, MELANI fornisce un servizio fondamentale all'economia svizzera aiutandola a migliorare il livello di protezione contro tali rischi.

Auguro a tutti una piacevole lettura,

Martin Sibler

3 Tema principale: Cyber-estorsione – trend criminale della rete

Cosa hanno in comune Cryptolocker, Armada Collective, Rex Mundi: campagne che negli anni hanno guadagnato grande popolarità? Si tratta in tutti i casi di cyber-estorsione. In effetti, da diversi anni, i criminali optano sempre più spesso per questo modus operandi molto redditizio e invece di rubare direttamente, cercano uno strumento di pressione per costringere la vittima stessa a effettuare un versamento. Espressioni concrete recenti di questo modus operandi sono trattate nei capitoli 4.6.3 (*ransomware*) e 4.4.1 (*DDoS* ed estorsione), ma è utile chiedersi innanzitutto quali sono le ragioni di questo successo e le dinamiche in atto.

3.1 Le ricette di un successo

Secondo i criminali, questo metodo offre numerosi vantaggi. In primo luogo, nessuna necessità di puntare soltanto ai sistemi di transito del denaro. La cerchia di potenziali vittime è quasi illimitato: basta impossessarsi di dati o sistemi sufficientemente importanti per un utente o un'azienda da costringerli a pagare per recuperarli. Questo funzionamento semplifica notevolmente anche il passaggio tra l'atto criminale e i contanti utilizzabili dall'autore («cash out»). Non c'è bisogno di riciclare il denaro tramite terzi: basta farsi pagare direttamente nella valuta di propria scelta, la più difficile da rintracciare. D'altronde, non è casuale che lo sviluppo di questi metodi sia strettamente legato all'avvento di nuovi mezzi di pagamento che permettono di occultare l'identità reale del beneficiario come i *bitcoin*. Grazie a servizi di mixage, i criminali ormai sono in grado di rendere quasi impossibile l'identificazione dei destinatari dei pagamenti in bitcoin.

I diversi tipi di attacchi che ricorrono all'estorsione illustrano molto bene il funzionamento dei gruppi criminali che operano attualmente su Internet. Spesso prevale l'approccio imprenditoriale, basato su opportunismo, ricerca dell'efficacia e adattabilità. Fino a quando un modello d'attacco comporta ritorni finanziari positivi, sarà conservato e spesso migliorato. Un esempio tipico di questa logica è fornito dai ransomware. Anche se il funzionamento di base di questo tipo di malware è noto da parecchi anni, questa minaccia si riproduce in numerose varianti, si reinventa costantemente integrando nuove funzioni per una maggior efficacia. Come in un circolo vizioso: le somme di denaro pagate dalle vittime alimentano il potere monetario di queste imprese criminali, permettendo loro di rafforzare le proprie infrastrutture e di finanziare i loro dipartimenti di ricerca e sviluppo. Di conseguenza, i malware possono essere più efficaci grazie a molte innovazioni, consentendo così ai criminali di continuare a estorcere un numero sufficiente di vittime malgrado le misure di protezione adottate.

3.2 Dinamismo dell'ecosistema criminale

Il dinamismo e la ricerca di efficacia della criminalità informatica si esprimono attraverso necessità comuni a numerose imprese motivate dal denaro e che permettono a quest'ultime di prosperare. I criminali devono innanzitutto precorrere i tempi a livello tecnologico. In questo settore, l'inviolabilità dei metodi di crittografia è fondamentale, trattandosi dell'elemento centrale di tutta l'impresa criminale. Gli operatori devono essere estremamente reattivi, migliorando i metodi di crittografia quando viene individuata una soluzione di decrittazione per una versione di ransomware. Il secondo aspetto cruciale per i criminali è dato dalla necessità di accrescere costantemente la cerchia potenziale dei loro clienti (ossia le vittime). Ciò avviene in primo luogo migliorando i metodi utilizzati per infettare le proprievittime: trucchi che per-

mettono alle loro e-mail di aggirare i filtri, ad esempio e-mail inviate direttamente dal conto manomesso di un contatto, oppure a nome di un'autorità ufficiale. Sono stati osservati nuovi metodi di manomissione per cui, in certi casi, il ransomware viene installato direttamente tramite un accesso RDP («*Remote Desktop Protocol*», che permette di collegarsi in remoto a un server Windows) compromesso da un attacco di *forza bruta (brute force)*. Sempre in tale ottica, i criminali cercano di ampliare il loro ambito di attacco, ad esempio crittografando, non solo i dati di utenti o di aziende, ma anche i contenuti di siti web. Attaccare obiettivi particolarmente redditizi richiede talvolta sforzi eccezionali con conseguenze spesso drammatiche, come nel caso degli attacchi a ospedali. Con l'Internet delle cose e il collegamento in rete di numerosi dispositivi mai connessi in precedenza, l'ambito in cui possono essere attivati i ransomware sembra illimitato. Una volta sferrato un attacco a una sistema, è importante massimizzare il profitto ottenuto. Dotati di uno spiccato senso degli affari, i criminali adottano un approccio «orientato al cliente», creando canali di comunicazione diretta (*live chats*) con le proprie vittime per spiegare loro come pagare il riscatto. Inoltre cercano modi per aumentare la pressione sulle singole vittime, non solo rendendo i dati illeggibili, ma anche minacciando di svelare i dati più sensibili.

3.3 Un successo che incentiva l'uso

Questi attacchi sono talmente redditizi da incentivarne, purtroppo, l'uso. Esistono innumerevoli varianti di ransomware. Questa dinamica si verifica anche in un altro tipo di cyberestorsione, basata su attacchi DDoS, in un contesto dai contorni poco chiari, caratterizzato principalmente dalla comparsa di numerosi «*copycats*» (imitatori) che emulano i depositari del modus operandi originario e sfruttano l'estrema facilità attuale di acquistare un «servizio» d'attacco DDoS («*booter», «stresser*»). Più recentemente hanno iniziato ad agire soprattutto attori meramente opportunisti che si accontentano di «cavalcare l'onda» inviando e-mail ricattatorie, senza preoccuparsi di sferrare attacchi, non avendo peraltro nemmeno la capacità di farlo. Usurpando il nome di gruppi noti e ampiamente mediatizzati (come Armada Collective), sperano che il timore di un attacco sia sufficiente ad estorcere un pagamento.

Siamo pertanto di fronte a fenomeni estremamente remunerativi che attraggono diversi attori criminali, alcuni dei quali dotati di grande inventiva. Si teme che siano attacchi di lunga durata che si rinnovano costantemente. Tuttavia, in fin dei conti questo mercato si basa su una sola condizione: la necessità di avere una massa critica di vittime disposte a pagare, affinché questi gruppi trovino il finanziamento necessario per sviluppare le proprie attività. Senza questa fonte di entrata il sistema crolla. Non finiremo mai di ricordare quanto sia importante che le vittime non cedano in nessun caso al ricatto. Ripetere il messaggio non è però sufficiente; contestualmente occorre far presente gli strumenti per premunirsi contro questi attacchi. Ogni azienda deve riflettere individualmente e porsi le seguenti domande: quali sistemi o informazioni sono sensibili al punto di espormi al ricatto nel caso in cui vengano colpite? Come è possibile colpire i truffatori? Come sono protetti questi sistemi o informazioni? Quali procedure vengono adottate per far fronte a un attacco estorsivo? Gli utenti e le aziende con una preparazione insufficiente sfortunatamente decideranno di pagare.

Raccomandazione:

MELANI propone diversi prodotti per proteggersi da queste minacce, in particolare:

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

Misure contro i ransomware
https://www.melani.admin.ch/melani/it/home/themen/Ransomware.html

4 La situazione a livello nazionale

4.1 Spionaggio

4.1.1 Turla in un'azienda produttrice di armamenti

Il 4 maggio 2016 il Dipartimento della difesa, della protezione della popolazione e dello sport (DDPS) ha pubblicato un comunicato stampa[1] dal quale si apprende, che nel mese di gennaio 2016, il Servizio delle attività informative della Confederazione (SIC) comunicava al Ministero pubblico della Confederazione che i computer della ditta di armamenti RUAG erano stati infettati con un software di spionaggio. Il 25 gennaio 2016 il Ministero pubblico della Confederazione ha avviato un'inchiesta penale contro ignoti. Questo comunicato stampa ha destato un grandissimo interesse a livello mediatico, tant'è che l'elaborazione delle conseguenze che verranno tratte a livello politico non si è ancora conclusa. Il 23 maggio 2016 la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) ha pubblicato, su incarico del Consiglio federale, un rapporto con i risultati tecnici relativi al caso RUAG. Questo provvedimento mira a consentire ad altre aziende di verificare le proprie reti e adottare misure di protezione adeguate[2,3].

Il malware utilizzato dagli hacker é un tipo di trojan, in circolazione da parecchi anni, denominato «Turla». La variante rilevata nella rete della RUAG non presentava funzionalità *root-kit*, ma si avvaleva di tecniche di mimetizzazione per non essere individuata. Gli hacker sono stati molto pazienti durante l'infiltrazione e anche durante i movimenti laterali all'interno della rete. Hanno attaccato solo i sistemi designati.

---

1 https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-61618.html (stato: 31 agosto 2016)

2 https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-61788.html (stato: 31 agosto 2016)

3 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/fachberichte/technical-report_apt_case_ruag.html (stato: 31 agosto 2016).

Uno degli obiettivi principali dell'attacco era il servizio di directory, l'*active directory*. Attraverso questa rubrica centrale, impostando opportunamente diritti e appartenenze ai gruppi, si poteva accedere ad altre applicazioni e dispositivi contenenti dati ritenuti di interesse. Per occultare la comunicazione in modo efficace, il malware utilizzava il protocollo «http» per il trasferimento dei dati a svariati *server di comando e di controllo*. Questi server di controllo avevano a loro volta il compito di inviare comandi (i cosiddetti *task*) ai dispositivi infettati (ad es. scaricare nuovi file binari e di configurazione o *batch jobs*). La comunicazione era impostata secondo un sistema gerarchico: in questa architettura non tutti i dispositivi infettati comunicavano con i server di controllo, ma vigeva una ripartizione delle attività. Alcuni sistemi (i cosiddetti droni di comunicazione) erano preposti alla comunicazione con il mondo esterno. Altri (i cosiddetti droni di lavoro) venivano utilizzati esclusivamente per sottrarre e inviare i dati ai droni di comunicazione.

Stimare il danno effettivo è difficile e non è lo scopo né del rapporto RUAG pubblicato da MELANI né del presente documento. L'analisi dei *proxy logs* ha tuttavia evidenziato come i dati non venissero rilevati costantemente: si sono osservate fasi con scarsa attività sia in termini di richieste sia di quantità di dati trasferiti ma anche periodi con numerose richieste e grandi quantità di dati trafugati.

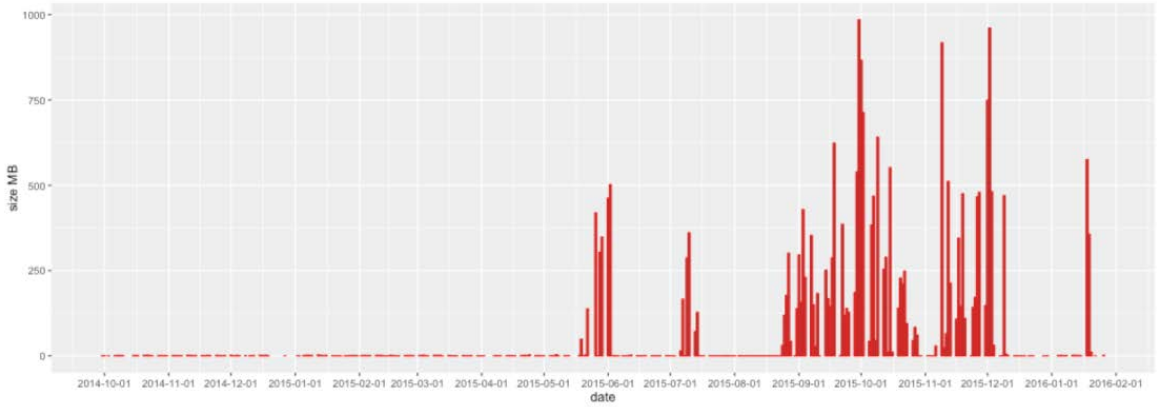


Figura 1: Quantità di dati trafugati quotidianamente

È difficile mettere a punto un sistema che sia in grado di garantire una protezione completa da attacchi così sofisticati. Tuttavia, molte contromisure non sono eccessivamente costose e possono essere implementate con un ragionevole dispendio di risorse. È possibile rilevare un incidente soprattutto quando un hacker commette un errore. I collaboratori devono però essere sensibilizzati a riconoscere malfunzionamenti e comportamenti sospetti nei sistemi, a interpretarli correttamente e a reagire di conseguenza. Un elenco di queste misure è riportato nel MELANI/GovCERT Ruag Report[4] a partire dalla pagina 27.

La sensibilizzazione costituisce un aspetto fondamentale anche in relazione allo scambio di esperienze e informazioni con altre imprese, il settore economico di appartenenza o l'Amministrazione federale. La cerchia chiusa di clienti di MELANI che conta ormai più di 190 aziende che operano nell'ambito delle infrastrutture critiche fornisce alle società un ambiente prezioso per scambiare informazioni di questo tipo, e se necessario, anche in forma anonima. La rete internazionale di MELANI apporta inoltre un contributo essenziale all'individuazione degli attacchi, visto e considerato che gli incidenti informatici non conosco-

[4] https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/fachberichte/technical-report_apt_case_ruag.html (stato: 31 agosto 2016).

no frontiere. Quotidianamente pervengono diverse segnalazioni dalla Svizzera e dall'estero che possono portare a progressi fondamentali. Nell'ambito dei propri compiti e della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) MELANI promuove lo scambio di informazioni tra i gestori di infrastrutture critiche affinché, anche in futuro, sia possibile individuare e, idealmente, sventare un numero sempre crescente di attacchi mirati.

La figura seguente illustra la cronologia del caso di spionaggio informatico:

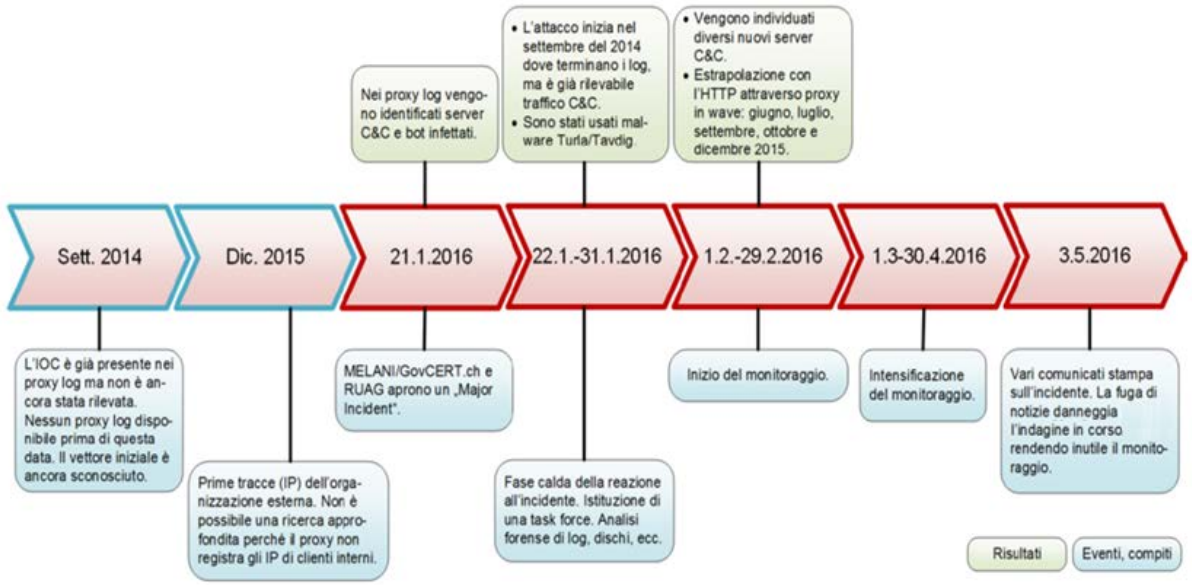


Figura 2: Spiegazione dell'attacco per singole tappe

Conclusione / raccomandazione:

Lo spionaggio informatico è una realtà, come già dimostrato dai numerosi casi descritti nei rapporti MELANI dei semestri precedenti. Questo tema viene affrontato anche nel rapporto annuale del Servizio delle attività informative della Confederazione (SIC). La prevenzione è una componente fondamentale della lotta contro lo spionaggio. Come sottolineato da diversi casi segnalati a MELANI, il primo e principale passo in tal senso è costituito dalla presa di coscienza da parte di un'azienda di trovarsi di fronte a un rischio reale e non ipotetico. Per poter contrastare in modo efficace lo spionaggio occorre inoltre assicurare il flusso di informazioni. Se vengono segnalati casi di spionaggio, le autorità competenti possono adottare le misure necessarie ed elaborare le conoscenze acquisite sottoponendole all'attenzione dei responsabili delle decisioni in ambito politico ed economico. Queste informazioni consentono infine ad altre organizzazioni di individuare eventuali attacchi ai loro sistemi. Il trattamento confidenziale delle informazioni riveste naturalmente la massima priorità per le autorità.

MELANI opera da 12 anni sul fronte della lotta contro i pericoli IT in collaborazione con diversi enti privati. Sul sito Web di MELANI è disponibile un modulo per segnalare gli incidenti legati alla garanzia di sicurezza delle informazioni:

Modulo di segnalazione MELANI:

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

Con il programma Prophylax, il SIC porta avanti un'iniziativa di prevenzione e sensibilizzazione nel campo della non proliferazione e dello spionaggio economico volta a sensibilizzare le aziende e le istituzioni educative.

Programma Prophylax:

http://www.vbs.admin.ch/it/tematiche/acquisizione-informazioni/spionaggio-economico.detail.publication.html/vbs-internet/it/publications/servizioattivitainformative/SIC-Prophylax.pdf.html

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

4.2 Furti di dati

4.2.1 Password calcolabili per i router

I *router* della ditta UPC vengono forniti dotati di una password generata automaticamente: il nome della *WLAN* (il cosiddetto *SSID*) contiene una sequenza numerica casuale a sette cifre. La passowrd viene generata su base individuale per tutti i router automaticamente dal produttore e presenta caratteristiche di casualità. Grazie a una pubblicazione comparsa su Internet a cavallo tra il 2015 e il 2016, diventa possibile che delle persone non autorizzate indovinino la Password standard della rete WLAN. Gli utenti che hanno personalizzato la propria password del Router, evidentemente non sono stati colpiti. Per determinati dispositivi

UPC, questo strumento consente di calcolare, partendo dal nome della *WLAN*, una serie di 8 fino a 12 password per la *chiave WPA2*. A pochi giorni di distanza, oltre a questo tool destinato sostanzialmente agli esperti, è stato diffuso in rete un semplice tool online alla portata di tutti. Con questa azione, lo scopritore della falla di sicurezza vuole richiamare l'attenzione sul fatto che determinati produttori trascurano l'aspetto della sicurezza nella generazione delle password. A dire il vero, la falla di sicurezza sfruttata non è una novità, ma si basava su un lavoro di ricerca scientifica olandese già pubblicato nella primavera del 2015 e presentato a una conferenza sulla sicurezza a Las Vegas nell'estate dello stesso anno.

All'inizio del mese di luglio del 2016, la storia si è ripetuta. Questa volta, l'incidente ha coinvolto il router «Ubee EVW3226», utilizzato anche in Svizzera. In questo caso, per il calcolo non è stato necessario conoscere l'SSID, ma il cosiddetto indirizzo MAC del dispositivo che può essere facilmente rilevato con diversi tool nel raggio di azione di una rete WLAN. L'informazione carpita consente di calcolare le password standard correlate e l'SSID. Anche in questo caso sono stati colpiti unicamente quegli utenti che non hanno prontamente cambiato e modificato la propria password, come consigliato.

Conclusione / raccomandazione:

L'utilizzo di password standard è da evitare, soprattutto in ambito IT se si accede ai dispositivi via Internet o tramite un segnale radio. Alcuni produttori hanno reagito a questa minaccia impostando una password individuale al posto della consueta combinazione «123456». È ancora peggio se questa password individuale preimpostata può essere calcolata da terzi, causando così una falla di sicurezza. Oggi come ieri vale dunque la regola di cambiare, rispettivamente personalizzare in ogni caso la password quando il dispositivo viene attivato e prima di collegarlo a Internet. Inoltre, la maggior parte dei dispositivi è dotata di una funzione di reset nell'eventualità in cui la password venga dimenticata. Per effettuare il reset, tuttavia, è richiesta la presenza fisica in loco e di solito occorre premere un apposito pulsante situato sul dispositivo. Per la propria sicurezza è consigliabile modificare la password standard – proprio come per altri strumenti o dati login. Ciò non è solo più sicuro ma anche più semplice per l'utilizzo quotidiano.

4.2.2 Password di 6000 account di posta elettronica svizzeri in circolazione

Il 16 marzo 2016 MELANI si è vista recapitare 6000 combinazioni di e-mail / account che gli hacker avevano rubato in occasione di un precedente attacco di pirateria informatica. Questi account avrebbero potuto essere utilizzati impropriamente a fini illegali (ad es. per truffe, estorsioni, phishing ecc.), se i titolari non avessero provveduto tempestivamente a modificare la password. MELANI ha pertanto deciso di pubblicare un tool online per consentire agli utenti di controllare se il proprio indirizzo di posta elettronica fosse stato interessato dall'attacco. Per effettuare la verifica bastava inserire l'indirizzo di posta elettronica che è stato trasmesso in forma crittografata e non è stato salvato.

Le reazioni all'iniziativa sono state nella maggior parte dei casi positive. Tuttavia, ci sono state anche critiche e più volte è stata sollevata la questione se la pagina fosse realmente legittima e creata da MELANI. Nell'ottica della sensibilizzazione e della prevenzione si tratta di una reazione apprezzabile. Di fronte a simili iniziative un sano scetticismo non deve assolutamente considerarsi fuori luogo ed è senz'altro un bene accertarsi ripetutamente e verificare se una pagina sia legittima. Nel caso in questione, MELANI ha ritenuto che la celere

pubblicazione di questo tool online fosse il metodo più pratico ed efficiente per offrire un'opportunità di controllo alle potenziali vittime degli attacchi.

4.2.3 Banca dati dell'Unione democratica di centro nel mirino degli hacker

Alla metà di marzo 2016, nell'ambito di un attacco sferrato a una banca dati dell'Unione democratica di centro (UDC) sono stati copiati circa 50000 indirizzi di posta elettronica. L'azione è stata rivendicata da un gruppo denominato «NSHC». A questo proposito, l'NSHC aveva rilasciato delle dichiarazioni alla rivista «inside-channels.ch» in cui affermava che l'azione voleva dimostrare come la Svizzera non fosse sufficientemente protetta contro i cyber-attacchi[5]. Il gruppo appartiene per sua stessa dichiarazione alla categoria dei «*grey hats*», ossia gli hacker che, pur non attenendosi alla legge, non intendono arrecare danni diretti. Inoltre, l'NSHC ha ammesso la propria responsabilità per gli attacchi *DDoS* sferrati la stessa settimana contro Interdiscount, Microspot e FFS. Anche in questo caso, il gruppo ha addotto come motivazione la volontà di smuovere i responsabili della sicurezza IT. Non si sa se NSHC disponga effettivamente di capacità DDoS o abbia voluto semplicemente saltare sul treno in corsa dei crescenti attacchi di questo tipo sferrati nel mese di marzo. Fino a quel momento, il gruppo non era mai uscito allo scoperto e successivamente non si sono üiù avute sue notizie.

4.3 Sistemi industriali di controllo

Oggi se una pagina Internet o un servizio online non è disponibile, si pensa immancabilmente a un possibile attacco di pirateria informatica. I problemi tecnici, però, continuano a essere il motivo principale dei guasti ai sistemi industriali di controllo. Lo dimostra con eloquenza l'esempio seguente, anche se riferito a un fatto ormai piuttosto datato: il 22 giugno 2005 la rete elettrica delle FFS si è bloccata poiché, a causa di lavori in corso, sono stati interrotti due dei tre elettrodotti transalpini sopravvalutando la capacità di trasmissione della terza linea. Ciò ha comportato la disattivazione della terza linea per motivi di sicurezza e la separazione delle linee elettriche in due tronconi (versante nord e versante sud delle Alpi). Gli eventi che si sono verificati nel primo semestre del 2016 non erano di questa portata, tuttavia le ripercussioni sono state gravi e hanno evidenziato la dipendenza dai mezzi di comunicazione moderni.

4.3.1 Problema ai terminali di pagamento

Il 20 giugno 2016 si sono verificate delle limitazioni ai pagamenti senza contanti. Il problema ha interessato gli operatori di tutte le regioni della Svizzera e dell'Austria che utilizzavano un *terminale di pagamento* gestito dal fornitore di servizi finanziari SIX. Non essendosi manifestato a livello capillare e tantomeno in forma permanente, il guasto è stato piuttosto complicato da individuare. La causa era un'anomalia sulla rete.

4.3.2 Internet bloccato per i clienti commerciali

Un mese prima a finire nei guai è stata la Swisscom. Il problema ha interessato la rete Internet per i clienti commerciali. A causa di un guasto importante, a mezzogiorno del 24 maggio 2016, Internet si è bloccato presso vari clienti. Il blackout ha coinvolto

[5] http://www.inside-it.ch/articles/43272 (in tedesco; stato: 31 agosto 2016)

temporaneamente anche i bancomat. Il guasto è stato attribuito a un problema alla «Ethernet access platform» della Swisscom nella zona di Losanna.

4.3.3 Attentato incendiario alla conduttura per cavi delle FFS

Il blackout verificatosi lungo l'importante collegamento ferroviario con l'aeroporto di Zurigo è stato invece causato da un attacco fisico nella zona di Zurigo Oerlikon. Nelle prime ore del mattino del 7 giugno, ignoti hanno appiccato il fuoco a due punti in una conduttura per cavi che scorreva parallela ai binari del treno. Gli incendiari sono penetrati fisicamente nell'area della ferrovia danneggiando i cavi che corrono nel terreno. Gli specialisti hanno potuto porre rimedio al danno unicamente con un lavoro artigianale di fino sostituendo ogni cavo. Il traffico ferroviario tra Oerlikon e l'aeroporto di Zurigo è stato fortemente disturbato durante tutta la giornata. La linea ferroviariaper l'aeroporto di Zurigo è rimasta bloccata fino a sera.

Conclusione:

I rischi non derivano soltanto dagli attacchi elettronici ma anche dagli attacchi agli impianti elettronici veri e propri. I cavi elettrici e per le telecomunicazioni, che possono essere protetti solo parzialmente per lunghi tratti del loro tragitto, sono particolarmente vulnerabili. Di solito, un'azione fisica ha solo ripercussioni locali. Tuttavia, la protezione di punti e sistemi nevralgici non dovrebbe essere limitata all'ambito elettronico, ma dovrebbe essere estesa anche agli impianti veri e propri.

4.4 Attacchi

In Svizzera i privati e le aziende continuano a essere oggetto di diversi tipi di attacchi che colpiscono principalmente i loro siti Web. La vulnerabilità nei confronti di *attacchi DDoS* e *defacement* costituisce un problema particolarmente rilevante per le aziende per cui è importante preservare la credibilità della propria immagine online.

4.4.1 DDoS ed estorsione

Il modus operandi che integra ricatto e minaccia d'attacco DDoS rientra nel vasto ambito dell'estorsione, che è il tema principale del presente rapporto. I gruppi «DD4BC» e «Armada Collective» sono già stati trattati in alcuni capitoli dei precedenti rapporti semestrali (2015/1 e 2015/2). Questi criminali utilizzavano un modus operandi molto noto e documentato: a un primo attacco DDoS, a titolo dimostrativo, seguiva un ricatto. Se la somma in bitcoin non veniva versata entro il termine prestabilito, minacciavano di procedere a un secondo attacco molto più potente del primo.

L'anno 2016 è iniziato con un'informazione importante a livello di perseguimento penale: a gennaio l'Europol ha annunciato di aver arrestato due membri di DD4BC[6]. Da allora non è stato registrato alcun attacco da parte di Armada Collective o DD4BC, neppure utilizzando il modus operandi «originario» descritto sopra. Ciò avvalorerebbe la tesi secondo la quale Ar-

[6] https://www.europol.europa.eu/content/international-action-against-dd4bc-cybercriminal-group (in inglese; stato: 31 agosto 2016)

mada Collective e DD4BC sono in realtà un'unica entità della quale alcuni membri importanti sarebbero già stati arrestati.

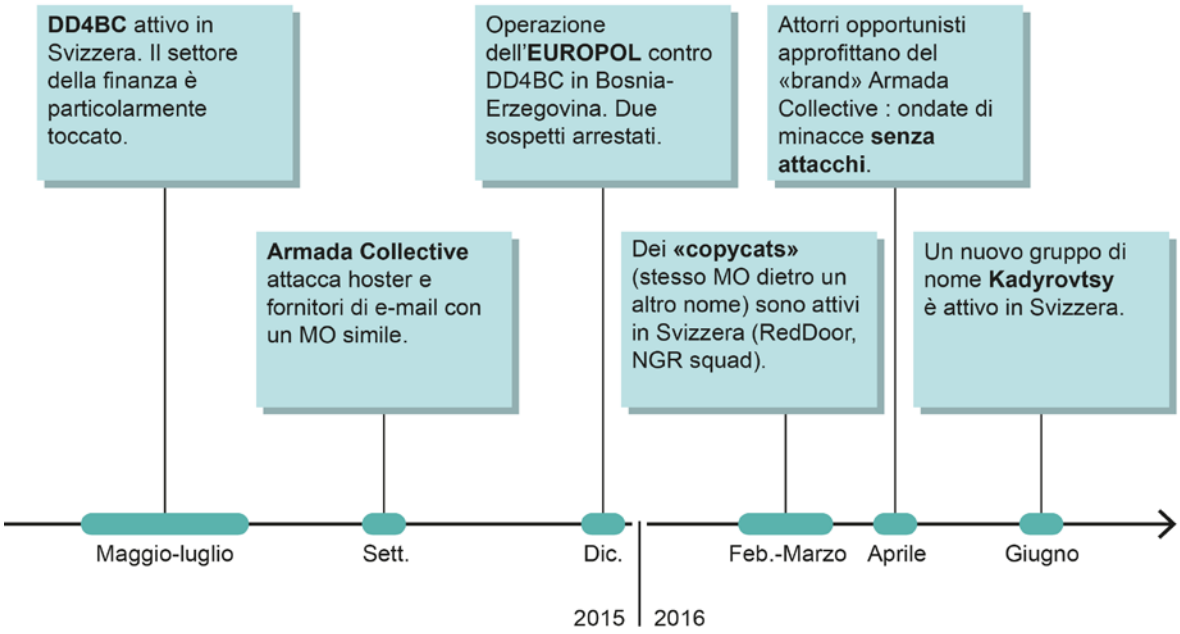


Figura 3: DDoS ed estorsione: timeline

Se questa operazione ha cambiato l'aspetto di questa minaccia, sono entrati in scena altri gruppi che si sono appropriati in parte dei suoi metodi. Innanzitutto, diversi gruppi hanno sferrato attacchi secondo il modus operandi tipico di DD4BC/Armada Collective, ossia un attacco DDoS dimostrativo seguito da un ricatto. Questi gruppi, che finora hanno sferrato un numero di attacchi limitato in Svizzera rispetto a quello di DD4BC/Armada Collective, hanno operato tra marzo e giugno sotto gli psudonimi RedDoor, NGR Squad, Gladius e Kadyrovtsy. Possiamo considerarli «copycats» che emulano un metodo sperimentato. Tuttavia, il fenomeno più significativo dei primi sei mesi dell'anno è la comparsa di gruppi meramente opportunisti che hanno sfruttato il nome di Armada Collective per inviare e-mail ricattatorie e minacciare attacchi DDoS, pur non avendo né l'intenzione né la capacità di effettuare questo tipo di attacchi, nemmeno a titolo dimostrativo. Per contro, basandosi su diversi articoli pubblicati su Armada Collective, questi gruppi hanno cercato di sfruttare il timore suscitato da Armada per estorcere denaro. Sovente gli indirizzi bitcoin attribuiti alle vittime erano identici; in tal caso l'attaccante non sarebbe stato in grado di distinguere chi aveva pagato e chi, non avendo pagato, avrebbe dovuto essere attaccato. Inoltre molte vittime contemporaneamente venivano minacciate di venir attaccate allo stesso giorno e alla stessa ora, cosa che avrebbe necessitato una notevole capacità di potenza per sferrare gli attacchi DDoS. Questo modo di procedere avvalora l'ipotesi che questi soggetti operino a fini opportunistici. Quale risvolto comico, una persona dichiaratasi portavoce del gruppo Armada Collective ha scritto a MELANI denunciando l'usurpazione spudorata del marchio «Armada Collective».

> I'm member of original Armada Collective and I have just noticed your report on Twitter. Armada Collective is dead. We have stopped all operations, because it wasn't profitable enough and risk was too big. When I realized that somebody is using our name I got mad. It is obviously an amateur copycat using our name who copied our text (maybe from your site) and is probably not even capable of launching DDoS attacks. Good luck with your investigation.

Figura 4: Messaggio ricevuto da MELANI mediante il suo modulo di segnalazione

Questo aumento dell'attività illustra chiaramente come l'estorsione sia un metodo redditizio per i criminali. Gli ultimi sviluppi dimostrano inoltre che i criminali possono basarsi su attacchi concreti, ma anche sul timore suscitato da un attacco ipotetico. In questa dinamica, un elemento difficile da controllare è quello della fonte d'ispirazione rappresentata da rapporti che evidenziano l'attività di questi soggetti. Riteniamo sia opportuno fornire informazioni su queste modalità operative. Non si può tuttavia escludere che un'«eco mediatica» intensa ne incentivi l'uso, ma soprattutto non si deve permettere agli attaccanti di sfruttare la notorietà acquisita da un gruppo o da tutto un modus operandi in seno all'opinione pubblica. In ogni caso, quando un gran numero di aziende riceve simultaneamente questo tipo di e-mail ricattatorie, occorre ribadire quanto sia importante la condivisione di informazioni e la segnalazione di eventuali incidenti. Le informazioni comunicate a un ente come MELANI facilitano l'allestimento di una panoramica per la valutazione di altri casi analoghi. Elementi quali gli indirizzi Bitcoin o le date degli attacchi rivestono molta importanza. Infine, ricordiamo che la protezione contro gli attacchi DDoS deve essere prioritaria, essendo essi un'arma alla quale numerosi truffatori possono ricorrere per vari motivi.

Raccomandazione:

Un'azienda colta alla sprovvista da un attacco DDoS difficilmente riuscirà ad adottare contromisure rapide ed efficaci. Le misure di sicurezza contro gli attacchi DDoS assumono un'importanza ancora maggiore per le aziende fortemente dipendenti dalle vendite online. In questi casi, la protezione della piattaforma di vendita dovrebbe essere considerata una priorità assoluta. Per questo si raccomanda di sviluppare una strategia da attuare nell'eventualità di un attacco di questo tipo e di reperire i nominativi dei servizi competenti in materia, sia interni che esterni, e degli altri interlocutori cui rivolgersi durante un'urgenza. Inoltre, sarebbe auspicabile che un'azienda affrontasse la problematica DDoS nel quadro della gestione generale dei rischi e che definisse una determinata strategia di difesa a livello aziendale, senza attendere di essere attaccata. Qualsiasi organizzazione può subire un attacco DDoS. Discutete con il vostro fornitore di servizi Internet delle vostre necessità e di adeguate misure di prevenzione. Una lista di controllo con l'indicazione delle misure da adottare contro gli attacchi DDoS è disponibile sul sito Web di MELANI al seguente link:

Liste di controllo e guide per le misure contro attacchi DDoS:

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

4.4.2 Infezione sul sito Web 20min.ch[7]

Già nel corso del passato semestre «Gozi ISFB», il *trojan* che colpisce il settore dell'e-banking, si è diffuso attraverso diversi portali d'informazione del gruppo editoriale Tamedia.

[7] http://www.srf.ch/news/schweiz/nach-malware-attacke-auf-20-minuten-was-sie-jetzt-tun-koennen (in tedesco)
http://www.20min.ch/digital/news/story/20minuten-ch-erneut-Ziel-von-Malware-Attacke-15457508 (in tedesco)
http://www.nzz.ch/digital/malware-auf-20minch-tamedia-gab-zu-frueh-entwarnung-ld.12431 (in tedesco)
http://www.tagesanzeiger.ch/digital/internet/Erneut-ein-Trojaner-auf-20minutench/story/19684342 (in tedesco; stato: 31 agosto 2016)

La notizia è comparsa anche nell'ultimo rapporto semestrale MELANI[8]. All'inizio di aprile di quest'anno l'incidente si è ripetuto, questa volta sul sito Web del giornale gratuito «20 Minuten», anch'esso di proprietà del gruppo Tamedia. A partire dal 7 aprile, l'Amministrazione federale e varie aziende hanno bloccato temporaneamente l'accesso al sito Web 20min.ch. Tamedia è stata informata della misura adottata. L'incidente scoperto da MELANI è stato causato da un *JavaScript* inserito in un file multimediale (*file di animazione SWF)* sul sito Web. Durante la navigazione viene avviato lo script che conduce il visitatore all'*exploit kit* «Niteris» che, a sua volta, scarica automaticamente il trojan «Gozi» sul computer della vittima. Pochi giorni dopo aver eliminato il malware, il sito Web è finito nuovamente nel mirino degli hacker. In quest'altro caso, però, l'attacco non era diretto soltanto a «20 Minuten» ma anche alla rete di un operatore pubblicitario esterno la cui finestra era stata inserita nel sito Web di «20 Minuten». Il malware «Bedep» è stato diffuso attraverso il noto exploit kit «Angler». Quest'ultimo è stato utilizzato per attacchi simili anche sui siti Web nytimes.com e bbc.com[9]. I quotidiani elettronici vengono consultati ogni giorno da milioni di visitatori e sono pertanto bersagli ideali per gli attacchi drive-by-download. Questo modus operandi è stato osservato più volte in Svizzera dalla primavera del 2015[10]. Secondo le affermazioni di «20 Minuten» i server di proprietà dell'azienda subiscono ogni giorno tra i 20 e i 50 attacchi informatici[11].

---

8 Rapporto semestrale MELANI 2015/2, capitolo 4.3.1.1 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2015-2.html (stato: 31 agosto 2016)

9 http://www.nzz.ch/digital/newssite-gesperrt-mittels-20minch-malware-verbreitet-ld.12263 (in tedesco; stato: 31 agosto 2016)

10 https://www.govcert.admin.ch/blog/21/20min.ch-malvertising-incident (in inglese; stato: 31 agosto 2016) https://www.govcert.admin.ch/blog/13/swiss-advertising-network-compromised-and-distributing-a-trojan https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature (in inglese; stato: 31 agosto 2016)

11 http://www.20min.ch/digital/news/story/Keine-Gefahr-fuer-die-Nutzer-der-20-Min-App-10440966 (in tedesco; stato: 31 agosto 2016)

Raccomandazione:

Per evitare infezioni di questo tipo sul versante del cliente finale, i sistemi operativi e le applicazioni devono essere aggiornati regolarmente (meglio se in automatico). Limitate il più possibile l'esecuzione di JavaScript (active scripting) mediante le impostazioni del browser o l'installazione di altri programmi o disattivatelo addirittura. In quest'ultimo caso tenete però presente che molti siti Web non funzioneranno più in modo corretto. Qualora la navigazione ne risentisse eccessivamente, allentate (per gradi) le limitazioni sino a raggiungere un «compromesso» accettabile. A seconda del metodo prescelto è anche possibile definire determinate pagine in cui è consentita l'esecuzione di JavaScript (*white listing*).

Se avete il sospetto che il vostro computer sia infettato, rivolgetevi a uno specialista che sia in grado di analizzare il PC e, all'occorrenza, ripulirlo dai software nocivi o reinstallare i programmi.

Regole di comportamento ➔ Navigazione:

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

4.4.3 OpnessunDorma di Anonymous contro portali d'impiego in Ticino e in Italia

37 portali d'impiego italiani e sette in altri Paesi (di cui 4 in Ticino) sono finiti nel mirino di un cyber-attacco tra il 9 e l'11 aprile 2016. Gli hacker hanno deturpato i siti Web delle aziende colpite e rubato milioni di dati. L'attacco è stato rivendicato dai gruppi «Anonymous Italia» e «LulzSecITA» che hanno pubblicato i dati di login degli utenti così come le informazioni relative alla struttura di varie banche dati e i nomi dei documenti di parecchie migliaia di curricula (i curricula stessi, però, non sono stati pubblicati). Entrambe le organizzazioni hanno indicato due motivi per l'attacco: da un lato l'intenzione di richiamare l'attenzione sul fatto che «le agenzie del lavoro sono dei parassiti che vivono e sopravvivono sulle spalle dei lavoratori». Dall'altro, gli autori dell'attacco puntavano a mettere a nudo la vulnerabilità e la scarsa sicurezza delle piattaforme IT su cui vengono salvati i dati degli utenti[12]. Il sito Web ticinoonline.ch ha pubblicato uno screenshot del sito Web deturpato di e-lavoro.ch (dell'Associazione industrie Ticinesi AITI), uno dei bersagli presi di mira insieme a BFKconsulting.ch, helvia.com e workandwork.ch[13], in cui si rinfaccia alle vittime ticinesi di essere sottomesse «ai diritti

[12] https://share.cyberguerrilla.info/?3263d9dcba87924c#nxVUhZU/s/diAc9ZJ1v+cjkH1F+oT3K+iiljOHLLT+0= (stato: 31 agosto 2016)

[13] http://www.rsi.ch/news/ticino-e-grigioni-e-insubria/Siti-ticinesi-hackerati-7176668.html (stato: 31 agosto 2016)
http://www.radiondadurto.org/2016/04/12/anonymous-italia-operazione-nessundorma-e-la-violazione-della-legge-sulla-privacy/ (stato: 31 agosto 2016)
http://www.tio.ch/News/Ticino/Cronaca/1079978/Attacco-hacker-colpiti-4-siti-ticinesi--Rubati-milioni-di-dati/ (stato: 31 agosto 2016)

svizzeri xenofobi e razzisti» e di pubblicare inserzioni di lavoro che si rivolgono esclusivamente alla popolazione residente in Svizzera[14].

4.4.4 Hacker al Politecnico federale

Nel gennaio scorso, un hacker è penetrato per alcuni giorni nella rete del Politecnico federale di Zurigo utilizzando dati di accesso sconosciuti; attraverso il sistema dell'ETH ha poi effettuato ordinazioni di software e scaricato dati sensibili. Una volta accertato l'uso improprio della rete, l'ETH ha contattato il ministero pubblico del Centro di competenza per la cybercriminalità di Zurigo che insieme agli investigatori di polizia ha tempestivamente adottato le prime misure di sicurezza e portato avanti le indagini. Il presunto autore dell'attacco ha potuto essere arrestato a soli 10 giorni dall'inizio dell'inchiesta. L'imputato si trova in custodia preventiva. È stato aperto un procedimento penale per intrusione in un sistema per l'elaborazione dei dati e per l'acquisizione illecita di dati.[15]

4.5 Social engineering, phishing

Oltre agli attacchi tecnici, tra gli hacker sono popolari anche i metodi che sfruttano le debolezze umane.

4.5.1 Phishing: statistiche

Nel corso degli ultimi anni è notevolmente aumentato il numero di richieste relative al *phishing* che sono state evase da MELANI. Per elaborare in maniera più efficiente le numerose segnalazioni di phishing ricevute, nel 2015 la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione ha attivato il sito Internet «antiphishing.ch» sul quale è possibile segnalare pagine sospette di phishing. Nel primo semestre 2016, attraverso questo portale sono state segnalate complessivamente 2343 singole pagine. La figura 5 mostra le pagine di phishing segnalate settimanalmente. Il numero vari nel tempo per svariati motivi: oltre alle oscillazioni stagionali dovute al fatto che nei periodi di vacanza vengono effettuate meno segnalazioni, gli hacker cambiano regolarmente il Paese che desiderano colpire.

Figura 5: Pagine di phishing segnalate e confermate settimanalmente su antiphishing.ch

[14] A tale proposito viene citato in particolare un gruppo di aziende che opera nella produzione e nella vendita di protesi ortopediche.

[15] https://www.ethz.ch/de/news-und-veranstaltungen/eth-news/news/2016/02/mm-mutmasslicher-hacker-verhaftet.html (stato: 31 agosto 2016)

4.5.2 IL «CEO Fraud» persiste e si perfeziona

Il modus operandi del «CEO Fraud» è stato più volte evocato da MELANI nelle sue newsletter o nei suoi rapporti semestrali. 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 (solitamente) all'estero. La richiesta parte perlopiù da un indirizzo e-mail contraffatto; in alcuni casi anche manomettendo un conto esistente. Le motivazioni per il versamento variano, includendo spesso un'operazione finanziaria urgente ed estremamente sensibile (in particolare acquisti). Nel contesto può intervenire un consulente o uno studio legale fittizio la cui identità è stata usurpata. I truffatori sono in grado di esercitare una forte pressione sull'impiegato preso di mira, avanzando il pretesto di una situazione urgente per costringerlo a effettuare il versamento e talvolta aggirando i processi esistenti.

Nei sei mesi in rassegna, alcuni casi sono stati alla ribalta della cronaca all'estero. Ad esempio, l'azienda austriaca FACC, che opera nel settore aerospaziale, ha perso 42 milioni di euro in una truffa analoga, a seguito della quale il suo CEO[16] (Chief Executive Officer, amministratore delegato) è stato licenziato. Anche in Svizzera sono stati segnalati a MELANI alcuni casi. Questo tipo di frode non si attenua in nessun Paese, ma sembra perfezionarsi per essere sempre più efficace. Si tratta di un modo di agire tipico dei gruppi criminali attivi su Internet: se un modus operandi si è dimostrato valido, verrà mantenuto con perfezionamenti e aggiornato di singoli stadi della truffa.

Le reti sociali rappresentano una vera e propria miniera d'oro per la ricerca iniziale di informazioni su un'azienda. LinkedIn è particolarmente interessante per i truffatori che cercano notizie sulle relazioni commerciali, sull'identità e sulle funzioni degli impiegati. Il registro di commercio, o più semplicemente il sito Web dell'azienda, possono contenere informazioni molto utili. Se le informazioni per organizzare la frode non sono disponibili in rete, i criminali possono effettuare dei contatti telefonici preparatori e in alcuni casi utilizzare l'invio di fax con l'intestazione di un'amministrazione cantonale. Tra le informazioni cercate primeggiano le coordinate precise degli impiegati dell'ufficio contabilità, ai quali vengono rivolte in ultima istanza le richieste fraudolente di pagamento. Queste prime prese di contatto permetteranno di inviare e-mail mirate, che illustrano situazioni del tutto plausibili per l'impresa in questione.

Per l'invio di e-mail apparentemente legittime, i truffatori utilizzano in particolare nomi di dominio simili a quello dell'azienda mirata. Ad esempio, nel mese di giugno 2016 MELANI è venuta a sapere della registrazione simultanea di 20 nomi di dominio che imitavano quelli di aziende svizzere. Inviando e-mail tramite questi domini, i truffatori cercano di ingannare i destinatari che pensano di essere in contatto con l'azienda legittima. Un altro tipo di e-mail molto utilizzato dai criminali è quello in cui si fa riferimento a una posizione o a una professione, ad esempio «lawyer.com», «president.com», «consultant.com».

[16] http://www.reuters.com/article/us-facc-ceo-idUSKCN0YG0ZF (in inglese; stato: 31 agosto 2016)

Raccomandazione:

È molto difficile ostacolare questi tentativi di frode. I truffatori sono in grado di mascherare la propria identità ed origine e, se necessario, di cambiare facilmente l'indirizzo di posta elettronica utilizzato. La raccomandazione principale in materia di prevenzione è senza dubbio la sensibilizzazione del personale, soprattutto dei collaboratori che occupano posizioni chiave, verso questi fenomeni. La regola principale consiste nel non fornire alcuna informazione e non effettuare nessuna azione a seguito di richieste inconsuete e sospette, anche se si è messi sotto pressione. Inoltre si raccomanda di controllare le informazioni sull'azienda disponibili online. Infine, i processi devono essere definiti e seguiti da tutti e in ogni momento. Per i trasferimenti di denaro, si raccomanda di seguire un principio di controllo plurimo con l'utilizzo di una firma collettiva.

4.6 Crimeware

Il crimeware è una forma di malware sviluppata da criminali economici che dal punto di vista criminologico rientra nel campo della criminalità informatica e giuridicamente rientra nel settore del danneggiamento di dati e dell'abuso di un impianto per l'elaborazione dei dati. Anche nel primo semestre del 2016 la maggior parte delle infezioni è da attribuire a «Downadup» (noto anche come «Conficker»), un worm che esiste già da più di otto anni e che si diffonde tramite una falla di sicurezza rilevata nel sistema operativo Windows nel 2008 e perciò riparata da lungo tempo. Ai vertici della statistica si segnalano però alcuni cambiamenti nel primo semestre del 2016, con la comparsa di spambot che, in termini percentuali, hanno scalzato i trojan di e-banking. Al secondo posto si colloca il malware lethic, che distribuisce spam inerenti prodotti farmaceutici e pubblicità riguardanti merci contraffatte. Necurs, terzo classificato, si è specializzato nell'invio del trojan di crittografia Locky e del malware di e-banking Dridex. Colpisce la scomparsa dalle prime posizioni del malware di e-banking Dyre. Gli arresti negli ambienti vicini a Dyre hanno praticamente portato all'eliminazione di questo malware, perlomeno nel breve periodo. Per maggiori informazioni si rimanda al capitolo 5.3.3.

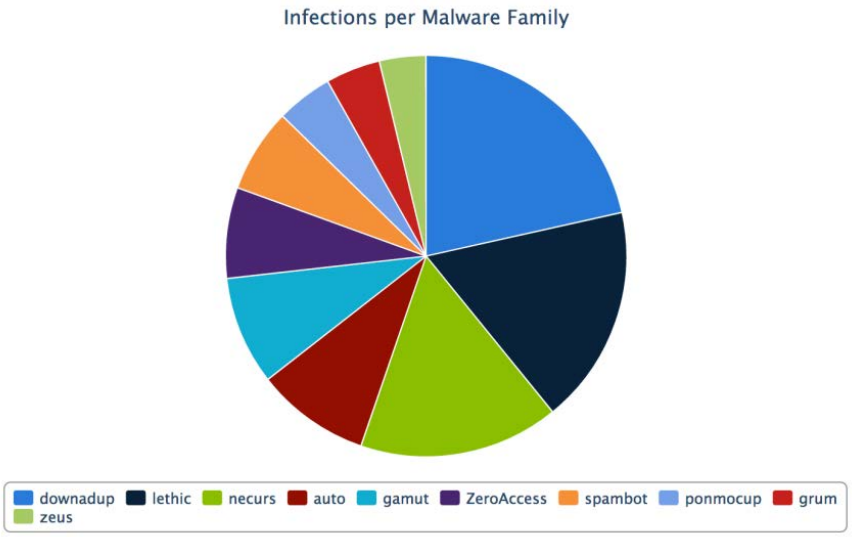


Figura 6: Distribuzione dei malware in Svizzera secondo i dati in possesso di MELANI. Giorno di riferimento: 30 giugno 2016. I dati attuali sono disponibili al link: http://www.govcert.admin.ch/statistics/dronemap/

4.6.1 App nocive per Android sempre più frequenti in Svizzera

Nei mesi di giugno e luglio del 2016 sono stati inviati migliaia di SMS a destinatari in Svizzera che davano l'impressione di provenire dalla Posta Svizzera, ma di fatto contenevano un link a un sito Web in Lettonia. Cliccando su questo link, la vittima veniva reindirizzata a una pagina Web piratata e veniva indotta a installare un'app nociva per Android[17]. Se il destinatario ignorava le notifiche di sicurezza di Android e installava l'app, infettava il proprio dispositivo con un malware.

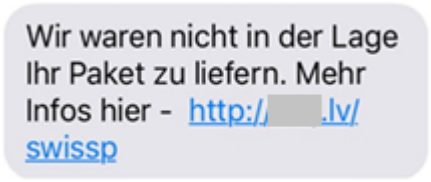


Figura 7: SMS contraffatto che sembra provenire dalla Posta Svizzera

Il malware si mimetizzava dietro il nome «*SwissPost*» e utilizzava il logo della Posta Svizzera. L'app, senza che l'utente se ne accorgesse, copiava in background i dati di accesso di popolari app come Facebook, Uber o Viber e li trasmetteva agli hacker.

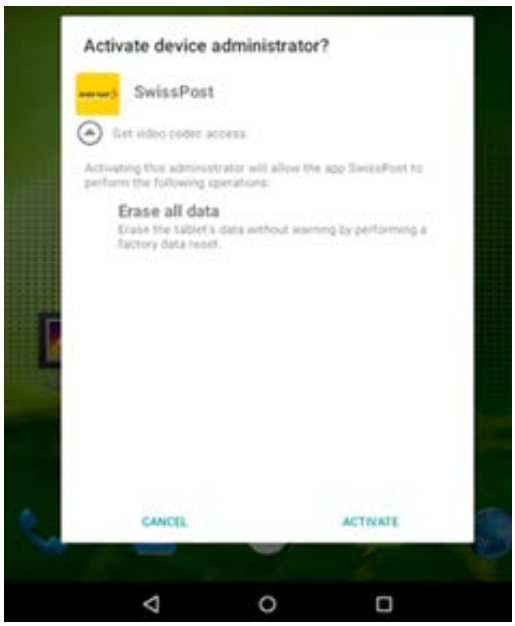


Figura 8: Il malware si mimetizza da app della Posta Svizzera

Raccomandazione:

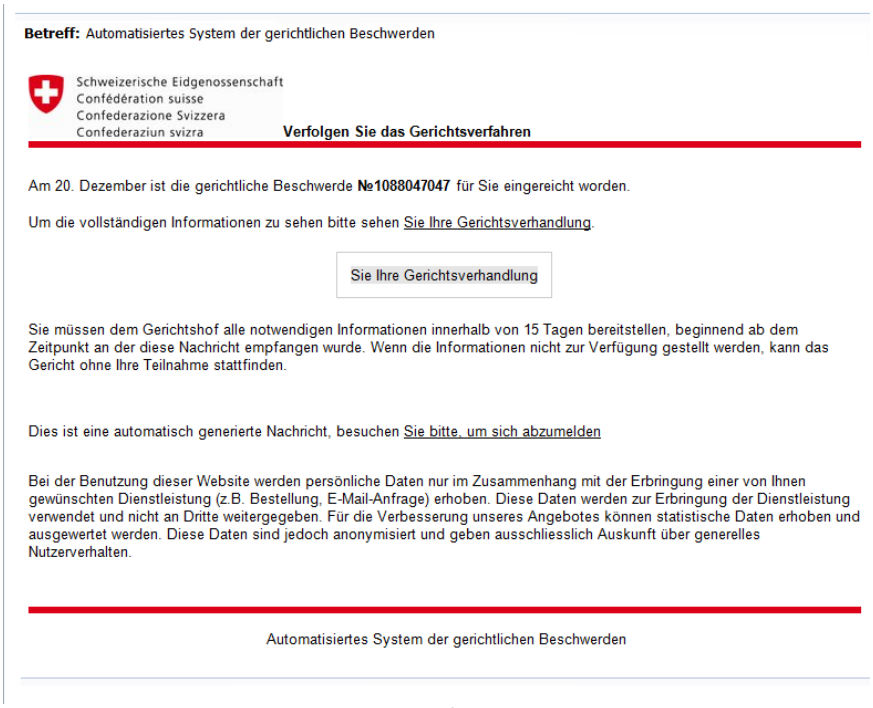
In generale non si dovrebbero installare app non ufficiali. La cosa migliore da fare è utilizzare esclusivamente l'App Store ufficiale del produttore.

[17] https://www.govcert.admin.ch/blog/24/sms-spam-run-targeting-android-users-in-switzerland (in inglese; stato: 31 agosto 2016)

4.6.2 Mandati di comparizione contraffatti distribuiscono trojan di crittografia

La minaccia dei cosiddetti *trojan di crittografia* è cresciuta anche durante il periodo in rassegna. La semplicità del modus operandi, così come la disponibilità ancora eccessiva delle vittime a cedere a richieste di riscatto, ha alimentato la propagazione dei *ransomware*.

Per indurre l'utente a cliccare sul link di un'e-mail o ad aprire allegati, scaricando il ransomware sul computer, l'hacker deve riuscire a rendere il più plausibile possibile il contenuto dell'e-mail. In molti casi, il messaggio viene spacciato per una comunicazione di un'istituzione che il destinatario conosce e considera affidabile. Così il malcapitato non si insospettisce. MELANI ha riferito di un episodio analogo nel GovCERT-Blog del mese di gennaio 2016[18]. In questo caso specifico si trattava di un'ondata di e-mail che diffondevano il ransomware «TorrentLocker». La mail fraudolenta comunicava al destinatario che era stato presentato un ricorso nei suoi confronti e che veniva convocato per un'udienza in tribunale. Per ottenere ulteriori informazioni, il destinatario doveva cliccare su un link e scaricare dei documenti. In questa occasione i malfattori hanno fatto leva non solo sull'attendibilità dell'autorità, ma anche sull'incertezza e sulla paura dei destinatari delle e-mail. Le intimidazioni sono sempre un buon espediente per indurre le vittime a cliccare su un link. Tuttavia, i tribunali non utilizzano mai la posta elettronica come mezzo di comunicazione per una convocazione ufficiale.



Betreff: Automatisiertes System der gerichtlichen Beschwerden

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Verfolgen Sie das Gerichtsverfahren

Am 20. Dezember ist die gerichtliche Beschwerde **№1088047047** für Sie eingereicht worden.

Um die vollständigen Informationen zu sehen bitte sehen Sie Ihre Gerichtsverhandlung.

Sie Ihre Gerichtsverhandlung

Sie müssen dem Gerichtshof alle notwendigen Informationen innerhalb von 15 Tagen bereitstellen, beginnend ab dem Zeitpunkt an der diese Nachricht empfangen wurde. Wenn die Informationen nicht zur Verfügung gestellt werden, kann das Gericht ohne Ihre Teilnahme stattfinden.

Dies ist eine automatisch generierte Nachricht, besuchen Sie bitte, um sich abzumelden

Bei der Benutzung dieser Website werden persönliche Daten nur im Zusammenhang mit der Erbringung einer von Ihnen gewünschten Dienstleistung (z.B. Bestellung, E-Mail-Anfrage) erhoben. Diese Daten werden zur Erbringung der Dienstleistung verwendet und nicht an Dritte weitergegeben. Für die Verbesserung unseres Angebotes können statistische Daten erhoben und ausgewertet werden. Diese Daten sind jedoch anonymisiert und geben ausschliesslich Auskunft über generelles Nutzerverhalten.

Automatisiertes System der gerichtlichen Beschwerden

Figura 9: Al destinatario viene comunicato che è stato presentato un ricorso del tribunale nei suoi confronti. Per ottenere ulteriori informazioni, deve cliccare su un link e scaricare dei documenti. Questi ultimi contengono un malware.

4.6.3 Candidature spontanee con trojan di crittografia

Altri metodi privilegiati per indurre i destinatari a cliccare su un link o aprire un file fanno leva sugli interessi o sulle esigenze delle vittime, oppure puntano a conquistare la loro fiducia, chiamandole ad esempio per nome e cognome. Nel maggio scorso, in Svizzera, circolavano

[18] https://www.govcert.admin.ch/blog/17/torrentlocker-ransomware-targeting-swiss-internet-users (in inglese; stato: 31 agosto 2016)

e-mail che utilizzavano proprio questa tecnica. I malcapitati, selezionati in modo mirato, ricevevano delle e-mail contenenti candidature spontanee. Per avere accesso al dossier completo, i destinatari erano invitati a cliccare su un collegamento che avrebbe dovuto farli accedere all'intero dossier. Il link a Dropbox reindirizzava però direttamente ai trojan di crittografia «Petya» e «Mischa». Ultimamente, dietro candidature spontanee dall'aspetto del tutto innocuo si cela anche il malware «Locky», ancora molto attivo sia in Svizzera che all'estero.

4.6.4 Trojan di crittografia: aspetti tecnici

Tra gli aspetti tecnici rilevanti del primo semestre segnaliamo la versione 3.1 di CryptXXX. Questo *virus* non solo crittografa i dati sul computer della vittima e quelli salvati nei dispositivi collegati, ma è anche in grado, scaricando un ulteriore *malware* («stiller.dll»), di impossessarsi di password e altri dati d'accesso[19].

È tornato alla ribalta anche «CBT-Locker», un ransomware molto attivo soprattutto nell'estate del 2014. Si tratta di una nuova versione che si è specializzata nel crittografare il contenuto di siti Web. Il metodo con cui viene diffuso il virus non è ancora del tutto chiaro. Analisi di diverse fonti evidenziano tuttavia come l'attacco avvenga attraverso pagine vulnerabili di Wordpress. Se il sito Web viene infettato, compare un messaggio che comunica le modalità per rientrare in possesso dei dati personali. Il malware decodifica due file in base al principio di casualità per dimostrare che gli hacker sono in grado di decifrare i dati. Viene anche mostrato un video che, parodicamente, ripropone una sorta di supporto clienti e spiega come ottenere i *bitcoin* necessari per il pagamento del riscatto. Inoltre, è disponibile una funzione di chat che consente di mettersi in contatto con gli hacker, qualora fossero necessarie ulteriori informazioni[20]. CBT-Locker non è, però, l'unico trojan di crittografia che comunica l'avvenuta infezione alle proprie vittime in modo fantasioso. «Cerber», comparso in Svizzera durante l'ultimo semestre, è ad esempio il primo *macro-malware* a dare letteralmente voce alla richiesta di riscatto attraverso l'altoparlante del computer: «Attention! Attention! Attention! Your documents, photos, databases and other important files have been encrypted!».

Per aumentare ulteriormente la pressione psicologica sulla vittima, il trojan di estorsione «Jigsaw» adotta un metodo particolarmente perfido: per ogni ora trascorsa, il ransomware cancella un determinato numero di documenti e al tempo stesso aumenta l'importo del riscatto. Nel giro di 72 ore vengono cancellati tutti i documenti[21].

Nel frattempo, anche gli utenti Mac non possono più pensare di essere al sicuro. Il ransomware «KeRanger», scoperto in marzo, è il primo trojan di crittografia in grado di attaccare anche le piattaforme OS X[22]. Con un certificato valido per le applicazioni Mac, i criminali

---

19 https://www.proofpoint.com/us/threat-insight/post/cryptxxx-ransomware-learns-samba-other-new-tricks-with-version3100 (in inglese; stato: 31 agosto 2016). Il trojan di crittografia CryptXXX, scoperto per la prima volta in aprile, è in grado di aggirare il tool di decodifica sviluppato da Kaspersky Lab.

20 http://www.bleepingcomputer.com/news/security/ctb-locker-for-websites-reinventing-an-old-ransomware/ http://www.heise.de/security/meldung/Admins-aufgepasst-Krypto-Trojaner-befaellt-hunderte-Webserver-3116470.html (in inglese; stato: 31 agosto 2016)

21 http://blog.trendmicro.com/trendlabs-security-intelligence/jigsaw-ransomware-plays-games-victims/ (in inglese; stato: 31 agosto 2016)

22 Il ransomware FileCoder, rilevato da Kaspersky Lab nel 2014, era ancora incompleto al momento della sua scoperta e quindi non ha potuto danneggiare i sistemi operativi OS X. http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/ (in inglese; stato: 31 agosto 2016)

hanno infettato due programmi d'installazione del software di BitTorrent «Transmission» per OS X nella versione 2.90. Il malware è rimasto sul sito Web tra il 4 e il 5 marzo 2016. Chi ha scaricato il programma «Transmission» per OS X in questo lasso di tempo è stato infettato. I file d'installazione infettati sono poi stati cancellati da Transmission. Nel frattempo, Apple ha ritirato il *certificato*[23].

Raccomandazione:

In base a quanto riportato da Kaspersky Lab, tra l'aprile 2015 e il marzo 2016 il numero di ransomware si è quintuplicato rispetto allo stesso periodo dell'anno precedente. Questa crescita esponenziale ha determinato un aumento, negli ultimi sei mesi, degli avvisi pubblicati da varie organizzazioni. Nel mese di maggio l'Ufficio federale della sicurezza della tecnologia dell'informazione tedesco (BSI) ha divulgato un rapporto dettagliato sul tema dei ransomware; la polizia olandese in collaborazione con Europol e due società di sicurezza informatica (Kaspersky Lab e Intel Security) ha creato il sito Web «nomoreransom.org». Sempre nel mese di maggio MELANI in collaborazione con vari partner svizzeri ha organizzato una giornata di sensibilizzazione contro i «ransomware» e richiamato l'attenzione in particolare su quattro misure:

- Eseguire regolarmente copie di sicurezza (backup) dei dati: La copia di sicurezza dovrebbe essere salvata offline, cioè su un supporto esterno, ad esempio un disco rigido esterno. Assicuratevi che il supporto su cui eseguite la copia di sicurezza venga staccato dal computer subito dopo il processo di backup.
- Aggiornare regolarmente le applicazioni e i plug-in installati.
- MELANI raccomanda agli utenti Internet di non aprire nessun allegato e-mail sospetto anche se i messaggi provengono da mittenti apparentemente affidabili e
- di assicurarsi che sul proprio computer sia installato un antivirus che venga tenuto sempre aggiornato.

Misure contro i ransomware:

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

Ransomware: minacce attuali, prevenzione e reazione del BSI:

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

Progetto No More Ransom:

https://www.nomoreransom.org/decryption-tools.html (in inglese)

Regole di comportamento ➔ E-mail

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

[23] http://www.welivesecurity.com/2016/03/07/new-mac-ransomware-appears-keranger-spread-via-transmission-app/ (in inglese; stato: 31 agosto 2016)

4.7 Misure di prevenzione

4.7.1 Prima giornata di sensibilizzazione MELANI: Ransomware Day

Il 19 maggio 2016 MELANI, insieme a numerosi partner, ha indetto la prima giornata di sensibilizzazione contro i *ransomware*. In questa occasione organizzazioni di vari settori, produttori di software, uffici federali, associazioni svizzere e organizzazioni a tutela dei consumatori hanno affrontato l'argomento e divulgato diverse pubblicazioni per sensibilizzare la popolazione su questo tema. Al momento si sta valutando se e come riproporre una giornata di questo genere.

5 La situazione a livello internazionale

5.1 Spionaggio

5.1.1 Campagna elettorale scombussolata da un attacco di spionaggio

Alla vigilia del Congresso nazionale del Partito democratico statunitense a Philadelphia (USA), la presidente del Comitato nazionale Debbie Wasserman Schultz (Democratic National Committee, DNC) ha rassegnato le dimissioni[24]. Il momento è stato palesemente poco propizio per un cambio ai vertici del partito. Cosa era successo? Due giorni prima Wikileaks[25] aveva pubblicato 20 000 e-mail interne di leader del DNC dalle quali era emerso che il Comitato non solo prediligeva la candidatura di Hillary Clinton, ma aveva anche intrapreso sforzi coordinati per favorirla nei confronti del suo maggiore competitor Bernie Sanders.

Per risalire agli inizi della storia, però, occorre fare un passo indietro di oltre un mese, quando il «Washington Post»[26] aveva diffuso la notizia di un attacco all'infrastruttura digitale del DNC. Già da un anno i pirati informatici rovistavano tra le analisi sull'avversario repubblicano Donald Trump e leggevano anche, come è stato dimostrato con clamore dalla pubblicazione su Wikileaks, la corrispondenza via e-mail.

Alla fine del mese di aprile 2016, i responsabili IT del DNC si sono accorti di alcuni «movimenti» strani e hanno deciso di rivolgersi agli esperti della ditta Crowdstrike. L'Incident Response Team di Crowdstrike ha poi scoperto due hacker che agivano separatamente nella rete del partito identificandoli con due gruppi a loro noti come «COZY BEAR» e «FANCY BEAR». «FANCY BEAR», famoso per l'attacco al Bundestag tedesco del 2015, secondo quanto riportato da Crowdstrike, era attivo nella rete diel DNC già dall'estate del 2015. L'infiltrazione di «COZY BEAR», invece, ha potuto essere documentata soltanto a partire dal

---

[24] https://www.washingtonpost.com/politics/hacked-emails-cast-doubt-on-hopes-for-party-unity-at-democratic-convention/2016/07/24/a446c260-51a9-11e6-b7de-dfe509430c39_story.html (in inglese; stato: 31 agosto 2016)

[25] https://wikileaks.org/dnc-emails/ (in inglese; stato: 31 agosto 2016)

[26] https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html (in inglese; stato: 31 agosto 2016)

mese di aprile 2016. Nel suo rapporto[27] Crowdstrike ha avanzato l'ipotesi che dietro gli attacchi vi fossero due diversi servizi segreti russi. Lo stesso giorno, l'azione è stata rivendicata da un hacker di presunta nazionalità rumena con lo pseudonimo «Guccifer 2.0», il quale ha dichiarato di essere l'unico responsabile dell'attacco. Inoltre, ha annunciato di voler pubblicare stralci del suo «bottino» su Wikileaks. I fatti hanno indotto Crowdstrike ad aggiornare il rapporto per smascherare Guccifer 2.0. Al fianco di Crowdstrike si sono schierati in un secondo tempo le società di sicurezza informatica Fidelis Cybersecurity e Mandiant, giunte alle medesime conclusioni[28], così come Thomas Rid, professore al King's College di Londra. Quest'ultimo ha rilevato nel malware trovato nella rete del DNC un server di comando e di controllo (C&C) identico a quello già utilizzato per l'attacco al Bundestag tedesco. L'origine rumena di «Guccifer 2.0» e quindi la sua credibilità, è stata poi messa definitivamente in dubbio nel momento in cui l'hacker si è dimostrato incapace di conversare fluentemente e in maniera comprensibile con un giornalista di madre lingua rumena.

Conclusione:

Questo episodio dimostra chiaramente come la politica del potere possa esercitare la propria influenza nel cyberspazio. Lo spionaggio dei dati sensibili di un avversario e la pubblicazione selettiva di informazioni diffamanti sono un ottimo strumento per condizionare rapidamente l'opinione pubblica.

5.2 Furto di dati

5.2.1 Spoglio pubblico indesiderato di registri elettorali

Nel primo semestre del 2016 le sottrazioni di dati dai registri elettorali sono finite per ben due volte sulle prime pagine dei giornali. Il 30 marzo 2016 un hacker anonimo ha pubblicato un file contenente le informazioni personali di 50 milioni di cittadini turchi[29]. Le informazioni comprendevano cognomi, indirizzi, nomi di battesimo dei genitori, luoghi e date di nascita nonché numeri d'identificazione nazionali. Oltre ai dati è stata divulgata anche una presa di posizione che rimproverava al governo Erdogan di non saper proteggere in maniera adeguata i dati dei cittadini. In un secondo tempo si è appreso che non si trattava di dati aggiornati, ma risalenti al 2008. La loro autenticità è stata però confermata dall'agenzia di stampa Associated Press. La pubblicazione di informazioni di questo tipo cela sempre il pericolo che possano fungere da base per furti d'identità.

A distanza di una sola settimana, le Filippine hanno annunciato una sottrazione di dati ancora più estesa[30]. A seguito di un attacco alla banca dati della Commission on Elections filippina (COMELEC[31]) sono stati divulgati i dati di 55 milioni di elettori filippini tra cui, secondo

---

27 https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ (in inglese; stato: 31 agosto 2016)

28 https://www.wired.com/2016/07/heres-know-russia-dnc-hack/ (in inglese; stato: 31 agosto 2016)

29 https://www.wired.com/2016/04/hack-brief-turkey-breach-spills-info-half-citizens/ (in inglese; stato: 31 agosto 2016)

30 http://www.theregister.co.uk/2016/04/07/philippine_voter_data_breach/ (in inglese; stato: 31 agosto 2016)

31 La COMELEC è una delle tre Commissioni governative filippine. Il suo compito principale consiste nell'applicare leggi e regolamenti che consentano lo svolgimento di elezioni nelle Filippine.

quanto riportato dal fornitore del software di sicurezza Trend Micro[32], vi erano anche informazioni sensibili come ad esempio password e 15,8 milioni di impronte digitali registrate. L'incidente vero e proprio risale al 27 marzo 2016 (defacement del sito Web della COMELEC da parte di «Anonymous Philippines»). Alcuni giorni dopo, i dati rubati sono stati pubblicati online da un utente Facebook chiamato «Lulzsec Pilipinas».

5.2.2 Informazioni condivise involontariamente con la rete professionale

Oltre alle informazioni che, come descritto al capitolo 5.2.1, devono essere comunicate alle autorità, molti utenti Internet forniscono volontariamente un gran numero di dati ad aziende private. Ovviamente, anche queste informazioni non sono immuni da furti. Già nel 2014 la rete professionale LinkedIn era stata colpita da un attacco che aveva causato la pubblicazione online di 6,5 milioni di password crittografate. A metà maggio un hacker chiamato «Pace» ha messo in vendita per 5 bitcoin (pari a fr. 2000 circa) 117 milioni di informazioni di account inclusi indirizzi e-mail e password crittografate[33]. LinkedIn ha confermato la correttezza delle informazioni. Pur trattandosi di dati che risalgono ormai a quattro anni fa, la loro vendita rappresenta comunque un pericolo, poiché numerosi utenti Internet tendono a non cambiare mai o solo raramente le password e utilizzano la stessa password anche per altri servizi.

Raccomandazione:

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

Informazioni sulla sicurezza IT per le PMI:

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

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

Regole di comportamento per le password

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

5.2.3 Dati di accesso a Twitter sul mercato nero

Quando i dati di accesso finiscono nelle mani dei criminali, non sempre devono essere colpevolizzati gli operatori online. Nel mese di giugno sono stati offerti sul mercato nero 32 mi-

[32] http://blog.trendmicro.com/trendlabs-security-intelligence/55m-registered-voters-risk-philippine-commission-elections-hacked/ (in inglese; stato: 31 agosto 2016)

[33] http://motherboard.vice.com/read/another-day-another-hack-117-million-linkedin-emails-and-password (in inglese; stato: 31 agosto 2016)

lioni di dati di accesso a Twitter (password incluse) [34]. In questo caso si presume che le password siano state copiate e poi trasmesse agli hacker attraverso un malware che si era annidato nei browser degli utenti finali. Quasi sempre, la copia e la vendita dei dati di accesso costituisce un'ulteriore forma di pubblicità lucrativa per i criminali. Per questo motivo, nella maggior parte dei casi anche il malware concepito per altri scopi (come ad es. le truffe nel settore dell'e-banking o la crittografia) annovera un *keylogger* come funzione secondaria.

5.3 Sistemi industriali di controllo

5.3.1 Malware in una centrale nucleare tedesca

Nell'area isolata della centrale nucleare di Gundremmingen (Germania) sono stati rinvenuti, nell'ambito di lavori di controllo per la preparazione di una revisione, due diversi malware su 18 supporti dati rimovibili e su di un computer. Secondo le informazioni fornite dalla centrale nucleare, il sistema interessato rientrava tra le attrezzature per la movimentazione delle barre di combustibile nucleare e veniva utilizzato solamente a scopo di visualizzazione. In altre parole, pare che non avesse alcuna influenza sul controllo dei processi. Stando alle notizie pubblicate dai media, uno dei *malware* incriminati sarebbe «Conficker». Ampiamente diffuso e conosciuto già dal 2008, nonostante Microsoft abbia fornito un aggiornamento di sicurezza poco dopo la sua comparsa, «Conficker» rimane il malware più presente anche in Svizzera secondo la statistica di MELANI/GovCERT.ch. Il secondo malware rinvenuto dovrebbe essere «Ramnit», attivo dal 2010, la cui botnet è stata disattivata nel 2015 da Europol e dal fornitore di soluzioni per la sicurezza Symantec.

Il fatto che una *falla di Windows*, rilevata in una centrale nucleare otto anni fa, non sia stata ancora colmata può risultare sorprendente di primo acchito. Tuttavia, il sistema interessato si trovava nell'area isolata (ossia non collegata a Internet) dell'impianto. Spesso, inoltre, gli impianti dell'area industriale vengono certificati all'installazione; ciò significa che il produttore ne garantisce il funzionamento ineccepibile in una precisa configurazione e, per qualsiasi modifica al sistema − anche dovuta a un aggiornamento di sicurezza − tale garanzia decade. Considerato poi che i sistemi operano in modalità isolata, il rischio di un malfunzionamento causato da un aggiornamento è decisamente superiore rispetto alla minaccia derivante da una falla di sicurezza. Infine, dato l'isolamento totale dei sistemi, le falle interne di sicurezza dovrebbero risultare irrilevanti. Tuttavia, esistono situazioni in cui un malware può penetrare anche in aree molto protette:

- I sistemi, essendo privi di connessione a Internet, non possono essere sottoposti a interventi di manutenzione e controlli online. In questo caso, la rete può essere esposta a qualche rischio nel momento in cui vengono collegati sistemi esterni (ad es. notebook o chiavette USB) per la manutenzione, l'importazione o l'esportazione di dati.
  Un'operazione di questo tipo consente teoricamente di aggirare il cosiddetto *air gap* (ossia l'isolamento del sistema) facendo penetrare un virus. Un esempio reale è fornito dal worm informatico «Stuxnet» che alcuni anni fa è riuscito a insinuarsi in un impianto di arricchimento dell'uranio iraniano tramite una chiavetta USB.

- Il worm era presente nel computer sin dall'inizio senza però risultare evidente. Questo caso potrebbe verificarsi se il computer venisse collegato a Internet in fase

[34] https://techcrunch.com/2016/06/08/twitter-hack/ (in inglese; stato: 31 agosto 2016)

d'installazione ed isolato solo in un secondo tempo oppure se l'infezione fosse già presente nel supporto dati con cui i file d'installazione sono stati caricati sul computer.

Conclusione:

Per gli attacchi mirati si utilizzano in genere malware programmati appositamente che vengono fatti circolare in misura limitata in modo da non essere intercettati. Pertanto, nel caso della centrale nucleare, si può sostanzialmente escludere un attacco mirato.

Tuttavia, anche per le infezioni «accidentali» vi è sempre il rischio di danni collaterali: il malware potrebbe innescare malfunzionamenti nel sistema provocandone, ad esempio, l'arresto spontaneo. Poiché però le aree sensibili di una centrale nucleare vengono controllate analogicamente, anche un episodio come quello accaduto a Gundremmingen non avrebbe avuto ripercussioni sui processi critici.

5.3.2 Rapporto su un attacco informatico ai danni di una centrale idrica

Nel mese di marzo 2016[35] Verizon, azienda che opera nel settore della sicurezza, ha pubblicato nel proprio «Data Breach Report» i risultati di una valutazione proattiva effettuata presso una società per l'approvvigionamento di acqua potabile. All'azienda è stato attribuito il nome fittizio di «Kemuri Water Company (KWC)». Verizon non ha divulgato informazioni più precise sulla società. In questa valutazione sono state riscontrate tracce di un attacco informatico al sito Web di KWC. L'applicazione Web per i pagamenti è stata colpita attraverso falle conosciute. Su questo sistema front-end erano stati salvati in chiaro, all'interno di un *file .ini*, anche i dati di accesso al sistema back-end (IBM AS/400) che gli hacker sono riusciti a intercettare. Il sistema back-end, una soluzione molto in uso a cavallo tra il vecchio e il nuovo millennio, conteneva non solo la banca dati per la gestione dei pagamenti ma anche altre funzionalità come la contabilità, la gestione dei dati dei clienti e il *sistema ICS* di KWC. Quest'ultimo controllava centinaia di CLP (controllori logici programmabili) che gestivano le valvole e i sensori dell'approvvigionamento idrico. Poiché il sistema era collegato direttamente a Internet, i dati di accesso rubati hanno consentito di accedere direttamente ai CLP e di manipolare l'aggiunta di varie sostanze chimiche all'approvvigionamento pubblico di acqua potabile. Dall'indagine è emerso che il management di KWC era stato informato che nei 60 giorni precedenti si erano verificati eventi inspiegabili a valvole e condutture. In particolare, si era verificata un'aggiunta incontrollata di sostanze chimiche nel trattamento dell'acqua potabile. Grazie al monitoraggio della qualità dell'acqua indipendente dal sistema era stato però possibile, mediante interventi manuali, scongiurare un pericolo per i clienti della centrale idrica.

In questa fase, gli incidenti non erano stati riconosciuti come cyber-attacchi. Solo dall'indagine successiva si è giunti alla conclusione che gli hacker non fossero in possesso di informazioni dettagliate sull'impianto e per questo i danni arrecati sono stati contenuti. Con più tempo e informazioni, l'attacco avrebbe potuto avere un epilogo decisamente più critico.

[35] http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf (in inglese; stato: 31 agosto 2016)

5.3.3 Rinvenuto un nuovo tipo di malware chiaramente focalizzato sugli ICS ma con obiettivo

FireEye, il fornitore di software di sicurezza, ha pubblicato nel mese di giugno 2016 un rapporto di analisi sul *malware ICS* «IronGate»[36]. Scoperto da FireEye lo scorso semestre, il malware ha evidenziato da subito funzioni degne di nota sotto svariati aspetti. Ad esempio, attraverso un attacco *man-in-the-middle*, è in grado di registrare per cinque secondi le informazioni inviate dal controllore logico programmabile (CLP) all'interfaccia utente. Queste ultime vengono poi riprodotte in un secondo tempo. Così, mentre l'operatore vede il «normale» traffico registrato senza insospettirsi, i comandi manipolati possono essere inviati in background al CLP. A questo scopo, il malware manipola una *dynamic link library (DLL)* che funge da intermediario tra il CLP e il software per il monitoraggio. Il malware controlla anche l'esistenza di sandbox e tool di analisi nell'ambiente di esecuzione, in particolare quelli utilizzati dai ricercatori in ambito di sicurezza e dagli analisti. Per questo motivo determinati *dropper* del malware non funzionano in ambiente Cuckoo o VMware.

Il malware prende di mira il software sviluppato da Siemens «S7 PLCSIM» e, a quanto pare, attacca specificamente un determinato tipo di impianto. FireEye presume che l'obiettivo sia l'industria del biogas. Questo, perlomeno, è quanto fa supporre il ritrovamento di un file denominato biogas.exe. Il ProductCERT di Siemens ha confermato che il codice dannoso non funziona in un ambiente di controllo standard. Il malware sembra essere destinato a operare in un simulatore, lasciando presagire che si tratti di un progetto di ricerca o di un test. Presenta però un tale livello di qualità e mutevolezza nello sviluppo da indurre a parlare di una nuova generazione di Stuxnet. Autore e uso previsto di questo malware rimangono ignoti. Il malware è stato caricato su Virustotal nel 2014, il che conferma la sua esistenza almeno a partire da questa data.

5.3.4 Accordo tra governo statunitense e produttori di automobili per una collaborazione nel settore della sicurezza

Il tema della sicurezza dei mezzi di trasporto e, in particolare, delle automobili è già stato affrontato da MELANI negli ultimi due rapporti semestrali. All'inizio di quest'anno, tenuto conto di svariati fattori quali il crescente utilizzo dell'informatica nelle automobili normali e gli sviluppi nel settore delle vetture autonome, il Ministero dei trasporti statunitense ha firmato una dichiarazione d'intenti in materia di sicurezza dei veicoli con 18 rinomati produttori di automobili. Accanto a dichiarazioni di carattere generale sulla considerazione preventiva dei rischi legati alla sicurezza, sullo scambio reciproco di informazioni e sulla collaborazione finalizzata a una maggiore sicurezza nel traffico stradale, un punto del documento fa esplicitamente riferimento al miglioramento della cybersicurezza dei veicoli. L'attenzione è però focalizzata principalmente sull'incolumità fisica delle persone (*safety*), mentre la sicurezza dei sistemi (*security*) viene trattata a titolo sussidiario quale potenziale causa di rischi per la sicurezza delle persone.

[36] https://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html (in inglese; stato: 31 agosto 2016)

Conclusione:

Nelle automobili vengono integrati sempre più servizi di assistenza computerizzati. La fiducia degli utenti nel corretto funzionamento di questi sistemi è però fondamentale. Il concetto appare subito più chiaro se rapportato alle vetture autonome: per poter essere un giorno generalmente accettate sulle strade, tutti gli utenti del traffico dovranno prima riporre in loro una grande fiducia.

5.3.5 Furto di automobili con l'ausilio dell'elettronica

La sicurezza delle persone (*safety*) è un aspetto che i produttori di automobili prendono molto sul serio (cfr. capitolo 5.3.4). Il settore è tendenzialmente regolamentato. Le case costruttrici devono mettere in conto azioni per il risarcimento dei danni e organizzare all'occorrenza dispendiose campagne di richiamo se vengono forniti prodotti difettosi che causano danni o mettono a repentaglio la vita delle persone. Le auto, però, sono anche dotate di sistemi che non hanno nulla a che vedere con la guida in senso stretto: le chiavi attualmente usate sono sostituite, ad esempio, da radiochiavi o, addirittura, gli sportelli si aprono con un'*app* del cellulare. In molte nuove vetture è persino scomparsa la serratura e, in questi casi, l'apertura e la chiusura è demandata esclusivamente all'elettronica.

In questa evoluzione, alcuni produttori sembrano però dare priorità alla funzionalità o alla velocità d'introduzione sul mercato a scapito della sicurezza (*security*): inizialmente, alcune radioserrature erano talmente rudimentali che un ladro d'auto doveva limitarsi a intercettarne e registrare il segnale. La sola riproduzione del segnale registrato consentiva al malintenzionato di aprire la portiera del veicolo. In seguito, con l'avvento sul mercato di prodotti che bloccavano automaticamente la vettura nel momento in cui qualcuno si avvicinava, i ladri si accorsero ben presto che la presenza della chiave poteva essere simulata con apparecchi radio appositamente predisposti. Era sufficiente che un complice si avvicinasse al proprietario e trasmettesse via radio il segnale in uscita dalla «chiave» al ladro vero e proprio che si trovava accanto all'automobile (attacchi a relè o *relay station attack*). Ma i «guai» non finiscono qui. In molti casi infatti, questi sistemi consentono anche di avviare il motore premendo semplicemente un pulsante quando il segnale radio della chiave viene riconosciuto all'interno della macchina. Spesso è difficile o addirittura impossibile risalire al metodo con cui è stata rubata la vettura. Così ci si limita a denunciare il furto e a comunicarlo all'assicurazione. Finché le assicurazioni risarciranno il danno, le case automobilistiche non sentiranno particolare urgenza di equipaggiare i propri prodotti con sistemi di chiusura il più possibile sicuri.

L'informatizzazione nel settore automobilistico non cela solo il pericolo che le vetture possano essere prese di mira e rubate dagli hacker. Se il cellulare diventa l'interfaccia tra il veicolo e il conducente, infiltrandosi nel telefonino o approfittando in altro modo di questa interfaccia, si possono compiere anche delle sciocchezze. Un classico esempio è fornito dall'auto elettrica «Nissan Leaf»: con l'apposita app e il numero di telaio (visibile nel finestrino frontale della vettura) era possibile acquisire i dati e azionare il climatizzatore. L'app non consentiva di accedere all'elettronica del veicolo. Tuttavia, attivando il climatizzatore, faceva lentamente e inesorabilmente scaricare la batteria del veicolo.

Conclusione / raccomandazione:

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

DOCU

Lista di controllo delle misure di protezione dei sistemi industriali di controllo:

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

5.4 Attacchi

5.4.1 Cyber-rapinatori di banche rubano 81 milioni di dollari americani

Secondo quanto affermato dalla Banca centrale del Bangladesh, gli hacker avrebbero rubato i dati di accesso al sistema di pagamento interno[37]. Gli autori dell'attacco sono penetrati nei sistemi della Banca centrale del Bangladesh e hanno installato speciali software tool appositamente programmati. Gli hacker hanno poi manipolato la banca dati, ad esempio le interfacce con il client software della Swift che gestisce le operazioni di pagamento internazionali. Durante l'attacco non solo hanno attivato transazioni contraffatte, ma anche cancellato le tracce nei protocolli. Inoltre, hanno bloccato la stampa delle conferme delle transazioni in modo che le operazioni rimanessero nell'ombra il più a lungo possibile. Il 4 e 5 febbraio 2016 i criminali hanno abusato del sistema per creare decine di ordini destinati alla Federal Reserve Bank di New York; l'obiettivo era spostare somme ingenti di denaro dal conto della Banca centrale del Bangladesh a conti nelle Filippine e nello Sri Lanka. Quattro di questi ordini per un importo di 81 milioni di dollari americani e con destinazione Filippine sono stati trasferiti con successo. Alla quinta transazione per un importo di altri 20 milioni di dollari americani, la banca di routing che fungeva da intermediaria ha però notato un errore di ortografia. Gli hacker avevano sbagliato a scrivere il nome di un'organizzazione non governativa dello Sri Lanka, inducendo la banca di routing a chiedere maggiori informazioni alla Banca centrale del Bangladesh che ha provveduto immediatamente a bloccare la transazione. Nel contempo, la Federal Reserve Bank of New York si è accorta di un numero insolitamente elevato di ordini di pagamento a favore di beneficiari privati. Allertata, la Banca centrale del Bangladesh è riuscita anche in questo caso a stornare le transazioni contraffatte evitando una perdita che si sarebbe aggirata intorno agli 850 milioni di dollari americani. Le quattro transazioni andate a buon fine sono state scambiate con fiche presso alcuni casinò filippini, dove però si sono perse le tracce del denaro, dato che nel settore delle case da gioco la vigilanza è meno stretta rispetto al sistema finanziario classico.

[37] http://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv-idUSKCN0XM0DR (in inglese; stato: 31 agosto 2016)

Per quella che fino a oggi è considerata la più grande cyber-truffa ai danni di un'unica banca, i responsabili delle autorità di perseguimento penale del Bangladesh hanno accusato la Swift di negligenza. A loro avviso infatti, sarebbe rientrato nelle competenze della Swift controllare l'intero sistema della banca, dopo l'installazione del circuito, per individuare eventuali falle. Dal canto suo, la Swift ha respinto immediatamente qualsiasi responsabilità in relazione all'attacco. Spetta infatti alla Banca centrale del Bangladesh, come d'altronde a tutti gli altri clienti, garantire la sicurezza degli ambienti e dei sistemi interfacciati con il sistema Swift. Questo episodio fa ricordare i dibattiti seguiti ai primi casi di truffe con malware nel settore dell'e-banking: fino a che punto una banca è chiamata a rispondere di un pagamento fraudolento e in quale misura il cliente ha violato l'obbligo di diligenza se il suo computer è infettato da un malware? Allora le banche reagirono aumentando la sicurezza dei sistemi di e-banking. Nel frattempo, anche la Swift ha adottato delle contromisure puntando su un maggiore rigore nel rispetto delle norme di sicurezza[38].

Il 12 maggio 2016 è stato scoperto un altro incidente ai danni di una banca commerciale in Vietnam. In questo caso pare sia stata avviata una transazione fraudolenta per 1,13 milioni di dollari americani attraverso la rete Swift utilizzata per le transazioni standard. In un terzo caso sarebbe stata invece presa di mira una banca ecuadoriana.

Nel rapporto di fornitore di servizi di sicurezza Symantec[39] si menziona il fatto che la componente del malware che cancella le tracce (*componente wipe*) era già stata utilizzata nell'«Operazione Blockbuster». «Blockbuster» è il gruppo responsabile dell'attacco sferrato alla Sony nel novembre 2014. Nel caso verificatosi in Vietnam sono state rinvenute funzioni identiche a questa componente; in Bangladesh, invece, le funzioni apparivano modificate. Non è chiaro se dietro gli attacchi ai sistemi bancari si nascondano gli stessi hacker o se il codice di programmazione sia stato venduto o condiviso tra i cybercriminali.

Conclusione:

Gli attacchi ai clienti dell'e-banking rientrano ormai da anni nel repertorio standard dei cybercriminali. Non più di un anno e mezzo fa, quando con il malware Carbanak sono stati sferrati anche attacchi diretti alle reti delle banche, è emerso chiaramente come per le rapine elettroniche ai danni delle banche venissero profusi sforzi analoghi al settore dello spionaggio avanzato, purché le prospettive di guadagno fossero adeguate. Una valutazione dettagliata di questa tendenza è riportata al capitolo 6.1.

5.4.2 Carbanak 2.0 e attacchi analoghi

Due anni fa, un attacco denominato «Carbanak» ha destato grande preoccupazione nel mondo della finanza internazionale. Per la prima volta, i cybertruffatori non avevano preso di mira un cliente finale ma direttamente la banca. I tool utilizzati, la professionalità e la caparbietà degli attacchi presentavano analogie ai cosiddetti *advanced persistent threats (APT)*. I criminali erano mossi da una logica relativamente semplice: a fronte di uno sforzo maggiore

[38] http://www.theregister.co.uk/2016/06/03/swift_threatens_insecure_bank_suspensions/ (in inglese; stato: 31 agosto 2016)

[39] http://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks (in inglese; stato: 31 agosto 2016)

era possibile realizzare un guadagno decisamente superiore. Dopo questa azione, il gruppo è rimasto tranquillo per alcuni mesi. Già nel mese di settembre 2015, però, si sono intravisti segnali di ripresa dell'attività con una vittima[40] e nel mese di febbraio 2016 l'azienda di software Kaspersky ha confermato il ritorno di «Carbanak 2.0». In un altro articolo un team di ricercatori di Proofpoint, un'azienda del settore della sicurezza informatica, asseriva di avere scoperto i preparativi della banda di Carbanak in vista di attacchi a banche in Europa, Medio Oriente e USA[41].

Una caratteristica di «Carbanak 2.0» è che il gruppo non prende di mira solo le banche, ma estende la cerchia delle proprie vittime anche ai reparti contabilità di altre aziende. In un caso gli hacker hanno modificato i rapporti di proprietà di una grande azienda. Un prestanome è stato fatto passare illegalmente per azionista della società. Non è dato sapere quali fossero le reali intenzioni degli hacker. L'incidente è stato scoperto prima che si verificassero dei danni[42].

«Carbanak», tuttavia, è solo il primo di una serie di incidenti analoghi. I cybercriminali imparano velocemente, integrano nuove tecniche nelle loro operazioni e sempre più spesso attaccano direttamente le banche. Altri due gruppi, chiamati «Metel» e «GCMAN», agiscono ad esempio in base allo stesso schema. Il gruppo «Metel» opera in modo simile al gruppo «Carbanak». Nei casi osservati finora, i criminali hanno svuotato nottetempo i bancomat di varie banche di città russe. L'altra parte del gruppo criminale ha manipolato i conti piratati facendo in modo che il saldo fosse riportato all'importo antecedente al prelievo. «GCMAN», invece, esegue transazioni da 200 dollari americani a intervalli di un minuto su *servizi di e-currency* come BitCoin, Perfect Money o Payza. L'aspetto peculiare di «GCMAN» è che gli hacker si sono mossi inosservati nella rete per 18 mesi.

5.4.3 Ransomware negli ospedali

L'ondata di ransomware osservata a partire dall'inizio dell'anno colpisce anche infrastrutture critiche. Obiettivi prediletti dei ricattatori sono, in questi ultimi tempi, gli ospedali. Con la digitalizzazione, il funzionamento del servizio informatico di un ospedale riveste un'importanza cruciale nel trattamento dei pazienti. Casi che hanno coinvolto diversi ospedali in Germania e negli Stati Uniti sono stati pubblicati nella prima metà del 2016. In alcuni casi sono stati pagati riscatti importanti ai criminali affinché sbloccassero l'infrastruttura. Nel caso del Kansas Heart Hospital, i criminali non hanno sbloccato tutti i file e hanno richiesto il pagamento di un secondo riscatto. Gli ospedali sembrano essere diventati la categoria di obiettivi con le richieste di riscatti più elevate. I truffatori sanno che un ospedale deve reagire rapidamente e in certi casi non può più fare a meno dell'infrastruttura informatica per salvare una vita umana. Queste istituzioni possono perciò diventare obiettivi prediletti.

Un'ulteriore sfida con la quale gli ospedali si devono confrontare è la presenza di apparecchiature informatizzate per le diagnosi e le analisi. Questi strumenti sono testati e certificati per poter essere utilizzati in campo medico. Tuttavia, nella maggior parte dei casi il sigillo di approvazione non permette ai servizi informatici di un ospedale di aggiornare il sistema operativo e il software antivirus, poiché questi interventi risulterebbero come manipolazioni delle

---

40 https://www.csis.dk/en/csis/blog/4710/ (in inglese; stato: 31 agosto 2016)

41 https://www.proofpoint.com/uk/threat-insight/post/carbanak-cybercrime-group-targets-executives-of-financial-organizations-in-middle-east (in inglese; stato: 31 agosto 2016)

42 https://securelist.com/blog/research/73638/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/ (in inglese; stato: 31 agosto 2016)

apparecchiature con la conseguente perdita della loro certificazione. Inoltre, i servizi informatici degli ospedali sono privi degli strumenti e della competenza tecnica per aggiornare questi sistemi specifici.

In passato, questi sistemi potevano essere indipendenti dalla rete informatica di un ospedale. Purtroppo, con il collegamento in rete delle macchine per il controllo digitale dei dati dei pazienti, le reti informatiche ospedaliere includono sempre più spesso sistemi vulnerabili la cui sicurezza non é garantita. Per questo motivo, è fondamentale fare un sforzo di sensibilizzazione e di collaborazione con i fornitori di materiale.

In definitiva, la digitalizzazione dei dati dei pazienti può essere utile anche ai truffatori. La cartella di un determinato paziente può diventare un obiettivo a fini di spionaggio o di sabotaggio. I dati relativi alle terapie, i risultati e le fisiologie forniscono un aiuto prezioso per sviluppare terapie con la cosiddetta analisi dei «big data» e sono molto promettenti nella ricerca di nuove terapie. Tuttavia, questi dati possono essere molto ambìti da individui e aziende che potrebbero servirsene per scopi illeciti. Occorre perciò interrogarsi su cosa inserire nei dossier dei pazienti visti i rischi che comporta la loro digitalizzazione e il modo in cui si minimizzano questi ultimi. Inoltre, si deve anche predisporre la procedura per comunicare ai pazienti la perdita dei loro dati sensibili.

5.4.4 Saccheggiati bancomat in Giappone

Tra le 5 e le 8 della mattina di domenica, 15 maggio 2016 circa 1700 bancomat giapponesi sono stati «alleggeriti» di una cifra pari a quasi 17 milioni di franchi nell'ambito di un'azione su vasta scala e ben coordinata. Per poter eseguire gli oltre 14 000 prelievi in così breve tempo, sono state utilizzate fino a 1600 carte di credito contraffatte da parte di 600 persone circa. Sulla banda magnetica delle carte falsificate erano memorizzati i dati rubati di clienti della South African Standard Bank.

In passato, le carte di credito straniere non erano praticamente accettate nei bancomat giapponesi. Tempo fa, per agevolare i prelievi di denaro dei turisti stranieri, il governo ha invitato le banche a intervenire per modificare questa situazione. A quanto pare, però, numerosi bancomat non sono ancora abilitati a leggere il chip presente sulle carte di credito e utilizzano tuttora la banda magnetica che può essere copiata facilmente. Questi incidenti hanno inoltre dimostrato come molto debba essere ancora fatto sul fronte del rilevamento dei prelievi fraudolenti con carte di credito straniere.

La straordinaria entità del danno potrebbe spiegarsi con il limite di prelievo che all'epoca dei fatti ammontava in molti bancomat a 100 000 o 200 000 yen (pari rispettivamente a fr. 900.- e fr. 1800.- circa). Come reazione, i limiti sono stati ridotti a un massimo di 50 000 yen.

5.4.5 Anonymous & Co: #campagne

Il primo semestre del 2016 è stato caratterizzato da numerose attività, in alcuni casi prolungate, degli hacktivist contro le organizzazioni da loro ritenute centri del potere.

Già all'inizio dell'anno, il collettivo di Anonymous aveva esortato «a impugnare le armi». Si stava pianificando un nuovo attacco contro il sistema finanziario globale dal nome mitologico «Operazione Icaro». «Come Icaro, i potenti hanno volato troppo vicino al sole ed è giunto il

momento di appiccare fuoco alle ali dell'impero...» [43]. L'operazione, già prevista nel 2011 ai tempi di Occupy Wallstreet, avrebbe dovuto fare da eco online alle proteste sul campo[44]. Il 4 maggio 2016 è stata annunciata con un video su YouTube una «30-day campaign against central bank sites across the world» (una campagna della durata di 30 giorni contro le sedi delle banche centrali in tutto il mondo). Il giorno stesso, Anonymous − coadiuvato dal gruppo di hacker «Ghost Squad» − ha sommerso di richieste via Web il sito Internet della banca centrale greca rendendo irraggiungibile il suo server per parecchie ore. Per tutto il mese di maggio la campagna #OpIcarus ha paralizzato, tra gli altri, i siti Web di oltre 30 banche centrali. Le vittime più illustri sono state la Bank of England, la Borsa di New York e la Banca vaticana. Gli attacchi sono stati sferrati con una potenza di ben 250 Gbps[45]. Anonymous ha pubblicato l'elenco completo degli obiettivi (oltre 200 siti Web) e ha proclamato su Twitter che l'operazione non era ancora terminata.

Un'operazione analoga, «#OpSilence», era stata annunciata per il mese di giugno dal gruppo di hacker Ghost Squad, ex sottogruppo di Anonymous[46]. Obiettivo era punire i media che non avevano fornito informazioni, o lo avevano fatto solo unilateralmente, sulla guerra in Palestina o sugli effettivi crimini commessi in Siria[47]. Tuttavia, «Ghost Squad»[48] non si è attenuto ai tempi indicati e ha sferrato l'attacco già il 31 maggio mettendo fuori uso per parecchie ore i sistemi di posta elettronica dei canali d'informazione CNN e FOX News. Gli hacker hanno annunciato inoltre altri attacchi contro i media per tutto il mese di giugno, indicando quali possibili obiettivi la NBC e la MSN. Queste minacce, tuttavia, non hanno avuto seguito. Infine, si deve segnalare un interessante aspetto secondario: Ghost Squad si è premurato di puntualizzare che si sarebbe trattato di un'operazione autonoma e che il gruppo non aveva (più) nulla a che vedere con Anonymous.

Conclusione:

La connessione non particolarmente stretta tra Anonymous e gruppi simili come Ghost Squad è sfociata in una serie di annunci e attacchi non coordinati, più o meno spettacolari. Poiché per motivi inerenti alla sua struttura non esiste adesione come membro ad Anonymous, né sono presenti un portavoce ufficiale e persone responsabili dell'intero movimento, ognuno può in linea di massima eseguire attacchi o pubblicare comunicazioni a nome del gruppo.

---

43 https://opicarus.wordpress.com/ (in inglese; stato: 31 agosto 2016)

44 http://www.ibtimes.co.uk/opicarus-anonymous-hacker-reveals-inspiration-behind-latest-operation-evolution-hacktivism-1561457 (in inglese; stato: 31 agosto 2016)

45 http://thefreethoughtproject.com/anonymous-hits-york-stock-exchange-world-bank-vatican-total-corporate-media-blackout-ensues/ (in inglese; stato: 31 agosto 2016)

46 http://thefreethoughtproject.com/not-anonymous-hacking-group-declares-war-mainstream-takes-cnn-fox/ http://anonhq.com/anonymous-opsilence/ (in inglese; stato: 31 agosto 2016)

47 http://news.softpedia.com/news/anonymous-announces-opsilence-month-long-attacks-on-mainstream-media-504760.shtml (in inglese; stato: 31 agosto 2016)

48 http://thefreethoughtproject.com/not-anonymous-hacking-group-declares-war-mainstream-takes-cnn-fox/ (in inglese; stato: 31 agosto 2016)

5.4.6 XDEDIC: l'accesso ai server piratati è in vendita on line

Nel mese di giugno, Kaspersky ha pubblicato i dettagli di un'inchiesta effettuata con un fornitore di servizi Internet europeo su un mercato underground denominato xDedic, attivo dal 2014, che proponeva di acquistare i dati d'accesso a circa 70 000 server piratati, accessibili tramite il *protocollo RDP («Remote Desktop Protocol»*, che permette di teleconnettersi a un server Windows). Il prezzo variava in base alla specificità del server, a partire da 6 dollari americani. Tali server possono essere utilizzati per sferrare attacchi (*DDoS, spam* ecc.), ma possono anche essere sfruttati per i dati o i sofware che contengono. Alcuni server particolarmente interessanti permettono, ad esempio, di accedere a *terminali di pagamento*. Poco dopo le rivelazioni di Kaspersky, il sito è scomparso e riapparso dopo breve tempo, ospitato questa volta dalla *rete TOR*.

Conclusione:

Questo caso rappresenta la tendenza verso una divisione del lavoro sempre più spinta nell'underground cybercriminale. Gli attori meno avanzati possono ricorrere a una gamma di servizi per sferrare attacchi con un investimento minimo di tempo e di competenze tecniche. Inoltre, dopo essere stato pubblicato da Kaspersky il sito è scomparso per riapparire su una piattaforma più anonima per amministratori,venditori e acquirenti. Ciò dimostra che, quando un mercato è redditizio, i suoi operatori ne adatteranno la forma affinché si perpetui.

5.5 Misure di prevenzione

La misura di prevenzione più efficace, oltre alla sensibilizzazione, è la cattura dei cybercriminali. Secondo un'opinione diffusa, gli arresti in ambito informatico sono difficili o addirittura impossibili da mettere a segno. Diverse retate dimostrano però come si possano riportare dei successi anche in questo settore.

5.5.1 Retata nella darknet

In occasione di una retata internazionale contro i gestori e gli utenti di piattaforme Web illegali sono stati fermati nove sospetti e perquisiti 69 appartamenti e aziende in Germania, Svizzera, Francia, Paesi Bassi, Lituania e Russia. Nove sono le persone gravemente indiziate per avere commesso i fatti. Le indagini hanno coinvolto vari forum di lingua tedesca della *underground economy* in cui si commerciavano merci illegali come armi, stupefacenti, denaro falso, documenti ufficiali contraffatti e informazioni violate come dati di carte di credito e di online banking. La gamma dell'offerta annoverava anche servizi criminali, ad esempio attacchi *DDoS* o l'infezione di computer con *malware*.

Il presunto gestore principale di complessivamente tre forum è un cittadino bosniaco di 27 anni. L'imputato è stato fermato il 24 febbraio 2016 in Bosnia-Erzegovina e si trova in custodia preventiva.

È stato possibile mettere al sicuro parecchio materiale probatorio, in particolare numerosi computer e supporti di memorizzazione, un'arma da fuoco, stupefacenti e valori patrimoniali per un controvalore di circa 150 000 euro. Sono stati inoltre sequestrati parecchi server in

Francia, Paesi Bassi, Lituania e Russia su cui venivano gestiti siti di commercio elettronico criminali. Sui siti Web interessati è stato attivato un avviso con cui si comunicava l'avvenuto sequestro dei server.[49]

Figura 10: Banner caricato dalla polizia sui server Web sequestrati.

Conclusione:

L'azione in oggetto fornisce l'ennesima dimostrazione di come non esista l'anonimato totale in Internet. Sottolinea inoltre l'importanza della collaborazione internazionale nella lotta alla criminalità informatica.

5.5.2 Scomparsa l'attività degli exploit kit «Angler» e «Nuclear»

Nel primo semestre del 2016 i due *exploit kit* di gran lunga più famosi sono quasi spariti dalla circolazione. Diversi sono però i motivi all'origine della loro scomparsa. Per quanto riguarda «Nuclear», deve avere giocato un ruolo fondamentale l'analisi divulgata nel mese di aprile 2016 da Check Point, un'azienda specializzata in prodotti relativi alla sicurezza. La dovizia di dettagli delle informazioni rivelate deve avere spaventato i gestori al punto tale da eclissarsi e sospendere, almeno temporaneamente, l'attività. L'esperto di exploit kit francese «Kafeine» non ha più rilevato attacchi di «Nuclear» dal 30 aprile.[50]

L'exploit «Angler», in base a quanto riportato da Kafeine, è totalmente scomparso dal 7 giugno. Anche in questo caso ci si chiede quale sia la causa della sua improvvisa scomparsa. Una spiegazione potrebbe essere l'arresto, eseguito proprio in quel periodo dalle autorità russe, di 50 presunti cybercriminali collegati al malware «Lurk». Pare che le persone catturate avessero utilizzato un trojan per rubare soldi da conti bancari russi. In questi attacchi, il vettore d'infezione era direttamente correlato all'exploit kit «Angler». Resta il dubbio se alcuni

49 https://www.bka.de/SharedDocs/Pressemitteilungen/DE/Presse_2016/pm160229_UndergroundEconomy.pdf?__blob=publicationFile&v=1 (in tedesco; stato: 31 agosto 2016)

50 http://www.securityweek.com/exploit-kit-activity-down-96-april (stato: 31 agosto 2016)

degli autori dell'exploit kit «Angler» siano stati effettivamente arrestati o siano stati semplicemente colti dal panico per timore che le persone prese potessero rivelare il nome di altri criminali. Chi però sperava che l'utilizzo degli exploit kit tra i criminali potesse diminuire in seguito all'uscita di scena di «Angler» è rimasto purtroppo deluso. A cambiare è solo il kit utilizzato, tant'è che dopo la fine di «Angler» si è assistito a una notevole espansione dell'exploit kit «Neutrino».

5.5.3 Parecchi arresti in vari Paesi tra i sostenitori di «Dyre»

In febbraio, la rivista Forbes[51] annunciava che nel novembre 2015 le autorità russe avevano bloccato la *botnet* del trojan di e-banking Dyre e fermato i dirigenti dell'organizzazione criminale. Secondo la IBM il trojan di e-banking più attivo del 2015, responsabile di circa un quarto dei casi di frode bancaria nel mondo, si era diffuso a dismisura anche in Svizzera. Inizialmente, il trojan prendeva di mira soprattutto le PMI. I truffatori erano così riusciti ad «alleggerire» un'azienda del Cantone di Friburgo di un importo a sette cifre[52]. Nel frattempo, però, «Dyre» ha colpito anche gli utenti privati. Sebbene la retata, ordinata probabilmente dal governo russo, non sia stata confermata, le attività di «Dyre» sono cessate come dimostra chiaramente la statistica sui malware del sito GovCERT.ch. Ormai restano solo le infezioni dei sistemi mai ripristinati. Secondo Forbes, però, il malware «Dyre» non può ancora considerarsi sconfitto; da poco, infatti, il *codice sorgente* è liberamente disponibile su Internet.

6 Tendenze e prospettive

6.1 Attacchi sofisticati – APT anche in ambienti criminali

Sempre più spesso i criminali intraprendono sforzi maggiori a fronte di guadagni superiori, adottano modalità operative più mirate e cercano di ottimizzare costi e benefici. Oltre agli attacchi d'inizio anno ai danni del sistema telematico interbancario Swift (capitolo 5.4.1) e agli incidenti imputabili a «Carbanak» (capitolo 5.4.2) si registra una rapida progressione degli attacchi sferrati contro i clienti finali. Tale tendenza è favorita da una ripartizione dei compiti e dal riciclaggio del malware nel mercato underground digitale.

Per le truffe, a lungo è valso il principio del minimo sforzo. Il bersaglio più ambito era dunque il sistema meno protetto. Questi «*low hanging fruits*» (ossia obiettivi più facili da conseguire) erano rappresentati soprattutto dai computer di utenti finali con cui si effettuavano, ad esempio, operazioni di e-banking. Fino a qualche anno fa, gli attacchi diretti a istituti finanziari venivano visti come una prerogativa esclusiva di cinema o televisione. Allora, infatti, l'impegno e la professionalità richiesti erano considerati eccessivi. Oggi, le cose sono cambiate e la tendenza verso cyber-rapine spettacolari non stupisce. Svariati sono i motivi all'origine di questa tendenza:

- Innanzitutto, il software necessario per sferrare attacchi così complessi nel frattempo è diventato reperibile nel mercato underground e anche i criminali hanno acquisito il

[51] http://www.forbes.com/sites/thomasbrewster/2016/02/08/russia-arrests-dyre-malware-masterminds/#5d5cf29a1e02 (in inglese; stato: 31 agosto 2016)

[52] http://www.20min.ch/digital/news/story/E-Banking-Trojaner-zielt-auf-Schweizer-Firmen-ab-23497999 (in tedesco; stato: 31 agosto 2016)

know-how. Tale circostanza viene peraltro favorita dalla linea di demarcazione sempre più labile tra gli attacchi sferrati dai criminali e quelli sponsorizzati dagli Stati.

- Un altro aspetto importante riguarda la crescente difficoltà nel riciclare il denaro. Trovare persone abbastanza sprovvedute da farsi reclutare come money mule (i cosiddetti agenti finanziari) è fortunatamente divenuta una missione assai ardua. A complicare ulteriormente la vita dei criminali contribuisce il fatto che, normalmente, un agente finanziario può essere già tolto di mezzo dopo un unico tentativo. I delinquenti sono dunque alla ricerca di alternative che facciano a meno dei money mule o consentano di impiegarli in modo efficiente. Il metodo più semplice per riciclare denaro con maggiore efficienza è trasferire somme più consistenti attraverso i money mule. Nel mirino dei criminali sono così finite soprattutto le aziende, dato che queste ultime possono spostare somme più ingenti dando meno nell'occhio.

I casi descritti nei capitoli 5.4.1 e 5.4.2 dimostrano a titolo esemplificativo come si stiano cercando nuove vie, che purtroppo vengono anche trovate, per cancellare le tracce dei flussi di denaro. Basti pensare al gruppo legato al malware «Carbanak» e «Metel» che ha manipolato i bancomat arrivando a un certo punto a farli emettere denaro senza doversi nemmeno preoccupare di riciclarlo dato che il «versamento» avveniva in contanti. Nel caso del gruppo «GCMAN» si utilizzavano invece monete elettroniche, un'altra soluzione che rende più difficile tracciare i flussi di denaro. Nella cyber-rapina contro la Banca centrale del Bangladesh il denaro delle quattro transazioni andate a buon fine è stato scambiato con fiche di casinò filippini, dove però si sono perse le tracce, poiché nel settore delle case da gioco la vigilanza è meno stretta rispetto al sistema finanziario classico. Nell'insieme si può affermare che i maggiori guadagni realizzati dai criminali consentono di mettere in campo anche tecniche di riciclaggio più laboriose e professionali.

Chi crede però che gli attacchi professionali arriveranno a scalzare le azioni più semplici si sbaglia. L'esperienza dimostra infatti che le vecchie forme di attacco non si estinguono, ma cambiano semplicemente paternità. Basti pensare ai tentativi di *phishing* in circolazione. Questi attacchi, pur non avendo più il successo di un tempo, continuano a essere sferrati e devono essere respinti. La torta, dunque, non solo viene ridistribuita ma nell'insieme tende anche a ingrandirsi.

6.2 Il futuro di Internet – Dal punto di vista tecnico e sociale

Le prime automobili non avevano il tetto, né una cintura di sicurezza o qualsiasi altro dispositivo che proteggesse il conducente. In pratica eravamo solo noi e la strada, felici che il veicolo andasse nella direzione desiderata. Una situazione analoga è stata vissuta agli albori di Internet, come illustrava già negli anni Ottanta l'ingegnere informatico statunitense Danny Hillis: «There were only two other Dannys on the Internet then. I knew them both. We didn't all know each other, but we all kind of trusted each other»[53] («C'erano solo due altri Danny su Internet. Li conoscevo entrambi. Non ci conoscevamo tutti, ma ci fidavamo reciprocamente» . Eravamo felici per il semplice motivo che la rete funzionava. Nel traffico stradale, con il passare del tempo e all'aumentare del numero di incidenti sono state introdotte regole per la circolazione, costruite strade sicure ed emanate norme che impongono di equipaggiare le automobili di cinture di sicurezza, zone deformabili per assorbire gli urti, ABS ed airbag. In

[53] https://www.ted.com/talks/danny_hillis_the_internet_could_crash_we_need_a_plan_b/transcript (stato: 31 agosto 2016)

Internet, invece, l'architettura originaria è rimasta in gran parte immutata e non sono state stabilite regole vincolanti per il traffico in rete. La sicurezza è stata demandata agli utenti e ai servizi che utilizzano Internet. Per restare alla nostra analogia, è come se l'automobilista dovesse semplicemente indossare un casco sempre più grande, anche questo però su base volontaria.

Fisicamente, Internet è costituita da 60 000 reti singole – i cosiddetti *sistemi autonomi (AS)*. Questi ultimi vengono gestiti soprattutto da grossi operatori di telecomunicazioni, ma anche le organizzazioni pubbliche e private più o meno grandi hanno i propri AS. All'interno di un singolo AS il gestore ha il controllo sulla rete; oltre i limiti dell'AS si segue invece un regolamento comune, il *Border Gateway Protocol (BGP)*. Il BGP è stato sviluppato negli anni Ottanta per far interagire le poche reti di allora e, ancora oggi, regolamenta i percorsi che prendono i nostri pacchetti dati nella rete globale. Tutto ciò espone la dorsale a errori rendendola facile da influenzare. Qualcuno ha anche già approfittato di questa vulnerabilità, come dimostra la raccolta di documenti di Snowden.

Un'alternativa potrebbe giungere dalla creazione ex novo di una nuova Internet. Esisterebbero anche ipotesi al riguardo. Il progetto SCION del Politecnico federale di Zurigo propone ad esempio un'architettura dall'approccio snello che permetterebbe di controllare i percorsi, isolare gli errori e praticare una comunicazione end-to-end basata sulla fiducia. Tuttavia, ci vorrà ancora del tempo prima che tale approccio possa affermarsi tra i 60 000 gestori di AS. Così, anziché preparare la struttura di base per il futuro, continueremo a romperci il capo con nuove applicazioni che offrono funzionalità sempre nuove su basi obsolete. E le prime pagine dei giornali saranno dominate da *big data* e *blockchain*. Se ciò porterà a un rinnovamento dell'«anima» attuale di Internet o alla nascita di una nuova struttura parallela, sarà il futuro a dirlo.

Chi vuole far parte della rete deve mettere necessariamente in conto gli svantaggi. Però, nel momento in cui l'utente finale ha ben presenti le inadeguatezze di Internet, acquisisce anche maggiore consapevolezza di dover provvedere personalmente alla tutela della propria sicurezza e sfera privata. Ecco perché trovano sempre più spazio tool di anonimizzazione come *TOR Browser*, mentre le pubblicazioni di Edward Snowden hanno portato all'affermazione della crittografia end-to-end. L'esempio più lampante giunge dall'integrazione del protocollo Signal[54] nel popolare servizio di messaggistica breve Whatsapp, che ha aperto all'utilizzo di massa un software speciale precedentemente considerato di nicchia.

In ultima analisi, però, la gestione dei rischi rientra nella sfera delle responsabilità di ciascun individuo, ciascuna organizzazione, ciascuna impresa. Domande del tipo: quali dati ho salvato e dove li ho messi, chi può avervi accesso, come vengono utilizzati e a chi procurano vantaggi finanziari assumono in questo senso un'importanza sempre maggiore. Internet è ormai costantemente esposta al fuoco incrociato di innovazione, sfera privata, sicurezza dei dati e anche certezza del diritto. L'inarrestabilità dell'innovazione, inoltre, non permette agli utenti di crogiolarsi nelle risposte di un tempo. Ciascuno di noi deve continuamente affrontare questioni nuove che esigono risposte nuove. Anonimità e sfera privata sono sempre più difficili da affermare. Questa evoluzione è illustrata chiaramente dal servizio russo «Find Face»: con una sola foto che ritrae una persona è possibile trovare il suo account nella rete sociale VK.com. Questa app è momentaneamente disponibile solo in lingua russa e l'accesso è limi-

[54] Moderno protocollo open source caratterizzato da una forte crittografia che è stato sviluppato per sistemi di messaggistica asincroni.

tato a VK.com. Ma è solo una questione di tempo e il riconoscimento facciale si diffonderà in tutto il mondo sotto forma di app: basterà una foto per identificare una persona e trovare in Internet tutte le informazioni sul suo conto. L'anonimità in pubblico è ormai storia passata. Il progresso in Internet metterà duramente alla prova il diritto alla sfera privata.

La società deve trovare delle risposte e, magari, un giorno definire addirittura dei limiti. L'evoluzione di Internet ma anche lo sviluppo e il cambiamento delle norme sociali sono un fenomeno tutt'altro che concluso. Ci attendono fasi interessanti nell'evoluzione di Internet, sia dal punto di vista tecnico e sociale sia giuridico e politico.

7 Politica, ricerca, policy

7.1 Svizzera: interventi parlamentari

Affare	N.	Titolo	Depositato da	Depositato il	CN/ CS	Dip.	Stato delle deliberazioni e link
Ip.	16.3606	Chi si occupa della cybersicurezza in Svizzera?	Derder Fathi	17.06.2016	CN	DDPS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163606
Ip.	16.3561	Dichiarazione della NATO. Gli attacchi da parte di hacker possono provocare un «casus foederis»	Josef Dittli	17.06.2016	CS	DDPS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163561
Mo.	16.3528	Competenza per la cyberdifesa	Ida Glanzmann-Hunkeler	16.06.2016	CN	DDPS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163528
Ip.	16.3462	Garantire la sicurezza dei dati elettronici dei pazienti	Edith Graf-Litscher	15.06.2016	CN	DFI	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163462
Ip.	16.3413	Criminalità informatica e rischi per gli impianti nucleari	Bea Heim	09.06.2016	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163413
Ip.	16.3394	Collaborazione nel settore della sicurezza con il Principato del Liechtenstein	Josef Dittli	07.06.2016	CS	DDPS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163394
I	16.1024	Interpol, rischi cibernetici e cybercriminalità	Hansjörg Knecht	07.06.2016	CN	DFGP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161024
Po.	16.3382	Sicurezza di Internet degli oggetti. Promuovere lo sviluppo di competenze specifiche	Claude Béglé	06.06.2016	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163382
I	16.1022	Accertamenti concernenti il cyberattacco contro la RUAG	CVP Fraktion	02.06.2016	CN	DDPS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161022
I	16.1021	Cyberattacchi contro RUAG e DDPS. È necessario trarre le dovute conclusioni!	Grüne Fraktion	02.06.2016	CN	DDPS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161021
I	16.1020	Sistema di controllo e centro di competenza come futuri strumenti nella lotta contro i cyber-rischi	Fraktion BD	02.06.2016	CN	DDPS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161020
Ip.	16.3359	Perseguimento penale in caso di attacchi DDos (cyberattacchi). Come sostiene la Confederazione i Cantoni a corto di know-how?	Marcel Dobler	31.05.2016	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163359
Ip.	16.3356	Ridistribuire finalmente le risorse finanziarie e di personale a favore della lotta per la cybersicurezza	Sozialdemokratische Fraktion	31.05.2016	CN	DDPS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163356
Ip.	16.3353	Scopo della Rete integrata Svizzera per la sicurezza	Werner Salzmann	30.05.2016	CN	DDPS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163353
Po.	16.3348	Creazione di un consiglio per la	Claude Béglé	27.04.2016	CN	DDPS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-

		cyberdefence. Una priorità per la nostra sovranità e la nostra sicurezza					vista/geschaeft?AffairId=20163348
Mo.	16.3186	Cyber-rischi. Scambio di informazioni tecniche	Corina Eichenberger	17.03.2016	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163186
Po.	16.3058	Abbandono del collegamento telefonico analogico. Conseguenze per i telefoni negli ascensori e altri sistemi d'emergenza	Hans Egloff	08.03.2016	CN	DA-TEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163058
Ip.	16.3440	Quali sono i mezzi tecnici per allertare l'intera popolazione svizzera in caso di catastrofe?	Mathias Reynard	15.06.2016	CN	DDPS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163440
Po.	16.3381	Industria 4.0. Creare un coordinamento a livello svizzero	Claude Béglé	06.06.2016	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163381
Ip.	16.3337	Determinazione dinamica della larghezza di banda minima secondo l'ordinanza sui servizi di telecomunicazione	Martin Candinas	24.04.2016	CN	DA-TEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163337
Mo.	16.3336	Aumento della velocità Internet minima a 10 megabit per secondo nel servizio universale	Martin Candinas	27.04.2016	CN	DA-TEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163336
Po.	16.3313	Vagliare possibili misure contro i curiosi che disturbano gli interventi o ledono i diritti della personalità	Bernhard Guhl	27.04.2016	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163313
Ip.	16.3296	Wi-fi ovunque tranne che sui treni svizzeri?	Derder Fathi	26.04.2016	CN	DA-TEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163296
Ip.	16.3272	La Svizzera e la sfida della tecnofinanza	Elisabeth Schneider-Schneiter	26.04.2016	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163272
Po.	16.3245	Valutazione sulla scissione di Swisscom in una società di rete pubblica e in un'impresa di servizi privata	Balthasar Glättli	18.03.2016	CN	DA-TEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163245
Po.	16.3219	Un piano d'azione per il voto elettronico	Marco Romano	18.03.2016	CN	CaF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163219
Mo.	16.3184	Digitalizzazione e istruzione informatica. Sviluppo comune di uno spazio formativo digitale	Jonas Fricker	17.03.2016	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163184
Ip.	16.3162	Pornografia della vendetta	Yvonne Feri	17.03.2016	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163162
Mo.	16.3128	Un piano nazionale per ridurre il divario digitale	Jean Christophe Schwaab	16.03.2016	CN	DA-TEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163128
Mo.	16.3120	Salvare e rafforzare le PMI - con il buono per l'innovazione e altri	Corrado Pardini	16.03.2016	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163120

		strumenti concreti					
Po.	16.3051	Abbandono del collegamento telefonico analogico. Conseguenze per i telefoni negli ascensori e altri sistemi d'emergenza	Joachim Eder	08.03.2016	CS	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163051
Mo.	16.3007	Garantire quanto prima l'ammodernamento delle reti di telefonia mobile	Kommission für Verkehr und Fernmeldewesen NR	01.02.2016	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163007
Ip.	16.3555	Guida autonoma. Condizioni quadro e conseguenze	Susanne Leutenegger Oberholzer	17.06.2016	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163555
Mo.	16.3526	Basta ingannare i consumatori. Stop ai numeri di telefono svizzeri usati per simulare attività economiche nel nostro Paese	Jean-François Steiert	16.06.2016	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163526
Mo.	16.3452	Tariffe di roaming. Ora basta	Elisabeth Schneider-Schneiter	15.06.2016	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163452
Domanda	16.5294	Come contra di rinforzare il pilotaggio numerico in Svizzera il Consiglio Federale?	Derder Fathi	08.01.1900	CN	DATEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20165294
Ip.	16.3387	La fattura elettronica senza firma elettronica è conforme alle disposizioni concernenti l'imposta sul valore aggiunto?	Fabio Regazzi	07.06.2016	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163387
Mo.	16.3310	Droni. Proteggere la popolazione dai rischi	Susanne Leutenegger Oberholzer	27.04.2016	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163310
Po.	16.3260	Istituire una gestione del digitale	Claude Béglé	18.03.2016	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163260
Domanda	16.5056	Guidare l'auto senza autista	Susanne Leutenegger Oberholzer	02.03.2016	CN	DATEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20165056
Mo.	16.3228	La Confederazione non deve più essere azionista di maggioranza di Swisscom	Ruedi Noser	18.03.2016	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163228
Mo.	16.3484	Rafforzare la posizione dominante della Svizzera nella tecnologia blockchain	Claude Béglé	16.06.2016	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163484
	16.044	Salvaguardia del valore di Polycom. Credito complessivo	Geschäft des Bundesrates	25.05.2016	CF		https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20160044
Po.	16.3256	Promozione della digitalizzazione nell'ambito della regolamentazione (RegTech)	Martin Landolt	18.03.2016	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163256

7.2 Direttiva europea sulla sicurezza della rete e dell'informazione (Direttiva NIS)

All'inizio del mese di luglio 2016, il Parlamento dell'UE ha raggiunto un'intesa sulla prima legge europea in materia di cybersicurezza. Con la cosiddetta direttiva sulla sicurezza della rete e dell'informazione (NIS), l'UE intende rafforzare la capacità dell'Europa di resistere agli attacchi informatici. Le aziende che gestiscono servizi essenziali (ad es. nel settore dell'energia, dei trasporti, delle banche e della sanità) o i fornitori di servizi digitali (come motori di ricerca, siti di commercio elettronico o *servizi cloud*) dovranno adottare misure di sicurezza adeguate al fine di migliorare la propria resistenza ai cyber-attacchi. Inoltre dovranno essere segnalati gli hackeraggi gravi ai danni dei sistemi aziendali. Qualora tale obbligo di notifica non fosse rispettato, scatteranno delle sanzioni. Il Parlamento dell'UE è convinto che la definizione di standard comuni in materia di cybersicurezza e il rafforzamento della collaborazione aiuterà le aziende a proteggersi dal numero crescente di attacchi informatici.

La direttiva è in vigore dall'agosto 2016 e, nell'arco di 21 mesi, dovrà essere attuata nel diritto nazionale degli Stati membri. Questi ultimi, inoltre, hanno sei mesi di tempo per stabilire gli «operatori di servizi essenziali».

Per la Svizzera, l'approvazione della direttiva NIS non ha alcuna ripercussione per il momento. Resta da vedere in che misura le disposizioni della NIS e i requisiti per la partecipazione al *digital single market* potrebbero spingere il nostro Paese, seppur nell'ambito del recepimento autonomo, a riprendere ampiamente propositi come gli standard comuni in materia di cybersicurezza e l'obbligo di segnalazione. Nel settore della sicurezza delle informazioni, la Svizzera si è finora affidata con successo alla collaborazione volontaria tra Stato ed economia. Certo è che l'emanazione di decreti lontani dalla prassi del diritto penale con obblighi di notifica degli incidenti informatici richiederà lo sviluppo e il potenziamento delle capacità esistenti come pure la creazione di appositi organi di controllo.

7.3 Francia: nuove regole d'importanza cruciale per gli operatori

In Francia, i primi decreti sull'obbligo legale d'importanza cruciale per gli operatori di proteggersi da cyberattacchi sono stati pubblicati dall'Agenzia nazionale di sicurezza dei sistemi d'informazione (ANSSI) e sono entrati in vigore il 1° luglio 2016. Essi concernono dapprima le aziende dei settori dei prodotti sanitari, dell'alimentazione e della gestione idrica. Decreti specifici per altri settori seguiranno. Questa base legale fa seguito alla legge sulla programmazione militare del dicembre 2013. Le infrastrutture critiche non dovranno solo adottare misure di protezione, ma anche comunicare gli incidenti nei quali incombono. La disposizione è vincolante, infatti sono previste sanzioni per le infrastrutture che non rispettano queste regole.

La Francia si dota di un dispositivo inedito in Europa, anticipando in tal modo le misure previste dalla direttiva «Network and Information Security» (NIS) per tutti i Paesi dell'Unione europea. La NIS avrà però una portata più ampia, poiché si estenderà alle aziende non interessate dai decreti.

8 Prodotti MELANI pubblicati

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

8.1 GovCERT.ch Blog

8.1.1 SMS spam run targeting Android Users in Switzerland

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

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

8.1.2 Dridex targeting Swiss Internet Users

08.07.2016 - In the past weeks, we have seen a rise of malicious Microsoft office documents that are being spammed out to Swiss internet users with the aim to infect them with a malicious software (malware) called Dridex. Dridex is an ebanking Trojan which is already around for some time now. The attackers are operating various botnets with Dridex infected computers. While most of these botnets do have a strong focus on financial institutions from abroad (such as US or UK), one particular botnet is also targeting financial institutions in Switzerland.

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

8.1.3 Technical Report about the RUAG espionage case

23.05.2016 - After several months of Incident Response and Analysis in the RUAG cyber espionage case, we got the assignment from the Federal Council to write and publish a report about the findings. The following is a purely technical report, intending to inform the public about Indicators of Compromise (IOCs) and the Modus Operandi of the attacker group behind this case. We strongly believe in sharing information as one of the most powerful countermeasures against such threats; this is the main reason we publish this report not only within our constituency, but to the public as well.

➔ https://www.govcert.admin.ch/blog/22/technical-report-about-the-ruag-espionage-case

8.1.4 20min.ch Malvertising Incident

08.04.2016 - With this blog post we would like to share Indicators Of Compromise (IOCs) related to the attacks against 20min.ch, a popular newspaper website in Switzerland which got compromised and abused by hackers to infect visitors with an ebanking Trojan called Gozi ISFB. The IOCs shared in this blogpost may be used to spot infections within corporate networks.

➔ https://www.govcert.admin.ch/blog/21/20min.ch-malvertising-incident

8.1.5 Leaked Mail Accounts

18.03.2016 - MELANI/GovCERT has been informed about potentially leaked eMail Accounts that are in danger of being abused. MELANI/GovCERT provides a tool for checking whether your account might be affected: https://checktool.ch.

➔ https://www.govcert.admin.ch/blog/20/leaked-mail-accounts

8.1.6 Armada Collective is back, extorting Financial Institutions in Switzerland

11.03.2016 - A new wave of extortion emails has arrived in different Swiss Onlineshops. We have strong indications, that those extortioner are a copycat of Armada Collective.

➔ https://www.govcert.admin.ch/blog/19/armada-collective-is-back-extorting-financial-institutions-in-switzerland

8.1.7 Gozi ISFB - When A Bug Really Is A Feature

05.02.2016 - Gozi ISFB is an eBanking Trojan we already know for quite some time. Just recently, a new wave was launched against financial institutions in Switzerland. Similar to the attack we had already reported in September 2015, Cybercriminals once again compromised a major advertising network in Switzerland daily visited by a large number of Swiss internet users; they all become potential victims of the Gozi eBanking Trojan.

➔ https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature

8.1.8 TorrentLocker Ransomware targeting Swiss Internet Users

21.01.2016 - On Wednesday, Jan 20 2016, we have noticed a major spam campaign hitting the Swiss cyberspace, distributing a ransomware called TorrentLocker. We have already warned about similar TorrentLocker attacks against Swiss internet users last year via Twitter. TorrentLocker is one of many ransomware families that encrypts any local file on a victim's computer and demands that the victim pays a ransom to have his files decrypted again. Since some ransomware families do not only encrypt files stored locally on the infected machine but also on any mapped network share, ransomware also represent a serious threat to corporate networks. To make sure that the malicious email goes through spam filters and gets opened by the recipient swiftly, the TorrentLocker gang is using a handful of tricks.

➔ https://www.govcert.admin.ch/blog/17/torrentlocker-ransomware-targeting-swiss-internet-users

8.2 Bollettino d'informazione

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

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

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

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

8.2.2 Numerosi documenti Office maligni in circolazione

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

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

8.2.3 Rapporto tecnico sul software nocivo utilizzato nell'attacco cyber contro la RUAG

23.05.16 - La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI ha ricevuto, dal Consiglio federale, il compito di pubblicare un rapporto contenente i dettagli tecnici sul caso RUAG. Esso è destinato principalmente a specialisti nell'ambito della sicurezza della rete ed ha l'obiettivo, in un'ottica di prevenzione e sensibilizzazione, di supportarli nell'identificazione dei rischi nella propria rete e nella messa in opera di eventuali ulteriori misure di sicurezza.

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

8.2.4 Giornata nazionale di sensibilizzazione contro i ransomware

19.05.16 - Questo giovedì la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), insieme ai propri partner, ha indetto una giornata nazionale di sensibilizzazione contro i ransomware. Vi partecipano organizzazioni di vari settori, produttori di software, uffici federali, associazioni svizzere e organizzazioni a tutela dei consumatori.

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

8.2.5 22° rapporto semestrale MELANI: gestione delle lacune di sicurezza, infrastrutture vulnerabili e diversi attacchi DDoS

28.04.2016 - Nel secondo semestre del 2015, nel mondo sono stati nuovamente registrati alcuni cyber-attacchi, talvolta spettacolari. Si rammentano in particolare diversi attacchi DDoS, attacchi phishing e contro sistemi di controllo industriali. Il tema centrale del 22° rapporto semestrale MELANI pubblicato in data odierna verte sulle lacune di sicurezza e su come affrontarle.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/rapporto_semestrale-2-2015.html

8.2.6 Password di 6‘000 account svizzeri di posta elettronica in circolazione

18.03.2016 - La Centrale d‘annuncio e d’analisi per la sicurezza e l‘informazione ha ricevuto 6‘000 indirizzi di account svizzeri di posta elettronica, che sono stati evidentemente violati e che vengono ora possibilmente usati per scopi illegali.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/passwoerter-von-6000-e-mail-konten-im-umlauf.html

8.2.7 Telefonate fraudolente contro le PMI in relazione con il cavallo di troia „Retefe“

16.02.2016 - Da inizio febbraio 2016 la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI, così come il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet SCOCI, riceve diversi annunci di telefonate fraudolente che mirano a perpetrare frodi ai danni degli utenti di portali e-banking.

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

8.3 Liste di controllo e guide

Nella prima metà dell’anno 2016 MELANI non ha pubblicato né nuove liste di controllo né nuove guide.

9 Glossario

Termine	Descrizione
Active Directory	Il servizio di rubrica di Microsoft Windows Server si chiama originariamente Active Directory (AD), anche se a partire dalla versione 2008 di il servizio è stato suddiviso in cinque parti e la componente centrale è stata definita Active Directory Domain Services (ADDS).
Advanced persistent threat (APT)	Questa minaccia provoca un danno molto 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.
Air gap	(letteralmente «vuoto d’aria») in informatica definisce un processo che separa fisicamente e logicamente due sistemi IT, pur consentendo la trasmissione dei dati di utilizzo.

App	Il concetto di app (dall'abbreviazione inglese di Application) designa in generale ogni forma di pro-grammi di applicazione. Nell'uso linguistico si fa nel frattempo perlopiù riferimento alle applicazioni per i moderni smartphone e tablet computer.
Attacco DDoS	Attacco Distributed-Denial-of-Service Un attacco DoS in cui la vittima è attaccata simultaneamente da numerosi sistemi diversi.
Batchjob	Termine derivante dall'elaborazione di dati. Con elaborazione batch si designa la modalità di funzionamento dei programmi in cui la quantità di compiti o dati predisposta come input in una o più raccolte di dati viene elaborata in forma completa, automatica e perlopiù sequenziale.
Bitcoin	Sistema di pagamento decentrato che può essere utilizzato in tutto il mondo e nome di un'unità di moneta digitale.
Booter / stresser	Strumenti informatici che scatenano attacchi DDoS a pagamento («DDoS as a service»).
Border Gateway Protocol (BGP)	Protocollo di routing utilizzato in Internet per connettere tra loro diversi sistemi autonomi.
Botnet	Rete formata da computer infettati da malware. Questi ultimi possono essere completamente telecomandati da un hacker (il botmaster). A seconda della grandezza, la botnet può essere composta da alcune centinaia fino a milioni di computer compromessi.
Browser / Navigatore	Programmi per computer utilizzati soprattutto per visualizzare diversi contenuti del World Wide Web. I browser più conosciuti sono Internet Explorer, Opera, Firefox e Safari
Brute force	Metodo di soluzione di problemi nei settori dell'informatica, della criptologia e della teoria dei giochi, fondato sulla sperimentazione di tutti i casi possibili.
Cavalli di Troia	I cavalli di Troia (sovente chiamati troiani) sono programmi che eseguono di nascosto operazioni nocive, camuffandosi in applicazioni e documenti utili per l'utente.
Certificato digitale	Certifica l'appartenenza di una chiave pubblica (PKI) a un soggetto (persona, elaboratore).
Cloud Computing	Servizio Cloud o «cloud computing» (sinonimo: «cloud IT», letteralmente «calcolare tra le nuvole»); concetto della tecnica dell'informazione (IT). Il paesaggio IT non è

	più messo a disposizione dall'utente stesso, bensì proposto da uno o più offerenti. Le applicazioni e i dati non si trovano più sul computer locale nel centro di calcolo della ditta, ma in una nuvola («cloud»). L'accesso a questi sistemi a distanza è effettuato tramite la rete.
Codice fonte	Il concetto di codice fonte, denominato anche codice sorgente (inglese: source code) designa in informatica la parte di un programma informatico scritto in linguaggio di programmazione che può essere letta dall'uomo.
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.
Controllore logico programmabile (CLP)	Un controllo logico programmabile (CLP), in inglese Programmable Logic Controller (PLC), è un'apparecchiatura utilizzata per il controllo o la regolazione di una macchina o di un impianto che viene programmata su base digitale. Da alcuni anni esso sostituisce nella maggior parte dei settori il controllore programmabile cablato a livello di hardware.
Dropper	File di programma, eseguibile autonomamente, che serve perlopiù a liberare per la prima volta un virus informatico.
Exploit-Kit	Kit che consente a criminali di generare programmi, script o righe di codice mediante i quali è possibile sfruttare le vulnerabilità di sistema del computer.
File .ini	File testuale che contiene coppie di valori. I file di inizializzazione vengono spesso utilizzati come file di configurazione dalle applicazioni Microsoft Windows.
File binario	Un file binario è un file che diversamente dai file di testo contiene anche caratteri non alfabetici. Ci può quindi essere qualsiasi valore di byte.
File di animazione SWF	L'abbreviazione SWF sta per Shockwave Flash. Inizialmente, Flash era prodotto da Macromedia, che lo commercializzava con il nome di Shockwave. Flash è il nome di una piattaforma per la programmazione e la riproduzione di contenuti multimediali e interattivi.
Grey hat	Categoria di hacker che possono anche contravvenire alle leggi o alle interpretazioni restrittive dell'etica della pirateria informatica, ma per raggiungere un obiettivo etico.
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.
JavaScript	Un linguaggio di script orientato sugli oggetti per lo sviluppo di applicazioni. Gli JavaScripts sono elementi di programma integrati nel codice HTML, che consentono determinate funzioni nel browser di Internet. Ne può essere un esempio il controllo dei dati immessi dall'utente in un modulo Web. È così possibile verificare se tutti i caratteri immessi alla richiesta di un numero telefonico corrispondono effettivamente a delle cifre. Come gli ActiveX Controls, gli JavaScripts sono eseguiti sul computer del visitatore di pagine Internet. Oltre a funzioni utili, è però anche possibile programmare funzioni nocive. Diversamente dagli ActiveX Controls, gli JavaScripts sono supportati da tutti i browser.
Keylogger	Apparecchi o programmi intercalati tra il computer e la tastiera per registrare i dati immessi sulla tastiera.
Lacune di sicurezza	Vulnerabilità dell'hardware o del software, tramite la quale gli aggressori possono accedere a un sistema.
Libreria a collegamento dinamico (DLL)	Termine generico per designare una libreria software dinamica.
Indirizzo MAC	Media Access Control Indirizzo hardware di un adattatore di rete per la sua identificazione univoca a livello mondiale. L'indirizzo MAC è scritto nella ROM dell'adattatore dai singoli fabbricanti (esempio: 00:0d:93:ff:fe:a1:96:72).
Macro-malware	Malware installato tramite macro. Una macro è costituita da una sequenza di istruzioni che possono essere eseguite con un semplice richiamo.
Malicious Code	Termine generico per software che esegue funzioni nocive su un computer. Rientrano tra l'altro in questo gruppo i virus, vermi informatici, cavalli di Toia, nonché le Logic Bombs.
Man-in-the-middle (MITM)	Un attacco man-in-the-middle (o «attacco MITM»), detto anche «attacco dell'uomo di mezzo», è una forma di attacco sferrata contro reti di computer. L'aggressore si interpone fisicamente, oggi perlopiù logicamente, tra i due partner della comunicazione, acquisendo con il proprio sistema il controllo totale sul traffico dati tra due o più utenti della rete.
Phishing	Nel caso del phishing i truffatori tentano di accedere ai dati confidenziali di ignari utenti di Internet. Si può tratta-

	re 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.
Pipe (o pipeline)	Flusso di dati tra due processi per cui vige la regola che i primi dati a essere acquisiti sono anche i primi a essere rilasciati (first in, first out).
Point-of-Sale Terminals (POS)	Terminali nei negozi presso i quali è possibile effettuare pagamenti senza contanti con carte di debito e di credito.
Programmable Logic Controller (PLC)	Designazione inglese dei controllori logici programmabili (CLP).
Ransomware	Malware tramite il quale i proprietari dei computer infettati sono ricattati (ransom: termine inglese per riscatto). Nel caso tipico i dati sono cifrati e nuovamente messi a disposizione dall'aggressore dopo il pagamento del riscatto per la chiave di decodificazione necessaria al loro ripristino.
Remote desktop protocol (RDP)	Protocollo di rete proprietario sviluppato da Microsoft che permette di riprodurre e comandare il contenuto dello schermo (desktop) di computer remoti.
Rete TOR	Sistema di anonimizzazione del traffico Web.
Rootkit	Un insieme di programmi e di tecniche che consentono di accedere inosservatamente a un elaboratore e di assumerne il controllo.
Router	Apparecchiature del settore delle reti di computer, della telecomunicazione o anche di Internet che collegano o separano più reti di computer. I router sono ad esempio utilizzati nelle reti domestiche per effettuare il collegamento tra la rete interna e Internet.
Service set identifier (SSID)	Identifica il nome di rete della WLAN. Per poter comunicare tra loro, tutti gli access point e i dispositivi terminali della WLAN devono utilizzare lo stesso SSID.
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.
Sistema autonomo	Insieme di reti IP che vengono amministrate come unità e che sono collegate attraverso uno o più protocolli in-

	terni al sistema autonomo (IGP).
Sistemi di controllo o di comando (ICS)	I sistemi di controllo o di comando (ICS) 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.
Sistemi SCADA	Supervisory Control And Data Acquisition Sistemi utilizzati per la sorveglianza e il comando di processi tecnici (ad es. approvvigionamento energetico e idrico).
Spam	Il termine spam designa l'invio non sollecitato e automatizzato di pubblicità di massa, definizione nella quale rientrano anche gli e-mail di spam. Si designa come spammer l'autore di queste comunicazioni mentre l'invio come tale è denominato spamming.
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).
User interface	(o «interfaccia utente») ciò che si interpone tra la macchina e l'utente consentendone l'interazione.
Virus	Un programma informatico capace di autoreplicarsi e provvisto di funzioni nocive, che si aggancia a un programma ospite o a un file ospite per diffondersi.
Wipe	Software (dall'inglese «spazzare» o «pulire») che serve a cancellare i file in sicurezza. Cancellando un file con Wipe, il documento viene sovrascritto più volte con zeri, pattern di bit speciali e/o dati casuali.
WLAN	L'abbreviazione WLAN (o Wireless Local Area Network) significa rete locale senza fili.
WPA2	Wi-Fi Protected Access 2 Nuovo standard di sicurezza per le reti via radio secondo la specificazione IEEE 802.11i. Versione successiva del metodo di cifratura WPA e di WEP, considerato insicuro.