Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

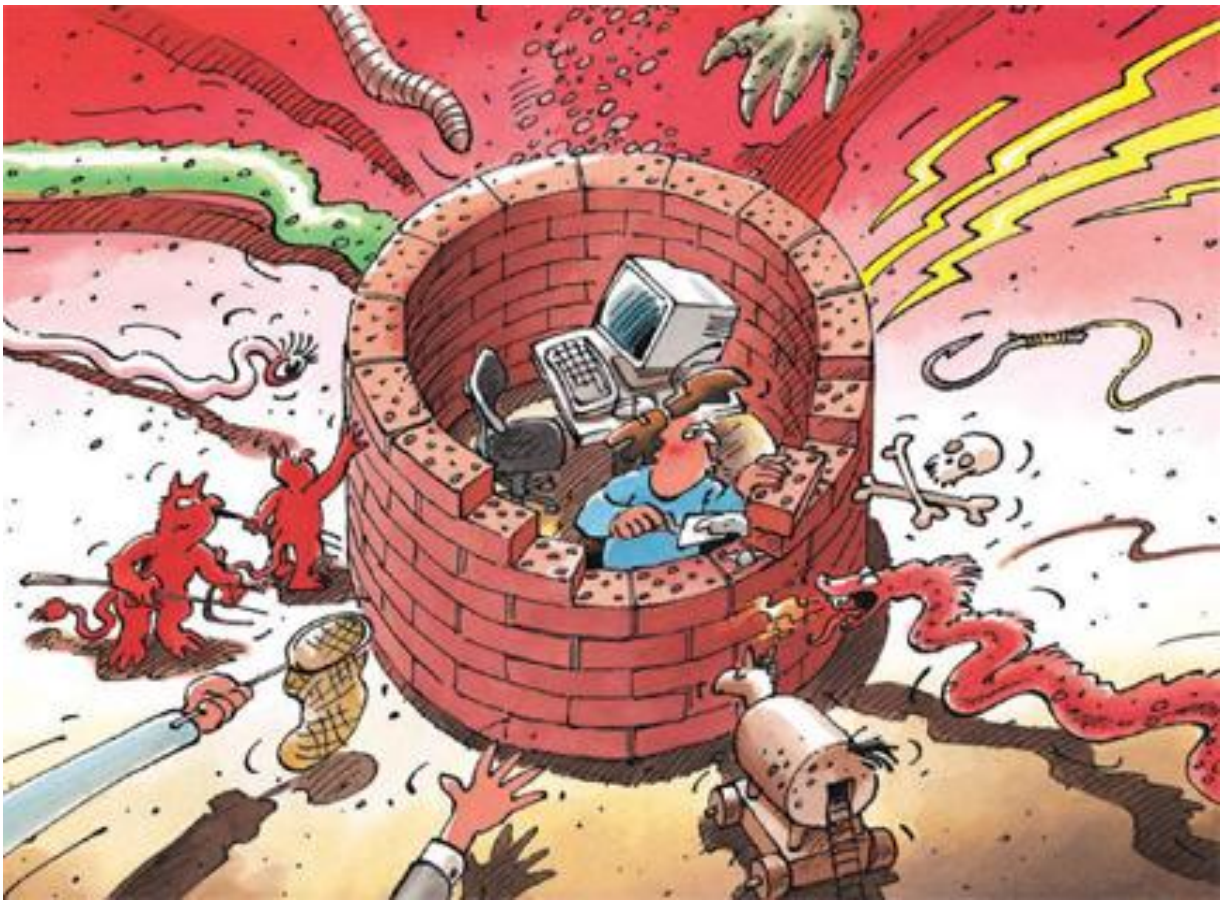
Organo direzione informatica della Confederazione ODIC
Servizio delle attività informative della Confederazione SIC

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

Sicurezza dell'informazione

La situazione in Svizzera e a livello internazionale

Rapporto semestrale 2013/I (gennaio - giugno)



Indice

1 Cardini dell'edizione 2013/I

- **DDoS – attacchi massicci anche in Svizzera**
  Nel primo semestre del 2013 si è assistito all'attuale maggiore attacco DDoS nella storia di Internet. Ne è stata bersaglio l'organizzazione non profit Spamhaus, con sede in Svizzera. Per perpetrare gli attacchi DDoS si è anche ricorso a server DNS svizzeri. Nel gennaio del 2013 si è sfruttata abusivamente l'infrastruttura della fondazione SWITCH per un attacco contro terzi. MELANI ha presentato le misure che possono essere prese per tutelare le proprie infrastrutture DNS dagli attacchi di amplificazione DNS.
  ► **Situazione attuale in Svizzera:** **capitolo 3.1**
- **Sorveglianza delle comunicazioni su Internet**
  Un tema in particolare ha fatto titolo nell'ultimo semestre: i probabili metodi di intercettazione dei diversi servizi di intelligence, resi pubblici dall'informatore Edward Snowden. Le rivelazioni sono iniziate con il programma di intercettazione Prism della NSA, seguite dalla pubblicazione relativa alle possibilità del Government Communications Headquarters (GCHQ) britannico di sorvegliare i cavi sottomarini transatlantici e la pubblicazione di una presentazione del programma di analisi XKeyscore.
  ► **Situazione attuale a livello internazionale:** **capitolo 4.1**
  ► **Tendenze / Prospettive:** **capitolo 5.1**
- **Advanced Persistent Threats – pubblicazione di numerosi casi**
  Nel primo semestre del 2013 sono stati resi noti numerosi attacchi mirati e professionali ai danni di imprese o di servizi statali. Dato che dietro di essi si presumono nella maggior parte dei casi attori statali, questi attacchi hanno anche suscitato numerose prese di posizione politiche.
  ► **Situazione attuale a livello internazionale:** **capitolo 4.2**
- **Problematica del Content Management System**
  Nel corso degli ultimi anni il numero di siti Web su Internet è pressoché esploso. Anche utenti senza dimestichezza con la tecnica possono aprire un sito Web su Internet facendo capo a mezzi semplici. A tale scopo si ricorre sovente ai cosiddetti Content Management Systems (abbr. CMS). La diffusione crescente di simili sistemi li rende interessanti anche per i cibercriminali, che ne ricercano viepiù le vulnerabilità, rintracciandole poi anche ogniqualvolta.
  ► **Tendenze / Prospettive:** **capitolo 5.4**
- **In avanzata i cavalli di Troia per smartphone**
  Nel corso dell'ultimo semestre è proseguita la tendenza del software nocivo per smartphone, con una forte progressione negli ultimi mesi. Tale tendenza si accentra soprattutto sul sistema operativo Android.
  ► **Situazione attuale in Svizzera:** **capitolo 3.3**
  ► **Tendenze / Prospettive:** **capitolo 5.6**
  ► **Allegato:** **capitolo 7.1**
- **Sistemi SCADA e sistemi industriali di comando: problematiche, lacune di sicurezza, attacchi e protezione**
  In linea di principio si può parlare di «sistema industriale di comando (ICS)» nel caso di ogni sistema che regola e/o sorveglia un processo fisico. Se nel caso dei sistemi informatici classici si attribuisce, oltre che alla disponibilità, un valore posizionale elevato anche alla confidenzialità e all'integrità, nel caso degli ICS l'accento è maggiormente posto sulla disponibilità
  ► **Situazione attuale a livello internazionale:** **capitolo 4.5**

2 Introduzione

Il diciassettesimo rapporto semestrale (gennaio – giugno 2013) della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) spiega le principali tendenze nel campo dei pericoli e dei rischi che accompagnano le tecnologie dell'informazione e della comunicazione (TIC). Esso presenta un compendio degli avvenimenti in Svizzera e all'estero, illustra i principali sviluppi in ambito di prevenzione e presenta in sintesi le attività più importanti degli attori statali e privati. Le spiegazioni dei concetti di natura tecnica o specialistica (*termini in corsivo*) sono riunite in un **glossario** (**capitolo 6**) alla fine del presente rapporto. Le valutazioni di MELANI sono di volta in volta evidenziate dal loro colore.

I temi scelti del presente rapporto semestrale sono accennati nel **capitolo 1**.

I **capitoli 3 e 4** abbordano le avarie e i crash, gli attacchi, la criminalità e il terrorismo che presentano relazioni con le infrastrutture TIC. Per il tramite di esempi scelti sono illustrati i principali avvenimenti della prima metà del 2013. In merito il capitolo 3 tratta i temi nazionali, il capitolo 4 i temi internazionali.

Il **capitolo 5** presenta le tendenze e una prospettiva delle evoluzioni attese.

Il **capitolo 7** è un allegato contenente ampie spiegazioni e istruzioni tecniche su tematiche scelte del rapporto semestrale.

3 Situazione attuale dell'infrastruttura TIC a livello nazionale

3.1 Attacchi DDoS – più frequenti e più intensi

Nel corso degli ultimi mesi sono rimasti al centro dell'attenzione dei cibercriminali i cosiddetti attacchi di *Distributed Denial Of Service (DDoS)*. Al riguardo è possibile distinguere diversi tipi di attacchi DDoS. Alcuni di essi ricorrono alle cosiddette *reti bot*, reti formate da computer infettati (bot) o da server catturati su Internet. Altri tipi di attacchi DDoS sfruttano sistemi male o insufficientemente protetti e/o le vulnerabilità dei protocolli Internet. Siffatti attacchi DDoS non costituiscono affatto una novità, ma nel corso degli ultimi mesi ne sono accresciuti il numero e l'intensità. Se le banche US sono rimaste ulteriormente al centro degli attacchi DDoS (cfr. la sezione «Brobot ulteriormente attivo»), anche alcune imprese svizzere sono state bersaglio di attacchi DDoS. Maggiori informazioni al riguardo seguono nei capitoli successivi.

Il maggiore attacco della storia contro Spamhaus

Nel primo semestre del 2013 si è assistito all'attuale maggiore attacco DDoS nella storia di Internet. Ne è stata bersaglio l'organizzazione non profit Spamhaus[1], con sede in Svizzera, che si consacra alla lotta contri gli spam e altri pericoli provenienti dal ciberspazio.

Nel marzo del 2003 aggressori ignoti hanno sferrato un attacco DDoS massiccio contro il sito Web di Spamhaus. L'attacco si è prolungato su più giorni e ha raggiunto al momento del suo apice un volume di dati di 3000Gbp/s, corrispondente al contenuto di dati di 50 CD. Spamhaus si è rivolta al provider di cloud CloudFlare, che ha tentato di respingere l'attacco. Il tentativo di parata dell'attacco da parte di CloudFlare è stato ribaltato dagli aggressori con un attacco al nodo Internet LINX di Londra (London Internet Exchange), con la conseguenza che tutto il traffico di dati disbrigato attraverso questo nodo di Internet è stato ostacolato massicciamente durante un breve periodo di tempo[2].

Nel caso dell'attacco DDoS in questione si tratta di un cosiddetto *attacco di amplificazione DNS*. Nel suo contesto si inviano richieste *DNS* falsificate a server DNS aperti su Internet (cosiddetti *Open DNS resolvers*[3]). Dato che le richieste DNS erano falsificate e contenevano l'indirizzo IP fonte di Spamhaus, questa circostanza ha fatto sì che i server DNS aperti inviassero le loro risposte all'indirizzo IP di Spamhaus e non al mittente effettivo del *pacchetto di dati*. Poiché una risposta a una richiesta DNS supera tipicamente di un multiplo la richiesta DNS stessa è stato possibile generare un notevole carico di rete fino a 300Gbit/s con comparativamente poca larghezza di banda.

---

1 The Spamhaus Project: http://www.spamhaus.org/ (stato: 31 agosto 2013).

2 The Verge - Spam war caused failure at critical internet exchange center: http://www.theverge.com/2013/3/28/4156570/Dutch-spamhaus-DDoS-took-down-london-internet-exchange (stato: 31 agosto 2013).

3 Per ulteriori informazioni sulla quantità di Open DNS resolver presenti negli AS svizzeri si veda: http://securityblog.switch.ch/2013/05/02/ddos-and-open-resolvers-the-swiss-view/ (stato: 31 agosto 2013).

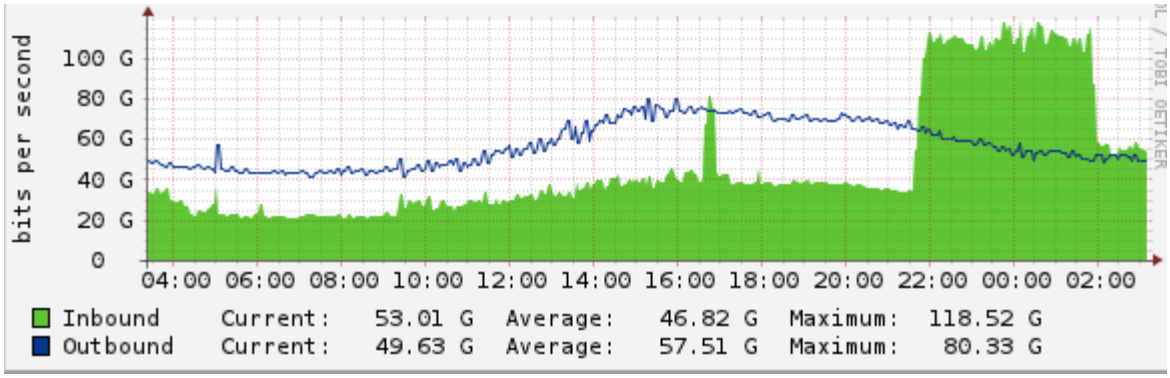


Figura 1: Traffico di rete prima, durante e dopo l'attacco DDoS (fonte: CloudFlare)

Alcune fonti presumono che l'attacco sia stato tanto potente da pregiudicare per breve tempo tutto l'Internet. MELANI non ha tuttavia potuto confermare queste supposizioni o perlomeno constatare alcun pregiudizio a Internet in Svizzera.

Si sono potute adottare le seguenti misure per tutelare le proprie infrastrutture DNS da abusi in caso di *attacchi di amplificazione DNS*:

Impedimento dell'IP address spoofing:

Si è dovuto assicurare che le apparecchiature su Internet non potessero inviare pacchetti di dati con un qualsiasi indirizzo IP di mittente (*IP address spoofing*). Al riguardo è stata sviluppata nel 2000 una Best Current Practice (BCP38), pubblicata sotto RFC2827. Sebbene esista da oltre un decennio questo standard non è ancora stato implementato o lo è stato solo parzialmente dalla maggior parte degli *Internet Service Provider (ISP)*.

Per impedire, rispettivamente per minimizzare la possibilità che l'infrastruttura TIC svizzera possa essere utilizzata per questo genere di attacchi DDoS, MELANI raccomanda a tutti i provider svizzeri di Internet di implementare lo standard descritto in RFC2827 (BCP38) per impedire a livello nazionale l'IP address spoofing.

Protezione dei server DNS:

Un'ulteriore misura per minimizzare o indebolire in futuro gli attacchi di DNS Reflection è la protezione dei server DNS. Numerosi server (DNS), ma anche altre apparecchiature periferiche, sono collegati a Internet mediante una configurazione standard (nella maggior parte dei casi la configurazione d'origine dell'apparecchiatura). Siffatte configurazioni standard sono sovente malsicure e insufficientemente restrittive. Concretamente simili apparecchiature accettano ad esempio richieste provenienti da tutto l'Internet. Le apparecchiature, rispettivamente il software, devono essere configurate in maniera tale da poter accettare soltanto le richieste provenienti da un settore di indirizzi IP locale o limitato. In tal modo si può impedire che le apparecchiature possano essere sfruttate dai criminali per attacchi contri terzi su Internet.

MELANI raccomanda ai gestori di server DNS o di apparecchiature che mettono a disposizione un servizio DNS di osservare, rispettivamente di attuare, i seguenti standard e Best Practices:

1. RFC 5358 (BCP140) Preventing Use of Recursive Nameservers in Reflector Attacks: http://tools.ietf.org/html/bcp140

2. Windows 2003 Server – Securing DNS: http://technet.microsoft.com/en-us/library/cc785404%28v=ws.10%29.aspx
3. Secure BIND Configuration Template: http://www.cymru.com/Documents/secure-bind-template.html
4. Disattivazione della recursione DNS (se non viene utilizzata): http://www.team-cymru.org/Services/Resolvers/instructions.html
5. Implementazione di Response Rate Limiting: http://www.redbarn.org/dns/ratelimits

Utilizzo abusivo di server DNS svizzeri per attacchi DDoS

Anche server DNS svizzeri sono stati utilizzati abusivamente per attacchi DDoS. Nel gennaio 2013 l'infrastruttura della fondazione SWITCH – che gestisce i Top Level Domains (TLD) «.ch» e «.li» – è stata utilizzata abusivamente per *attacchi di amplificazione DNS* contro terzi[4]. In questo contesto gli aggressori dal canto loro hanno potuto generare con poca larghezza di banda un forte carico sull'infrastruttura DNS, che ha sommerso il bersaglio dell'attacco sotto un flusso fino a 500Mbit/s.

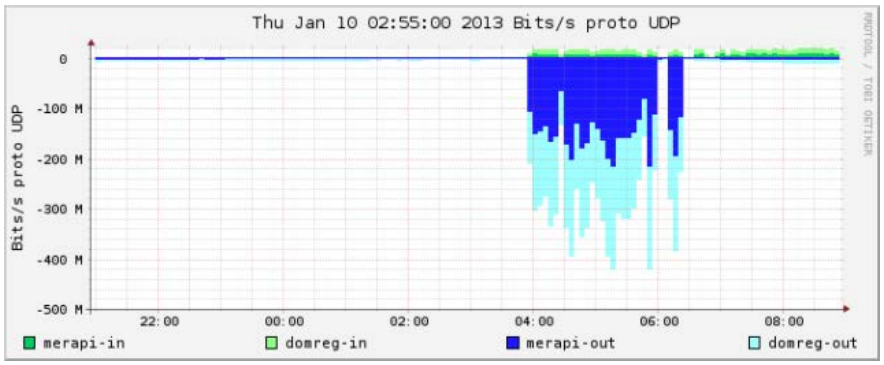


Figura 2: Traffico di rete prima, durante e dopo l'attacco DDoS (fonte: SWITCH Security Blog)

Dato che l'infrastruttura di SWITCH è predisposta per un forte traffico di dati, il suo utilizzo abusivo non ha avuto alcuna ripercussione sui Top Level Domains «.ch» e «.li».
Secondo SWITCH nel caso di questo attacco di amplificazione DNS è stato possibile generare risposte fino a 225MB/s con una larghezza di banda di soli 3 MB/s. Per poter eseguire un simile attacco basta una connessione DSL standard o una connessione via cavo (oltre al know-how necessario). Questo esempio evidenzia con quanto poca spesa sia già oggigiorno possibile un attacco DDoS. Grazie alla buona reazione di SWITCH si è potuto rapidamente porre fine a questo utilizzo abusivo.

[4] SWITCH Security Blog – Zona CH vittima di un attacco di amplificazione DNS: http://securityblog.switch.ch/2013/01/10/ch-zone-dns-angriff/ (stato: 31 agosto 2013).

DDoS con Brobot anche in Svizzera

Nel suo ultimo rapporto semestrale MELANI faceva stato di attacchi DDoS ai danni di banche US[5]. In tale contesto i siti Web di più banche US erano stati pregiudicati da volumi di dati fino 60Gbit/s e in parte anche paralizzati. Dietro a questi attacchi si presume la presenza dell'Iran.

Gli attacchi sono stati perpetrati con l'ausilio di server Web compromessi. A tale scopo gli aggressori hanno scandagliato Internet alla ricerca di installazioni Joomla![6] vulnerabili. Nell'ipotesi che rintraccino una simile installazione gli aggressori sfruttano una nota lacuna di Joomla! per collocare *software nocivo* sul sito Web della vittima. Per quanto riguarda il software nocivo si tratta di uno *script PHP* maligno, denominato Brobot[7], che apre una breccia nel sistema e dispone di una funzionalità DDoS. Nell'ottica degli aggressori i server Web hackerati offrono un grande vantaggio: i server Web dispongono sovente di una larghezza di banda maggiore di quella dei normali collegamenti a Internet, ragione per la quale si possono eseguire attacchi DDoS efficaci anche con un numero ridotto di bot.

Anche i siti Web svizzeri sono stati colpiti da Brobot. Nel primo semestre del 2013 MELANI ha informato in merito dozzine di gestori di siti Web infettati da Brobot:

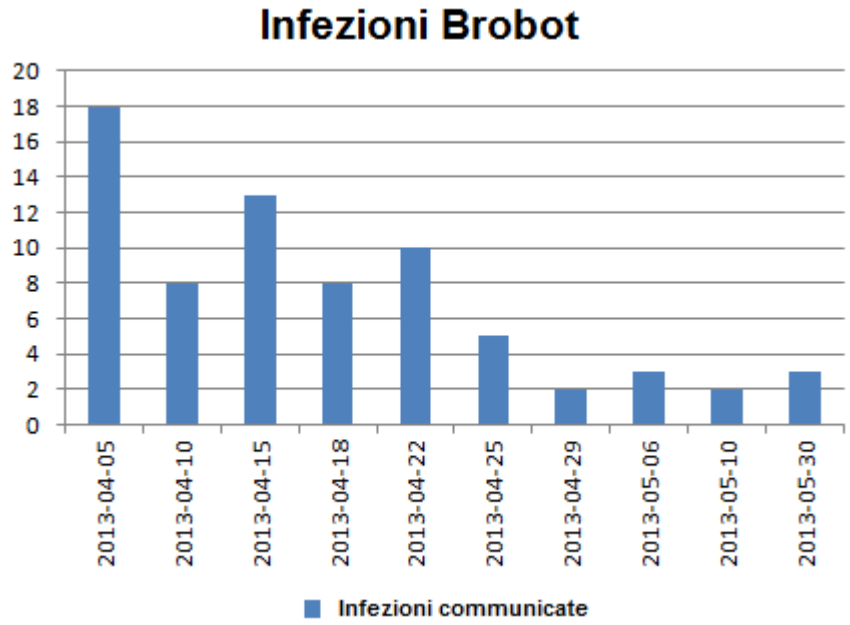


Figura 3: Infezioni Brobot comunicate da MELANI.

---

5 Rapporto semestrale MELANI 2012/2, capitolo 4.2.1: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=de (stato: 31 agosto 2013).

6 *Joomla!* è un *Content Management System* molto diffuso.

7 Symantec - PHP.Brobot: http://www.symantec.com/security_response/writeup.jsp?docid=2013-011012-0840-99&tabid=2 (stato: 31 agosto 2013).

I titolari interessati di siti Web come pure i provider di Web Hosting sono stati informati da MELANI in merito alle infezioni. Non tutti i gestori hanno tuttavia reagito – alcuni siti Web sono rimasti infettati per più mesi e sono stati regolarmente utilizzati abusivamente per attacchi DDoS ai danni delle banche US.

3.2 Tendenze in ambito di phishing

Anche nel corso del primo semestre del 2013 si sono nuovamente osservati numerosi tentativi di phishing. Si è ulteriormente affermata la tendenza degli aggressori di prendere nel proprio mirino anche i clienti e-banking di banche di minori dimensioni. Sembra che per i truffatori valga la pena configurare e adeguare appositamente i sistemi su questi bersagli anche se dal profilo statistico si possa contare solo su una o due vittime potenziali presso l'istituto finanziario interessato.

Difficoltà di disattivazione

Un precedente rapporto semestrale[8] aveva già abbordato le diverse tecniche grazie alle quali i criminali possono rendere difficile agli amministratori la disattivazione delle pagine di phishing. Per quanto riguarda il periodo attualmente in esame è stata osservata una nuova tecnica. Nella fattispecie l'affissione delle pagine di phishing dipendeva dal fuso orario configurato nel browser. Nel caso dell'ora mitteleuropea si procedeva al phishing mentre nel caso di altri fusi orari appariva un messaggio di errore. Lo scopo era ovviamente di far credere al provider (p. es. statunitense) che la pagina era già stata soppressa e che non erano quindi necessarie ulteriori azioni. La pagina per la truffa rimane online per un tempo corrispondentemente più lungo e raggiunge potenzialmente un numero maggiore di vittime.

Per la prima volta in Flash una pagina di phishing ai danni di un istituto finanziario svizzero

Nel caso normale i truffatori copiano, al momento dell'allestimento della pagina di phishing, la pagina originale della banca, introducendovi un paio di piccole modifiche, e la salvano successivamente su un server predisposto per questa truffa. Questo modo di procedere è relativamente semplice e non esige neppure grandi conoscenze in ambito di TIC. Sorprende invece il fatto della scoperta, per la prima volta in *Flash,* di una pagina di phishing ai danni di un istituto finanziario svizzero. Per quanto riguarda i motivi che hanno indotto i truffatori a ricorrere a un genere di programmazione piuttosto complicato si possono soltanto fare speculazioni. I dati ritrovati nella directory della pagina di phishing portano alla conclusione che i truffatori hanno utilizzato un semplice kit per l'allestimento di formulari Web, che genera versioni Flash. Un ulteriore motivo potrebbe consistere nel fatto che in questi programmi Flash il testo non è perquisibile. I programmi anti phishing dispongono di minori possibilità di individuazione delle pagine di phishing in base di parole chiave e di di minori possibilità avvertimento degli utenti dei computer.

[8] Rapporto semestrale MELANI 2011/2, capitolo 3.4: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (stato: 31 agosto 2013).

Colpiti anche i clienti e-banking di banche di minori dimensioni

Negli ultimi tempi si osservano sempre più – oltre ai numerosi tentativi di phishing ai danni delle imprese di carte di credito e delle grandi banche – tentativi di phishing ai danni di banche di minori dimensioni. Il motivo potrebbe risiedere nel fatto che i truffatori si spostano su questi istituti finanziari perché ivi le misure di sicurezza non sono ancora molto elevate, rispettivamente perché la loro clientela non è sovente ancora stata confrontata con questi fenomeni.

Da un profilo meramente statistico l'attacco ai danni di banche di minori dimensioni avrebbe un senso soltanto se esistesse un'eccellente situazione in fatto di dati e se si indirizzasse in maniera mirata esclusivamente ai clienti di queste banche. Finora questo modo di procedere mirato nel caso delle banche di minori dimensioni non ha potuto essere constatato – la diffusione, rispettivamente l'invio di e-mail di phishing, sembra tuttora funzionare secondo il principio di casualità.

3.3 In circolazione sugli smartphone software e-banking nocivo

Nel corso del primo semestre del 2013 la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI ha messo in guardia contro una nuova ondata di attacchi alle operazioni svizzere di e-banking mediante firma delle transazioni via SMS. Nel contesto di questo genere di attacco si installa un software nocivo sul computer. Nel momento in cui il cliente effettua il login sul proprio conto e-banking appare un messaggio secondo il quale si dovrebbe installare un nuovo certificato di e-sicurezza. Il cliente viene invitato a indicare il tipo di smartphone e il numero di telefonia mobile. Successivamente il cliente viene invitato a installare il nuovo certificato sullo smartphone. Sullo smartphone viene in realtà installato un software nocivo che consente all'aggressore di carpire lo SMS necessario alla firma della transazione e di effettuare pagamenti abusivi.

Figura 4: Finestra che viene visualizzata durante la procedura di login e che invita il cliente e-banking a installare un certificato sul proprio smartphone.

Le banche svizzere non invitano mai i propri clienti a installare nuovi elementi di sicurezza mediante inserti sullo schermo o via SMS. MELANI raccomanda a tutti i clienti e-banking invitati durante una sessione di e-banking a installare sul proprio smartphone un certificato

(cfr. figura) o qualcosa del genere a interrompere la procedura di e-banking, a chiudere il collegamento con l'e-banking (pulsante logout) e a contattare immediatamente la banca. L'allegato 7.1 contiene una descrizione dettagliata dell'attacco.

3.4 Attacchi mirati di social engineering ai danni di imprese svizzere

In ambito di tentativi mirati di truffa si ricorre a diversi metodi di social engineering. Questi attacchi sono peraltro sempre più sovente diretti contro piccole e medie imprese (PMI).

In questa sede saranno tematizzati due casi ai danni di imprese svizzere che erano stati comunicati a MELANI. Nel primo caso, che risale al mese di marzo 2013, il capo delle finanze di una PMI attiva a livello internazionale ha ricevuto una e-mail presuntivamente inviata dal CEO. L'e-mail assomigliava in maniera ingannevole a quelle usuali nell'impresa e invitava il capo delle finanze a trasferire un'importante somma di denaro sul conto di un avvocato in vista di un sedicente acquisto in Cina. Il progetto era evidentemente inventato e il tutto costituiva un trucco per ottenere una rimessa.

Il lato interessante di questo caso è il dispendio relativamente importante di ricerche che gli aggressori devono effettuare preliminarmente. Per poter imbastire un simile scenario i truffatori hanno dovuto occuparsi della struttura organizzativa dell'impresa e analizzarla.

Nel mese di giugno 2013 è stato comunicato a MELANI un altro attacco a una PMI svizzera. Nel contesto di questo attacco aggressori sconosciuti hanno tentato di penetrare nella rete aziendale di questa impresa del Cantone di Zurigo. L'aggressore ha telefonato a una collaboratrice dell'impresa, chiedendo di poter parlare con la contabilità in merito a una fattura ancora aperta. Dato che la collaboratrice non poté rintracciare l'allibramento della fattura nel sistema, l'aggressore – che si esprimeva in francese – offrì di scannerizzare la fattura e di inviarla via e-mail. La collaboratrice comunicò il proprio indirizzo di posta elettronica e ricevette dopo pochi minuti, come convenuto telefonicamente, una e-mail contenente un *hyperlink*. Cliccando l'hyperlink la collaboratrice non ricevette tuttavia la fattura attesa, ma un file eseguibile Windows con l'estensione «.exe». L'esecuzione del file ha installato inosservatamente un cosiddetto *Remote Administration Tool (RAT)* sul suo computer. Questo tool ha consentito agli aggressori di comandare in maniera inosservata a distanza il computer via Internet.

Fortunatamente la collaboratrice in questione si è insospettita e ha comunicato al servizio interno di supporto TIC dell'impresa l'e-mail sospetta. Tale servizio ha potuto confermare l'infezione dell'apparecchiatura e renderla innocua. L'impresa in questione ha sporto denuncia penale contro ignoti. MELANI parte dal presupposto che in questo caso gli aggressori perseguissero intenti finanziari.

Nel corso degli ultimi anni è aumentato il numero di simili attacchi ai danni di imprese svizzere. Dall'esempio emerge che non ne sono colpite soltanto le grandi imprese, ma anche aziende di medie e piccole dimensioni. Gli aggressori perseguono obiettivi diversi. Essi agiscono sovente per intenti finanziari (p. es. truffa ai danni dell'e-banking) o per interessi commerciali (procacciamento di informazioni sulla concorrenza, informazioni sulla clientela, spionaggio industriale).

Simili attacchi sono sovente realizzati con l'ausilio di un Remote Administration Tool

(RAT). Si tratta nella fattispecie di software nocivo che può essere acquistato su Internet per un paio di centinaia di dollari e offre un'ampia scelta di funzionalità (dalla registrazione delle immissioni sulla tastiera al comando a distanza integrale del computer). Se paragonati ai cavalli di Troia e ad altri parassiti, simili RAT non sono di norma tecnicamente molto sofisticati. Tuttavia numerosi programmi antivirus non li rintracciano oppure soltanto quando è troppo tardi.

3.5 In circolazione e-mail con link su pagine infettate

Sono ampiamente diffuse le e-mail destinate a indurre il destinatario a cliccare su qualcosa. In questo senso fin dal suo ultimo rapporto semestrale[9] MELANI ha accennato alle fatture o transazioni fittizie destinate a indurre il destinatario a cliccare sull'allegato. L'allegato contiene di volta in volta un software nocivo, perlopiù impacchettato in un *file zip*, che infetta il computer quando viene aperto. Un tentativo un poco diverso è stato osservato il 22 gennaio 2013. Una e-mail in lingua olandese si spacciava come proveniente da un servizio ufficiale del Cantone di Argovia. Cliccando sul link si tentava in sottofondo di individuare le vulnerabilità del computer per installarvi un software nocivo. Il Cantone di Argovia non è stato vittima di un attacco hacker – sono stati unicamente utilizzati come mittente indirizzi di posta elettronica del dominio «ag.ch». Si osserva sovente l'utilizzo abusivo come mittente di imprese o servizi conosciuti.


Betreff: Informatie met betrekking tot uw NAT3799 belastingformulier

Houd er rekening mee dat je hebt fouten gemaakt bij het invullen van de laatste NAT3799 aangifte (ID:).
Zie aanbevelingen en tips van onze fiscalisten Door hier te klikken
(Wacht 3 minuten tot rapport zal laden)

Alsjeblieft tot wijziging van de fouten en verzenden de herziene aangifte aan uw lokale belastingkantoor zo snel mogelijk.

Kanton Aargau

Figura 5: E-mail con link su un'infezione drive-by.

Non è chiaro per quale motivo l'e-mail sia stata redatta in lingua olandese. Si presume che si sia trattato di un errore dell'aggressore, dato che questa circostanza ha notevolmente ridotto le chance di riuscita. Non è neppure chiaro perché sia stato utilizzato come mittente un servizio ufficiale del Cantone di Argovia. Ciononostante va rammentato ancora una volta che va sempre usata grande prudenza nel caso di e-mail inaspettate di imprese o servizi conosciuti, visto che è semplice falsificare i mittenti delle e-mail. Il fatto che nella fattispecie si siano sfruttate le lacune di sicurezza del computer evidenzia quanto sia importante mantenere aggiornato non soltanto il sistema operativo, ma anche tutte le applicazioni.

[9] Rapporto semestrale MELANI 2012/2, capitolo 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=de (stato: 31 agosto 2013).

3.6 VoIP: Abusi in Svizzera

VoIP (Voice-over-IP) è la denominazione della tecnologia per il cui tramite è possibile telefonare utilizzando le reti IP, sia su una rete privata controllata, sia sull'Internet pubblico. Nel corso degli ultimi anni la telefonia VoIP e in particolare quella attraverso l'Internet pubblico ha registrato una forte crescita a livello di persone private e di imprese. Uno dei principali motivi della sua crescente popolarità ne è il prezzo conveniente, soprattutto delle conversazioni internazionali. La diffusione in aumento di questa tecnologia va nondimeno di pari passo con un incremento degli abusi.

Nel corso del primo semestre del 2013 la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI ha informato in merito a una truffa in grande stile nel cui contesto le infrastrutture di un'impresa svizzera, o più propriamente un server virtuale di questa impresa, sono state utilizzate abusivamente per una truffa effettuata mediante telefonate da numeri a pagamento di servizi a valore aggiunto (numeri Premium, *VoIP Toll Fraud*). Come controprestazione di questa attività particolarmente lucrativa lo hacker riceve una commissione dall'offerente del numero Premium.

In questo caso il server virtuale è stato hackerato e utilizzato abusivamente per l'esecuzione della truffa. È molto probabile che siano stati anche hackerati i conti che si situavano sul server e che alla fine i costi delle chiamate a questi numeri a valore aggiunto siano stati addebitati al titolare effettivo del pertinente conto telefonico, una persona privata o un'impresa.

Attualmente le truffe effettuate integralmente o parzialmente mediante il telefono sfruttano in ampia misure la tecnologia VoIP. Ciò riguarda in particolare il voice-phishing, nel cui contesto le vittime sono chiamate per carpire loro i dati di accesso all'e-banking. Anche i chiamanti che si spacciano per agenti di supporto di Microsoft e tentano di accedere al computer per un presunto problema di sicurezza sfruttano questa tecnologia. È il motivo per il quale la sicurezza di questa tecnologia è viepiù al centro dell'attenzione. Per gli aggressori l'utilizzo di un'infrastruttura hackerata comporta diversi vantaggi: anzitutto la possibilità di telefonare a spese di terzi, ma anche di meglio camuffare la propria identità. Oltre a queste truffe il capitolo 5.7 descrive ulteriori possibili abusi del VoIP.

3.7 Ondata di SMS con truffa dell'anticipo

Nel campo delle e-mail ci si è da lungo tempo abituati allo *spam*. In questo ambito i provider tentano di filtrare e di rimuovere nella misura del possibile le comunicazioni non desiderate. Il fatto che questo genere di attacco venisse utilizzato prima o poi sul vettore *SMS* non ne è che una conseguenza logica. Per gli spammer tuttavia l'invio a mezzo SMS era finora molto più costoso dell'invio a mezzo e-mail. Questa situazione sembra ora modificarsi, come illustrato da un caso avvenuto nel primo semestre del 2013.

Nel mese di aprile 2013 un'ondata di SMS di spam ha colpito anche la Svizzera. Oltre 500'000 clienti di Swisscom, ma anche clienti di Orange e di Sunrise, sono stati toccati da questa ondata. L'informazione è stata presumibilmente inviata seguendo il principio di causalità a settori conosciuti di numeri.

Per quanto concerne gli SMS inviati nella fattispecie si tratta di una tipica truffa dell'anticipo. Le offerte e le promesse contenute in una simile comunicazione – in questo caso una vincita alla lotteria – sono di volta inventate e sono unicamente destinate a offrire uno scenario cre-

dibile per perpetrare la truffa. Rispondendo alla comunicazione si riceve una richiesta di anticipo fondata su un pretesto qualsiasi. Le somme di denaro promesse non saranno però mai versate. Simultaneamente potrà essere fatto un uso abusivo dei dati personali resi noti (numero del passaporto, fotografie, ecc.) come falsa identità per ulteriori truffe.

Figura 6: SMS con truffa dell'anticipo.

Gli SMS sono stati inviati per il tramite dei provider britannici di telefonia T-Mobile UK e Orange UK, circostanza che ha indotto Swisscom ad adottare una misura a breve scadenza, ossia a non trasmettere gli SMS provenienti da questi due provider finché questi provider avessero potuto stopparli, rispettivamente bloccarli, sulle loro proprie reti.

Le comunicazioni spam a mezzo SMS sono meno diffuse degli spam mediante e-mail, che rappresentano secondo diverse fonti tra il 70%[10] e l'85%[11] dell'intero traffico e-mail. Nel caso degli spam via SMS esistono inoltre forti differenze a livello regionale. Negli USA la tecnologia SMS è poco utilizzata, ragione per la quale la percentuale di spam via SMS è inferiore all'uno per cento. In Asia invece tale percentuale può giungere al 30%[12]. Lo spam via SMS è più costoso rispetto allo spam via e-mail e quindi non veramente interessate per gli spammer. L'aumento del numero di smartphone in connessione con le corrispondenti possibilità di hackerare questi telefoni dovrebbe tuttavia incrementare il numero di invii spam via SMS.

La possibilità di filtrare gli spam via SMS non è tuttavia molto progredita e funziona perlopiù in base a «liste nere», diversamente dai filtri per e-mail mediante *Spam Score*.

3.8 Monitor pubblicitari pilotati da terzi

Un'azione particolare è avvenuta durante il mese di giugno a un ufficio postale a Zurigo. Alcuni ragazzi hanno avuto accesso a uno schermo pubblicitario. La Posta affitta a società di marketing degli spazi per installare degli schermi pubblicitari che sono gestiti interamente dal locatario.

Un ragazzo di 17 anni, dopo aver smontato alcuni elementi di sicurezza fisica e dopo aver riavviato il computer collegato allo schermo, è riuscito a connettersi al sistema. Ha in seguito installato una componente che gli ha permesso di pubblicare del contenuto pornografico sul-

[10] http://www.spamfighter.com/News-18508-Spam-Increases-to-707-of-Total-E-mail-Traffic.htm (stato: 31 agosto 2013).
[11] http://senderbase.org/static/spam#tab=1 (stato: 31 agosto 2013).
[12] http://en.wikipedia.org/wiki/Mobile_phone_spam (stato: 31 agosto 2013).

lo schermo a partire da una fonte esterna. L'intento è stato quello di attirare l'attenzione su una lacuna di sicurezza. Visto l'interesse mediatico suscitato, l'azione ha avuto un rilievo nazionale.

A prescindere dalle questioni giuridiche sollevate da questo caso concreto – ossia dalla punibilità del fatto di rendere materiale pornografico accessibile ai minori – questo evento solleva la questione del modo di procedere migliore quando viene individuata una lacuna di sicurezza. In merito occorre ponderare in quale misura una simile azione sia effettivamente destinata alla sensibilizzazione oppure alla compiacenza personale e se in simili casi non sarebbe molto più efficace informare direttamente il servizio interessato.

All'atto dell'individuazione di lacune di sicurezza svolgono sempre più sovente un ruolo anche considerazioni finanziarie. Il mercato del Security Business è fortemente conteso. In questo senso esistono imprese specializzate nella ricerca di simili lacune di sicurezza, che le rivendono alle imprese produttrici. La ricerca e la pubblicazione di lacune di sicurezza vengono anche sfruttate come opportunità pubblicitaria di richiamare l'attenzione sulla professionalità della propria impresa.

3.9 Swiss Cyber Storm e talenti informatici di domani

Il 13 giugno 2013 si è svolta al KKL di Lucerna la conferenza «Swiss Cyber Storm 4». Un ampio ventaglio di referenti internazionali dotati di eccellenti conoscenze specialistiche hanno anzitutto presentato le loro relazioni ai decisori dell'economia svizzera.

Si trattava poi anche di ricercare i migliori talenti informatici svizzeri. Nelle settimane precedenti questo congresso di un solo giorno gli studenti e gli scolari hanno avuto la possibilità di partecipare online a cosiddetti «Challenges». Nel loro contesto si trattava di risolvere indovinelli e rompicapo informatici. Non si ricercavano tuttavia hacker, bensì talenti capaci di riflessioni più vaste e globali degli hacker. Concretamente ciò significa: non basta essere in grado di forzare file zip criptati. I candidati devono piuttosto essere in misura di illustrare grazie a quale errore di cifratura hanno potuto forzare i file e come eliminerebbero questo errore. Non si trattava quindi di attaccare, ma di illustrare come dovrebbero essere protetti i propri sistemi.

Le esigenze poste ai partecipanti erano molto diverse. Oltre al superamento di sfide tecniche si trattava ad esempio di risolverle entro un tempo determinato, circostanza che accresceva ulteriormente la pressione esercitata sui candidati. Si richiedeva pertanto la capacità di non riflettere soltanto in una direzione prestabilita, bensì di reagire in maniera flessibile e di lavorare in modo orientato alla soluzione e al team.

Lo Swiss Cyber Storm ha costituito un arricchimento per tutti i partecipanti: essi hanno potuto ampliare le loro conoscenze e intessere importanti contatti con l'economia privata. In questo senso uno dei partecipanti ha già ricevuto un'offerta di lavoro.

Cosa farà seguito a Swiss Cyber Storm?

Il gruppo dei vincitori non può riposarsi sugli allori. Esso è stato invitato dagli organizzatori di Swiss Cyber Storm a partecipare nel novembre del 2013 alla finale del concorso, a Linz, con il team vincitore della finale austriaca della conferenza sorella[13].

MELANI ha assunto il patronato di Swiss Cyber Storm unitamente a Swiss Police ICT – un'associazione privata che con il congresso dell'informatica della polizia svizzera getta ogni anno un ponte tra informatica e perseguimento penale. L'obiettivo comune è di trovare anche in futuro nuovi talenti informatici svizzeri.

4 Situazione attuale dell'infrastruttura TIC a livello internazionale

4.1 Sorveglianza delle comunicazioni su Internet

Un tema in particolare ha fatto titolo nell'ultimo semestre: i probabili metodi di intercettazione di alcuni servizi di informazione, resi pubblici dall'informatore Edward Snowden. Le rivelazioni sono iniziate con il programma di intercettazione Prism della NSA, seguite dalla pubblicazione relativa alle possibilità del Government Communications Headquarters (GCHQ) britannico di sorvegliare i cavi sottomarini transatlantici e la pubblicazione di una presentazione del programma di analisi XKeyscore. Snowden era impiegato presso la CIA, prima di passare al fornitore privato di servizi di sicurezza Booz Allen Hamilton, che svolge tra l'altro mandati per conto della NSA[14]. Nel contesto di queste rivelazioni sono stati tematizzati programmi di sorveglianza in diversi altri Paesi.

Prism

Prism è il nome di un presunto programma di intercettazione della NSA, reso pubblico da Edward Snowden. Il nome proviene dal fatto che i segnali sui cavi di fibra ottica sono separati ed estratti mediante un prisma. È comunque dubbio se i dati vengano rilevati in questo modo. Nel caso di questo programma di intercettazione deve piuttosto trattarsi di un progetto grazie al quale la NSA ha accesso ai server di diverse imprese US, come ad esempio Microsoft, Google o Yahoo.

Non è affatto straordinario il fatto che servizi dello Stato abbiano accesso all'infrastruttura nazionale di telecomunicazione. Simili accessi sono tuttavia severamente regolamentati: per accedere a siffatti dati è tipicamente necessaria una procedura penale o un decreto del giudice, oppure motivi particolari, previsti da leggi speciali. La novità riguardo alle informazioni pubblicate è il fatto che i servizi US di intelligence vi abbiano non soltanto un accesso puntuale, bensì un accesso a questi dati apparentemente sistematico ed esteso a tutto il territorio. Tutte le imprese interessate hanno contestato una simile ampia collaborazione e indicato

[13] http://www.verbotengut.at/ (stato: 31 agosto 2013).

[14] Il presente rapporto riguarda il periodo gennaio-giugno 2013. Le ulteriori informazioni divenute di dominio pubblico concernenti l'informatore Edward Snowden saranno tematizzate nel prossimo rapporto semestrale.

che sono pubblicati unicamente i dati concernenti conti specifici in base a decisioni giudiziarie.

I servizi dello Stato hanno sempre ribadito che tutte le misure di intercettazione adottate sono legittimate per legge e approvate dai tre poteri istituzionali degli USA. Il «Foreign Intelligence Surveillance Act (FISA)» emanato nel 1978 disciplina la sorveglianza all'estero di persone straniere sul territorio US e di cittadini US. La Foreign Intelligence Surveillance Court (FISC) approva in quanto autorità giudiziaria misure corrispondenti di sorveglianza. Le modifiche del FISA consecutive ad atti come il «Patriot Act» (2001) o il «Protect America Act» (2007) hanno attribuito alle autorità ampie competenze in ambito di sorveglianza delle comunicazioni, adeguate alla mutata situazione di minaccia – in particolare il terrorismo – e all'evoluzione tecnica, come Internet in quanto media e il trasferimento delle comunicazioni internazionali dal satellite al cavo in fibra ottica.

Tempora

Un ulteriore rapporto che Snowden ha procurato al quotidiano britannico «The Guardian» tratta di un programma di intercettazione denominato Tempora, che sarebbe utilizzato dall'intelligence britannica. Nel quadro di questo programma il Government Communications Headquarter (GCHQ) britannico avrebbe accesso ai collegamenti transatlantici di dati, con la possibilità di estrarre e copiare i dati desiderati. Il rapporto è incentrato sul cavo TAT-14 che porta a New Jersey, via la Gran Bretagna, a partire dalla Germania, dalla Danimarca, dai Paesi Bassi e dalla Francia. Il GCHQ avrebbe accesso a questo cavo nella città portuale di Bude, suo punto di passaggio in Gran Bretagna. Farebbero parte dei dati carpiti e-mail, registrazioni su Facebook e anche comunicazioni telefoniche. Il GCHQ attingerebbe a oltre 200 collegamenti via fibra ottica e occuperebbe 500 collaboratori nelle analisi[15].

Nel corso degli ultimi anni il traffico transatlantico Internet si è sempre più spostato sui cavi sottomarini in fibra ottica. Se nel 1986 fino all'80% del traffico transatlantico di dati era effettuato via satellite, oggigiorno la maggior parte del traffico continentale e intercontinentale è effettuato mediante cavi in fibra ottica riuniti in una rete. Per la comunicazione tra due utenti esistono in genere più percorsi e solo al momento del trasferimento effettivo dei dati si decide quale percorso utilizzare. L'intercettazione del traffico su un cavo sottomarino non significa obbligatoriamente che tutta la comunicazione, ovvero un'intera e-mail, possa essere carpita, anche se nella prassi ciò succede frequentemente.

XKeyscore

XKeyscore è un software di analisi sviluppato dalla NSA e utilizzato da numerosi servizi di intelligence. Esso renderebbe possibile l'attribuzione in tempo reale a una determinata persona mirata di numerosi dati, come e-mail, chat online ecc, contenuti in diverse banche dati. Al riguardo si possono applicare i più diversi criteri di ricerca, come ad esempio indirizzo IP, lingua, browser, parametri di configurazione e numero di telefono. Sarà quindi possibile rintracciare tutti i dati raccolti in questo contesto. Secondo la presentazione segreta del 2008 pubblicata da Snowden la rete XKeyscore consta di oltre 700 server ripartiti su 150 ubicazioni nel mondo intero. I servizi di intelligence per l'estero di UK, Canada, Australia e Nuova

[15] http://www.handelsblatt.com/politik/international/abhoerskandal-auch-britischer-geheimdienst-spaeht-daten-aus/8391120.html (stato: 31 agosto 2013).

Zelanda parteciperebbero anch'essi a XKeyscore. Anche il Bundesnachrichtendienst (BND) tedesco dovrebbe introdurre il programma.[16]

Non sorprende affatto che servizi di intelligence dispongano di strumenti adeguati a una analisi efficace tra i dati già raccolti. Oggigiorno l'analisi di un grande fondo di dati è possibile soltanto con programmi di analisi corrispondenti. Tutti conoscono questa modalità di funzionamento dei diversi motori di ricerca: anche in questo caso è decisivo ottenere i risultati desiderati in una frazione di secondi. A prescindere da chi, a quale momento e a quali dati di un simile sistema abbia accesso, la questione non dovrebbe concentrarsi sulle modalità di analisi dei dati da parte dei servizi di intelligence, ma su quali dati essi possono in definitiva rilevare e memorizzare, rispettivamente su quali richieste sono effettivamente legittime all'interno di questi dati.

4.2 Advanced Persistent Threat: Red October, Net Traveller, MiniDuke

Nel corso del primo semestre del 2013 si è avuto nuovamente notizia di alcuni attacchi mirati e professionali ai danni di imprese o di servizi statali. Nel caso di questi attacchi si trattava in genere di cosiddetti *Advanced Persistent Threats (APT)*. È caratteristico del contesto degli APT che gli aggressori tentino ostinatamente e nei più diversi modi di accedere a determinati sistemi per annidarvisi ed eseguire inosservatamente le loro attività nocive. Sovente l'infezione iniziale avviene tramite *attacchi di Spear-Phishing* o di *Watering-Hole*. Vengono successivamente aperte brecce nel sistema e carpiti con l'inganno i diritti di amministratore. L'obiettivo finale è di permanere per lungo tempo inosservati nel sistema, di muoversi inosservati al suo interno, di spiare i dati e in parte di modificarli o di cancellarli. Per perpetrare con successo simili attacchi occorre un forte dispendio, ragione per la quale dietro di essi si presumono sovente attori statali. Ma anche gruppi criminali o singole persone che dispongono di molto tempo, altamente motivati e con prospettive di vendita a terzi dei dati raccolti, non possono essere esclusi come aggressori.

L'impresa di sicurezza TIC FireEye stima in un suo rapporto che le imprese, rispettivamente le organizzazioni, ricevono ogni tre minuti una e-mail contenente un link o un allegato nocivo[17]. Anche in Svizzera i sistemi con informazioni sensibili sono quotidianamente esposti a simili attacchi.

Nel corso del primo semestre del 2013 una comunicazione di attacchi di questo genere cacciava la precedente. Dato che nella maggior parte dei casi si presumono attori statali dietro di essi, questi attacchi hanno parimenti sollevato numerose prese politiche di posizione.

Gennaio: Operazione Red October

Il 13 gennaio 2013 l'impresa russa di sicurezza TIC Kaspersky ha fornito dettagli in merito a un'operazione di spionaggio ai danni delle missioni diplomatiche, dei governi e delle organizzazioni internazionali. I bersagli dell'operazione denominata Red October si situavano soprattutto nell'Europa dell'Est, in Asia centrale e negli Stati della CSI. Il rapporto di Kaspersky

[16] http://www.zeit.de/politik/deutschland/2013-08/bnd-xkeyscore-nsa (stato: 31 agosto 2013).
[17] http://www2.fireeye.com/WEB2012ATR2H_advanced-threat-report-2h2012.html (stato: 31 agosto 2013).

menziona altresì che si è acceduto all'*infrastruttura di comando e di controllo dei server* a partire da numerosi indirizzi IP svizzeri, circostanza che di primo acchito faceva pensare a molte vittime in Svizzera. Nel quadro di una sua prima analisi MELANI ha poi constatato che si trattava in numerosi casi di indirizzi IP dinamici. Dopo eliminazione dei casi sospetti, contati a più riprese, il numero di infezioni effettive va chiaramente corretto al di sotto delle cinque vittime. Nel caso delle vittime non si trattava peraltro di organizzazioni svizzere, bensì di infrastrutture estere gestite in Svizzera.

Le vittime sono state infettate dal software nocivo degli allegati alle e-mail. Una particolarità di questi attacchi consiste nel fatto che il software nocivo poteva procurarsi non soltanto i dati dei computer infettati ma anche quelli situati su apparecchiature mobili. Questa operazione di spionaggio deve già essere stata attiva fin dal 2007 o magari anche da molto tempo prima. Secondo l'impresa Kaspersky gli autori provengono da aree di lingua russa.

Febbraio: APT1

All'inizio di quest'anno si è soprattutto registrato un aumento degli attacchi ai danni delle imprese US. Questa serie di attacchi ha sollevato numerose prese di posizione da parte di politici US di spicco, che hanno perorato un rafforzamento delle misure di difesa e sovente additato la Cina come Paese di provenienza dei maggiori pericoli nel settore dello spionaggio informatico.

Nonostante la molteplicità degli attacchi e dei bersagli è possibile individuare determinati modelli. In questo senso essi avevano nel mirino grandi imprese industriali statunitensi come Apple, Facebook, Google, Microsoft e Twitter. I sistemi sono stati soprattutto infettati per il tramite di attacchi di *Watering-Hole* e più precisamente via un sito Web per sviluppatori di applicazioni mobili. I visitatori del sito erano infettati da uno *Zero-Day-Exploit* nel programma *Java*. In parallelo numerosi grandi media statunitensi (New York Times, Wall Street Journal, Bloomberg, Washington Post) hanno fatto stato di attacchi, in particolare ai conti di posta elettronica dei loro giornalisti. In entrambi i casi si è presunta una paternità cinese degli attacchi.

In questo contesto è stato pubblicato nel mese di febbraio 2013 un rapporto dell'impresa statunitense di sicurezza Mandiant che pretendeva di poter dimostrare la partecipazione dello Stato cinese alle operazioni di spionaggio informatico contro gli USA e alcuni Paesi europei. Tale rapporto si fonda su ricerche effettuate in collaborazione con le imprese vittime degli attacchi. A titolo di conclusione principale il rapporto presenta un legame tra un gruppo di aggressori informatici, denominato «APT1», e un'unità dell'esercito cinese. Mandiant pretende che il gruppo abbia derubato dal 2006 numerosissimi dati da 146 vittime prescelte.

Anche in questo caso la Svizzera è stata toccata solo indirettamente, perché nel caso dei sistemi interessati si tratta di infrastrutture estere gestite in Svizzera.

Febbraio: Operazione Beebus

Sempre nel medesimo contesto politico anche l'impresa statunitense FireEye ha pubblicato nel febbraio del 2013 i risultati di un suo lavoro su un'ulteriore operazione di spionaggio, un APT denominato Beebus. Sembra che questa operazione abbia avuto soprattutto nel mirino imprese del settore della difesa e dell'astronautica. Le vittime venivano infettate sia da e-mail mirate, sia *da infezioni drive-by* con il metodo del download. Secondo FireEye le prime tracce dell'attacco risalgono al 2011. FireEye presume che l'attacco potrebbe essere di origine cinese. Non sono noti bersagli in Svizzera.

Febbraio: MiniDuke

Sempre nel febbraio del 2013 l'impresa Kaspersky ha pubblicato un rapporto relativo a un attacco raffinato con il software nocivo MiniDuke. Sembra che l'attacco sia stato soprattutto diretto ai danni di strutture statali e di alcuni altri bersagli, situati esclusivamente in Europa. Le vittime sono state infettate tramite *Spear-Phishing* e documenti PDF appositamente predisposti. Una speciale peculiarità di questo attacco consiste nell'utilizzo di conti Twitter come generatori dei *nomi di dominio* dei *server di comando e di controllo*. Allo stato attuale delle conoscenze non sono state colpite infrastrutture in Svizzera.

Giugno: NetTraveler

All'inizio del mese di giugno 2013 l'impresa Kaspersky ha pubblicato dettagli su NetTraveler, una serie di programmi nocivi, utilizzati nel contesto degli attacchi APT. Ne sono state colpite 350 vittime in 40 Paesi, ma al momento non sono noti collegamenti con le infrastrutture svizzere. I bersagli si situavano nei settori dell'industria, dell'energia, della comunicazione, delle nuove tecnologie e del Governo. È interessante il fatto che secondo Kaspersky sei bersagli erano stati colpiti simultaneamente da NetTraveler e Red October. Questa sola constatazione non consente tuttavia di concludere che entrambi gli attacchi siano attribuibili alla medesima paternità o a paternità diverse.

I numerosi rapporti delle imprese di sicurezza, delle vittime o delle autorità hanno posto nuovamente alla ribalta lo spionaggio informatico e gli attacchi APT. Nel caso degli attacchi mirati di spionaggio non si tratta però più di singoli eventi o di singoli complessi di spionaggio. Esiste invece un interesse costante e quindi una pressione costante sui dati sensibili. Anche la Svizzera ne è toccata, proprio perché vi risiedono numerose imprese di punta che possiedono know-how e informazioni di grande valore. Oltre alle misure tecniche usuali e necessarie occorrono tuttavia anche misure organizzative. In linea di massima e a prescindere dagli eventi più recenti, la prevenzione deve inoltre assumere una priorità elevata ed essere effettuata attraverso la sensibilizzazione dei collaboratori, che devono tra l'altro essere istruiti a una manipolazione prudente della posta elettronica.

Gli attacchi possono essere raramente attribuiti a un determinato aggressore. Essi possono tuttavia essere localizzati con relativa precisione dal punto di vista geografico. Che poi lo Stato corrispondente sia responsabile degli attacchi può essere provato senza ombra di dubbio soltanto in rari casi.

È inoltre interessante il fatto che in alcuni di questi attacchi siano state utilizzate infrastrutture note anche nell'ambito di manovre criminali. Sembra che le infrastrutture criminali non siano unicamente utilizzate a fini di arricchimento finanziario, ma intervengano nell'interesse e al soldo di singoli Stati e dello loro mire di spionaggio.

4.3 Il conflitto coreano nel ciberspazio

Nel corso del primo semestre del 2013 si è aggravato il conflitto in Corea. Al seguito di segnalazioni di test con armi nucleari nella Corea del Nord[18] e del successivo inasprimento

[18] http://www.seismologie.bgr.de/sdac/erdbeben/kernexplosion/nkorea_20130212_deu.html (stato: 31 agosto 2013).

delle sanzioni dell'ONU nei suoi confronti, la Corea del Nord ha annunciato di essere ormai in stato di guerra con la Corea del Sud e minacciato per la prima volta gli USA di un attacco nucleare preventivo. Questo focolaio di conflitto comporta anche diverse componenti informatiche. In questo senso l'agenzia ufficiale nordcoreana di stampa KCNA ha rapportato il 14 marzo 2013 un'interruzione locale di Internet in seguito a un attacco informatico nemico. Alcuni giorni dopo si è assistito a un massiccio attacco informatico contro la Corea del Sud, diretto contro tre stazioni televisive sudcoreane e due istituti finanziari. I computer degli interessati non poterono più essere avviati perché i dischi rigidi erano stati cancellati da un software nocivo. Mentre si assisteva al crash dei bancomat, dei *Points of Sale* e del *Mobile Banking* delle banche interessate, il programma televisivo delle emittenti interessate non era limitato. Si sono poi anche constatati deturpamenti di siti Web da parte di un gruppo denominato «Whois Team», che ha reso noto per questo tramite che si trattava dell'inizio delle sue azioni. «I dati sarebbero nelle sue mani, ma cancellati dai computer». Anche un gruppo dal nome «New Romanic Cyber Army» ha affermato di essere il responsabile dell'attacco e di aver rubato informazioni da banche e da compagnie di media. McAfee ha pubblicato in un suo rapporto che questi attacchi erano legati a un'operazione di spionaggio, finora sconosciuta ma attiva fin dal 2009, il cui obiettivo era l'esercito sudcoreano. Questa operazione, dal nome "Operation Troy", aveva lo scopo di scandagliare computer del settore militare utilizzando parole chiave ben determinate[19]. Le azioni di hacktivismo possono quindi ben camuffare operazioni di spionaggio.

Il 25 giugno 2013, il 65° anniversario dell'inizio della guerra di Corea, si è verificato un nuovo attacco – questa volta sotto forma di attacco di DDoS ai danni dei *server DNS* del governo sudcoreano. Successivamente a questo attacco i siti Web ufficiali, tra i quali anche il sito Web della presidenza, non sono più stati raggiungibili. I rappresentanti del movimento Anonymous, designato da più parti come responsabile, si sono distanziati dagli attacchi. Da parte sudcoreana si è accusata la Corea del Nord sia degli attacchi del mese di marzo, sia di quelli del mese di giugno. A titolo di possibile prova sono stati presentati indirizzi IP nordcoreani e campioni di software nocivo[20].

Dopo questo ultimo attacco Symantec ha anche pubblicato un rapporto[21] secondo il quale esisterebbero indicazioni univoche che uno degli *attacchi di DDoS* del 25 giugno 2013 sarebbe in relazione con diversi attacchi degli ultimi quattro anni ai danni della Corea del Sud, quindi anche con gli attacchi del luglio 2009 e del marzo 2011[22], e potrebbe essere attribuito al gruppo «DarkSeoul». Dietro «DarkSeoul» Symantec presume un gruppo di 10-50 persone che, secondo il rapporto precitato, potrebbe essere messo in relazione con il *malware* per e-banking Castov. Il gruppo sarebbe responsabile di altri attacchi ai danni degli USA. L'esperienza insegna che è difficile accertare l'origine di un attacco e attribuirlo possibilmente a un attore statale.

---

19 http://blogs.mcafee.com/mcafee-labs/dissecting-operation-troy-cyberespionage-in-south-korea (stato: 31 agosto 2013).

20 http://www.csoonline.com/article/736531/south-korea-blames-north-korea-for-cyberattacks (stato: 31 agosto 2013).

21 http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war (stato: 31 agosto 2013).

22 Rapporto semestrale MELANI 2009/2, capitolo 4.2: http://www.melani.admin.ch/dokumentation/00123/00124/01109/index.html?lang=de (stato: 31 agosto 2013).

4.4 Hackeraggio del conto Twitter di Associated Press

Dal primo semestre del 2013 la rete sociale Twitter è finita a più riprese nel mirino degli aggressori. Il caso più grave si è verificato il 23 aprile 2013 quando è stato compromesso il conto Twitter di Associated Press (AP). Gli hacker si sono procurati l'accesso al conto Twitter dell'agenzia di stampa AP, pubblicando in suo nome un tweet secondo il quale ci sarebbero state due esplosioni alla Casa Bianca nel corso delle quali il presidente Obama sarebbe stato ferito. Oltre 2 milioni di persone hanno seguito questo tweet. Anche i mercati US ne sono stati influenzati per breve tempo. Nello spazio di tre minuti l'indice statunitense S&P ha subito una perdita di valore temporanea pari a 136.5 miliardi di dollari, riprendendosi poi poco tempo dopo. Sono pure stati hackerati i conti Twitter di BBC, CBS, France 24 TV, Al Jazeera e della National Public Radio (NPR). Il quotidiano britannico «The Guardian» è stato colpito da un attacco di questo genere il 29 aprile 2013. In tale contesto sono state diffuse parole e testi come «Long Live Syria» oppure «The Syrian Electronic Army was here». Sono stati altresì vittima di attacchi la FIFA e il suo presidente Joseph Blatter. Tramite i loro conti è stata diffusa la falsa informazione secondo la quale Blatter si era dimesso dal suo incarico a seguito di accuse di corruzione, per avere ricevuto denaro dall'emiro del Qatar per l'assegnazione dei campionati mondiali di calcio del 2022.

Si presume che dietro a questi attacchi si celi il gruppo «Syrian Electronic Army (SEA)», che si è prefisso di provocare «caos e sofferenze». Dovrebbe risultare chiaro che per questo tramite il gruppo SEA intende essere maggiormente conosciuto. Dal canto suo SEA ha accusato i media occidentali di diffondere «menzogne e gravi calunnie sulla Siria».

Il metodo è sempre lo stesso: gli aggressori inviano e-mail credibili, provviste di link a una pagina infettata, ai titolari di conti Twitter. Il software nocivo installato per questo tramite carpisce il nome di utente e la password, grazie ai quali l'aggressore può effettuare il login e diffondere notizie.

L'influenza dei media sociali sulla diffusione delle informazioni è in continua crescita. La lotta per la concorrenza tra i media ha fatto sì che rimanga sempre meno tempo per verificare le informazioni, soprattutto quando l'informazione sembra provenire da una fonte rinomata. Al riguardo ci si scorda facilmente che i conti Twitter sono unicamente protetti da un nome di utente e da una password. Basta un attacco mirato mediante metodi usuali di *phishing* o di *malware* per accedere alle password. Per questo motivo Twitter ha indirizzato al settore dei media un avvertimento per dire che si presume che tali attacchi perdureranno e saranno in particolare diretti contro media popolari e stimati. Per ridurre il rischio di infezione da malware Twitter raccomanda, oltre alle misure usuali, di utilizzare un computer separato per eliminare i tweet. Inoltre Twitter prende anche in considerazione misure tecniche e pone mano all'introduzione di un'*autentificazione a due fattori*, come quella implementata in ambito di e-banking[23].

False informazioni via Twitter sono possibili anche senza compromissione del conto, come illustrato dall'esempio di Andrea Caroni nel novembre del 2011. Sebbene il consigliere nazionale Caroni non disponesse di alcun conto Twitter, un conto falsificato a suo nome con-

[23] http://www.zdnet.de/88155870/twitter-fuhrt-zwei-faktor-authentifizierung-ein/?ModPagespeed=noscript (stato: 31 agosto 2013).

fermò la rielezione della consigliera federale Eveline Widmer-Schlumpf prima ancora che fosse reso noto il risultato ufficiale[24].

Oltre a tutte le misure tecniche occorrerebbe riflettere e definire preliminarmente le modalità e i canali per il cui tramite una falsa informazione può essere smentita in modo possibilmente efficace, rispettivamente rettificata, per impedire gravi confusioni e altre ripercussioni.

4.5 Sistemi SCADA e sistemi industriali di comando: accessi aperti, lacune di sicurezza, attacchi e protezione

I sistemi di controllo e di comando constano di una o più apparecchiature che comandano, regolano e/o sorvegliano altre apparecchiature o sistemi. Nella produzione industriale il concetto di «sistemi industriali di comando» (inglese: Industrial Control Systems, ICS) è corrente. Da un certo tempo i sistemi industriali di comando e di controllo si ritrovano anche all'infuori dell'industria di produzione, ad esempio in ambito di domotica o di regolazione del traffico. Nel caso di ogni sistema che regola e/o sorveglia un processo fisico si può di norma parlare di sistema industriale di comando. La maggior parte delle regole di base per la protezione dei simili sistemi si applica anche all'infuori della produzione industriale.

Serial-Port Server aperto su Internet

I *Serial-Port Server* offrono il passaggio dalla rete di telecomunicazione alle *interfacce* seriali delle apparecchiature. Dalle indagini condotte dalla ditta HD Moore[25] emerge che su un totale di oltre 100'000 siffatti server è possibile accedere via Internet, senza grandi ostacoli e in una forma o nell'altra, al 10% circa di essi. Ne fanno parte anche diversi impianti – dagli ICS delle caldaie di una birreria ai server *VPN* di un'impresa, ai *contatori smart* di un impianto di regolazione del traffico – i cui accessi aperti offrono un notevole potenziale di utilizzo abusivo.

Numerose apparecchiature comandabili mediante un'interfaccia seriale non necessitano di alcuna ulteriore autentificazione poiché in caso di collegamento fisico via un'interfaccia seriale (collegamento finora effettuato a livello locale) esse presumono che chi è collegato è anche legittimato ad accedere alla configurazione dell'apparecchiatura. Occorre tenere conto di questa circostanza in caso di estensione degli accessi remoti. Gli accessi remoti devono sempre essere protetti dagli utilizzi abusivi. A tale scopo si può ricorrere a tunnel VPN e/o a limitazioni dell'accesso a pochi indirizzi IP conosciuti. Occorre inoltre provvedere affinché l'accesso sia cifrato e che vengano utilizzate soltanto password potenti o *autentificazioni a due fattori*.

Lacuna di sicurezza nei moduli di comando: password leggibili

La microcentrale di cogenerazione «ecoPower 1.0» è un sistema del gruppo Valliant per la produzione di corrente e di calore a uso privato, con motore alimentato a gas. Anche il ri-

[24] Rapporto semestrale MELANI 2011/2, capitolo 3.6: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (stato: 31 agosto 2013).

[25] https://community.rapid7.com/community/metasploit/blog/2013/04/23/serial-offenders-widespread-flaws-in-serial-port-servers (stato: 31 agosto 2013).

scaldamento produce corrente che può essere utilizzata privatamente oppure essere immessa nella rete pubblica. L'impianto è comandato da uno schermo tattile integrato, da un'app per iPad oppure da un'*interfaccia Web*. All'atto dell'implementazione del telecomando via Internet alcuni meccanismi di sicurezza non sono tuttavia stati concepiti in maniera ottimale o sono addirittura assenti. In questo senso una lacuna di sicurezza consente di accedere a tutte le password. Si tratta, oltre che della password di configurazione del proprietario, di tutte le password per il servizio di manutenzione a distanza e addirittura quelle per gli sviluppatori di sistema – che vengono tutte e quante fornite in testo chiaro. Ciò consente a terzi non autorizzati di accedere alla microcentrale, di leggere i dati del suo proprietario e di modificare i parametri di esercizio. Il produttore ne venne informato dopo che l'esercente di una simile apparecchiatura era intervenuto presso gli esperti di sicurezza[26] e che questi ebbero esaminato i problemi. Il produttore raccomandò successivamente per lettera a tutti i clienti interessati di separare i riscaldamenti da Internet, staccando il cavo di rete, finché fossero elaborate soluzioni e che un tecnico di servizio avesse eliminato i problemi sul posto.

Sebbene Valliant abbia dovuto accettare il rimprovero che nonostante tutte le misure di sicurezza i suoi prodotti non potevano essere collegati direttamente a Internet – e non via un tunnel cifrato *VPN* – il problema dovrebbe in particolare essere accollato a Saia-Burgess, il produttore svizzero dei moduli di comando, che risulta responsabile della memorizzazione delle password in testo chiaro e della lacuna di sicurezza che ne consente la lettura. Questi moduli di comando infatti non sono unicamente utilizzati per i riscaldamenti della Valliant, ma anche in diversi altri impianti, in parte grandi e importanti.

Valliant e Saia-Burgess stanno colmando le lacune[27] e hanno pubblicato aggiornamenti corrispondenti[28]. Valliant ha inoltre istituito una hotline per i clienti interessati e installa presso di loro gli aggiornamenti e un box *VPN* per un accesso sicuro. Sono ulteriormente necessari alcuni sforzi finché gli aggiornamenti corrispondenti e misure supplementari di sicurezza saranno implementati su tutti i sistemi interessati.

Questo caso illustra in maniera esemplare la problematica che una società sempre più connessa (e sempre più da una sola rete) deve prendere in considerazione nel suo sviluppo. L'accesso remoto a un'apparecchiatura schiude sia al proprietario che la utilizza che al tecnico di servizio che provvede alla sua manutenzione nuove possibilità e notevoli vantaggi, ma cela anche nuovi bersagli di attacco e rischi corrispondenti. È quindi importante che tutte le imprese coinvolte nella catena di fornitura di un prodotto non considerino con occhio critico la sola convivialità delle nuove apparecchiature, ma che impongano esigenze di sicurezza che vengano integrate nel processo di sviluppo: la sicurezza è un compito comune! Il produttore del modulo di comando raccomanda invero (chiaramente e con forza al più tardi dopo l'incidente descritto qui sopra) di non collegare direttamente a Internet le proprie apparecchiature – ma ciò non lo esime dall'obbligo di fabbricare i propri prodotti in maniera conforme alle esigenze di sicurezza e di fornire se del caso in tempo utile un aggiornamento di sicurezza.

---

[26] http://www.bhkw-infothek.de/nachrichten/18555/2013-04-15-kritische-sicherheitslucke-ermoglicht-fremdzugriff-auf-systemregler-des-vaillant-ecopower-1-0/; http://heise.de/-1840919 (stato: 31 agosto 2013).

[27] http://www.heise.de/newsticker/meldung/Kritisches-Sicherheitsupdate-fuer-200-000-Industriesteuerungen-1934787.html (stato: 31 agosto 2013).

[28] Firmware Update di Saia: http://www.sbc-support.com/de/product-index/firmware-for-pcd-cosinus.html (stato: 31 agosto 2013).

Gli ICS sono in parte collegati alla rete delle telecomunicazioni fin da prima dell'era Internet – perlopiù attraverso una propria connessione telefonica. In genere il produttore/fornitore può se del caso collegarsi a questa connessione a scopi di diagnosi o di servizio, senza doversi recare sul posto. Se per effettuare questi accessi si utilizza ora Internet se ne devono osservare le caratteristiche. Il rischio che qualcuno si avvalga del numero telefonico dell'impianto, forzi una eventuale password e possa comprendere il protocollo di comando, generalmente proprietario, va considerato minore rispetto a quello di chi può rintracciare un impianto in Internet avvalendosi di uno speciale motore di ricerca[29] e può scandagliare i relativi server Web con tool standard alla ricerca di lacune di sicurezza. Ove subentri la necessità di comandare a distanza simili sistemi, ciò è ad esempio possibile via un tunnel *VPN* cifrato con una potente autentificazione.

Il turbine sollevato sui comandi vulnerabili ha anche un aspetto positivo: il tema della sicurezza è ora discusso attivamente nel ramo settoriale.

Attacco ai sistemi industriali di comando (ICS)

Kyle Wilhoit, un ricercatore della Trend Micro, ha studiato per un lungo periodo di tempo[30] gli attacchi agli ICS con l'ausilio di *Honeypot*, constatando in tal modo che sono continuamente in atto attacchi automatizzati e semiautomatizzati agli ICS.

Al riguardo sono state raccolte le seguenti informazioni:

- Oltre 16'00 attacchi automatizzati sull'arco di 5 mesi, provenienti da 605 diversi *indirizzi IP*. Non vi sono compresi gli attacchi che non avevano niente a che fare con gli ICS.

- Sono stati constatati tra l'altro i seguenti attacchi:
  - tentativo di accesso alle pagine di diagnosi dei sistemi simulati;
  - tentativo di accesso e modifica di *Modbus/DNP3* Traffic;
  - tentativi di modifica del sistema (simulato) di pompa;
  - tentativi di accesso a settori protetti;
  - accessi non autorizzati di lettura/scrittura su *PLC*[31].

- Contro uno degli indirizzi e-mail pubblicati sull'Honeypot sono stati osservati attacchi mirati con malware. L'aggressore ha tentato in questo modo di derubare dati utili in vista di attacchi più ampi (informazioni sulle configurazioni *VPN*, parametri di rete, nonché banca dati delle password di Windows).

Dall'analisi di Kyle Wilhoit emerge che gli ICS collegati a Internet sono regolarmente oggetto di attacchi, questo a prescindere dalla loro appartenenza o no a impianti conosciuti e partico-

---

29 Cfr. ad esempio il motore di ricerca Shodan: http://www.shodanhq.com (stato: 31 agosto 2013).

30 Trendmicro: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf e Blackhat: https://media.blackhat.com/us-13/US-13-Wilhoit-The-SCADA-That-Didnt-Cry-Wolf-Whos-Really-Attacking-Your-ICS-Devices-Slides.pdf (stato: 31 agosto 2013).

31 PLC significa controllore logico programmabile, utilizzato per comandare un impianto. PLC è l'abbreviazione dell'espressione inglese corrispondente (Programmable Logic Controller).

larmente esposti. Per questo motivo gli ICS non devono in nessun caso essere collegati a Internet senza meccanismi supplementari di protezione.

Cosa bisogna fare per proteggere i sistemi industriali di comando (ICS)?

SANS[32], un istituto di sicurezza degli USA, ha pubblicato i 20 elementi chiave[33] con i quali sono generalmente protette le infrastrutture TIC. Questi elementi possono in parte essere applicati anche agli ICS. Ulteriori raccomandazioni sono emesse dall'US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT[34]), come pure dal National Institute of Standards and Technology (NIST[35]).

Le seguenti 11 raccomandazioni di sicurezza poggiano su questi documenti. Spiegazioni dettagliate in merito figurano sul sito Web di MELANI[36].

1. Allestite e curate una banca dati Asset di tutte le apparecchiature
2. Allestite un Life Cycle e Patchmanagement per il software
3. Definite e utilizzate configurazioni sicure
4. Pianificate ed edificate architetture di rete robuste
5. Implementate una protezione malware a più livelli
6. Autentificazione e autorizzazione
7. Istituite una valutazione centrale dei log
8. Garantite la protezione fisica
9. Eseguite Backup e Recovery ed effettuatene test regolari
10. Istituite processi di Security Incident Management ed esercitateli
11. Istituite una cultura della sicurezza

È importante capire che nella maggior parte dei casi la sicurezza non è fulminea, né può essere garantita con un'azione unica, bensì che i miglioramenti costituiscono un processo costante che non prende mai fine. In questo senso occorre stabilire obiettivi sensati, realistici e raggiungibili ed elaborare anzitutto i punti che consentono di elevare sensibilmente la sicurezza con un dispendio relativamente esiguo, ad esempio modificare tutte le password per difetto e proteggere le interfacce di comando raggiungibili dall'esterno.

Se nei sistemi infornatici classici la disponibilità, la confidenzialità e l'integrità hanno valori posizionali pressoché identici, nel caso degli ICS figura al centro la disponibilità. La protezione della confidenzialità e dell'integrità serve anch'essa a mantenere la disponibilità. In questo

[32] SANS, http://www.sans.org (stato: 31 agosto 2013).
[33] SANS Top 20 Critical Security Controls: http://www.sans.org/critical-security-controls/ (Stand: 31. August 2013).
[34] ICS CERT: http://ics-cert.us-cert.gov/ (stato: 31 agosto 2013).
[35] NIST: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf (stato: 31 agosto 2013).
[36] Liste di controllo e guide: http://www.melani.admin.ch/dienstleistungen/00132/index.html?lang=it (stato: 31 agosto 2013).

senso un sistema che comunica attraverso un protocollo e che tutela la confidenzialità e l'integrità dei dati trasmessi è meglio protetto contro gli attacchi e può quindi raggiungere una maggiore disponibilità.

4.6 Avarie di software e loro ripercussioni

Errore nel sistema di prenotazione – Soppressione di numerosi voli di American Airlines

La mattina del 16 aprile 2013 un errore informatico nel sistema di prenotazione di American Airlines ha provocato un crash. Successivamente non è più stato possibile approntare alcun aereo per diverse ore. I sistemi hanno potuto essere riavviati soltanto nel pomeriggio. Sono stati complessivamente soppressi 700 voli, mentre numerosi altri voli sono rimasti ritardati. La American Airlines opera quotidianamente 3'400 voli [37]. L'origine di questa avaria non è stata comunicata.

Questo esempio illustra che non solo le avarie dei sistemi SCADA e dei sistemi industriali di comando possono provocare crash di infrastrutture critiche. È soprattutto quando sono in gioco processi fisici sulla disponibilità (di banche) di dati che i problemi corrispondenti possono provocare serie ripercussioni.

Chrysler richiama centinaia di migliaia di veicoli fuoristrada a causa di un errore di software

Le operazioni di richiamo non sono un fatto straordinario nel settore dell'automobile. Esse hanno sempre più frequentemente a che fare con errori di software. Nel maggio del 2013 ad esempio Chrysler ha richiamato oltre 400'000 veicoli fuoristrada a causa di un errore di software. In alcuni veicoli il passaggio delle marce era spostato involontariamente dal software, circostanza che nella peggiore delle ipotesi poteva provocare un incidente.

Nei veicoli moderni un numero sempre maggiore di funzioni è pilotato mediante software ed è quindi solo una questione di tempo finché appariranno con maggiore frequenza errori di software anche nelle automobili.

4.7 Operazioni, incriminazioni e arresti nei confronti di cibercriminali

Nel corso del primo semestre del 2013 si sono verificate numerose operazioni di polizia, arresti e condanne nei confronti di cibercriminali.

[37] http://www.handelszeitung.ch/news/peinlicher-computerfehler-american-airlines-kann-nicht-fliegen (stato: 31 agosto 2013).

DDoS: Operazione Payback

Nel gennaio del 2013 la giustizia britannica ha condannato Christopher Weatherhead del movimento Anonymous a 18 mesi di carcere per il suo ruolo nell'operazione Payback[38] ai danni di Paypal, Mastercard e Visa. Le condanne pronunciate nei confronti di altri attivisti di Anonymous sono state più blande. Il giudice ha ritenuto che Weatherhead avesse svolto un ruolo principale nell'organizzazione.

Malware ai danni dell'e-banking

Sempre nel gennaio del 2013 la giustizia statunitense ha sporto querela contro tre persone accusate di essere gli autori e di avere distribuito il *malware* Gozi ai danni dell'e-banking. Si presume che Gozi abbia infettato oltre un milione di PC nel mondo intero e provocato danni dell'ordine dei milioni.

Ransomware: Reveton

Nel febbraio del 2013 la polizia spagnola ha arrestato diversi autori e distributori del *ransomware* Reveton, fra i quali il capo presunto del gruppo criminale. Il software nocivo Reveton blocca il PC infettato e visualizza sullo schermo un presunto messaggio della polizia che incolpa la vittima di diversi reati. A condizione che venga pagata una determinata somma il perseguimento penale è dirottato e il PC è sbloccato. Il ransomware è stato adeguato ai singoli Paesi e ha colpito numerosi PC in quasi 30 Stati, fra i quali anche computer situati in Svizzera (cfr. in merito il rapporto semestrale MELANI 2012/I[39]). Gli arresti sono stati effettuati grazie alla collaborazione tra la polizia spagnola, Europol, Interpol e l'impresa di sicurezza Internet Trend Micro. Reveton e le sue diverse varianti sono tuttavia ulteriormente attivi, anche in Svizzera.

Rete bot: Citadel

Il Federal Bureau of Investigation (FBI) statunitense e l'impresa Microsoft hanno disattivato nel corso di un'azione comune, resa pubblica il 6 giugno 2013, oltre 1'400 server sfruttati da Citadel. Questo *software nocivo* di ampia diffusione esiste dal 2011 ed è destinato alle truffe in ambito di e-banking, anche in Svizzera. Secondo Microsoft Citadel è responsabile di perdite dell'ordine di 500 milioni di dollari ai danni dei clienti di numerosi istituti finanziari. Citadel è un software personalizzabile ai danni dell'e-banking, ottenibile sul mercato sotterraneo di Internet e utilizzato da numerosi gruppi criminali.

L'FBI e Microsoft hanno condotto l'azione denominata «b54» in collaborazione con gli istituti finanziari e le autorità di perseguimento penale di diversi Paesi. I *server di comando e di controllo* disattivati erano stati utilizzati per il comando e la gestione della rete bot. L'FBI ricerca in questo contesto una persona chiamata Aquabox e sospettata di essere l'autore del software nocivo.

---

[38] Rapporto semestrale MELANI 2010/2, capitolo 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=de (stato: 31 agosto 2013).

[39] Rapporto semestrale MELANI 2012/1, capitolo 3.3: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=de (stato: 31 agosto 2013).

L'operazione «b54» disturberà indubbiamente i buoni affari di diversi gruppi criminali che utilizzano Citadel. È tuttavia poco probabile che questa operazione abbia ripercussioni che durino nel tempo. Nemmeno l'esistenza del software nocivo dovrebbe essere pregiudicata. La capacità del software nocivo e delle reti bot di rigenerarsi dopo simili azioni si è già manifestata in passato. È addirittura possibile integrarvi nuove funzioni, rendendo in tal modo più difficile rintracciare il software nocivo e renderlo innocuo

4.8 Quarto esercizio internazionale Cyberstorm

Il 20 e 21 marzo 2013 si è svolto il quarto esercizio internazionale Cyberstorm. Nel suo contesto gli Stati membri dell'International Watch and Warning Networks (IWWN), fra i quali la Svizzera, testano la loro collaborazione e la loro capacità di reazione in caso di attacco informatico.

Cyberstrom è un esercizio informatico internazionale iniziato dagli USA e in particolare dal Department of Homeland Security per testare la capacità di reazione in caso di incidenti informatici. L'esercizio è prevalentemente orientato sugli USA e le loro organizzazioni di sicurezza, ma dispone di una componente internazionale fin dalla sua prima edizione. Il primo esercizio di questo genere si è svolto nel 2006. In maniera analoga all'esercizio informatico Cyber Europe 2012, nel caso «Cyberstorm IV» è stata verificata l'efficacia delle cosiddette Standard Operating Procedures (SOP). Le SOP disciplinano la presa di contatto, lo scambio di informazioni e la collaborazione in caso di incidente informatico internazionale.

Lo scenario d'esercizio di quest'anno presumeva l'infezione di grandi portali mediatici e di calcolatori dell'amministrazione, nonché un deflusso di dati verso server esteri. La complessità dell'esercizio, durato oltre 32 ore, ha consentito di testare la cooperazione tra i partecipanti. Sono stati complessivamente simulati 300 eventi.

Gli incidenti in ambito informatico sono praticamente sempre transfrontalieri. Occorre pertanto un approccio internazionale comune per poter affrontare in maniera efficace le crisi informatiche. L'esercizio ha evidenziato che lo scambio di informazioni a livello tecnico e operativo tra i Paesi è buono e funziona in modo efficiente. Costituisce poi in particolare una sfida la valutazione dei numerosi dati disponibili affinché in caso di emergenza possa essere effettuata, come base per i decisori, un'analisi della situazione contenente tutte le informazioni rilevanti.

5 Tendenze / Prospettive

5.1 Stati, economia e diritto

Ogni impresa, sia che essa operi sul mercato nazionale oppure a livello internazionale, sottostà alla legislazione del pertinente Stato nel quale è attiva. Al riguardo assume una particolare importanza il luogo delle sede principale. Lì vi è situata la direzione e con essa tipicamente l'ultima istanza decisionale e – a seconda del genere di attività – il luogo principale della produzione, della logistica e dell'amministrazione e delle informazioni rilevanti ai fini dell'attività.

Questa ferrea norma di base si applica nella medesima misura al fabbricate di macchine e alla catena di fast-food, come pure alle grandi imprese che con i loro prodotti e prestazioni di servizi forniscono le fondamenta e le infrastrutture di base della messa in rete mondiale. Va poi da sé che fra tutte le norme nazionali di diritto applicabili si trovino anche leggi in ambito di sicurezza che possono sopprimere la protezione dei dati in caso di perseguimento penale o di sospetto di attività terroristiche. È in genere accettato il fatto che le imprese tecniche altamente specializzate debbano rendere pubbliche alle autorità di controllo determinate operazioni estere per evitare esportazioni di beni a doppio uso a destinazione di Paesi che non si attengono ai diritti fondamentali dell'uomo. Il problema principale risiede meno nel senso e nell'orientamento, ma piuttosto nelle ripercussioni e nell'applicazione della legge.

Nel caso degli offerenti di tecnologie di informazione e di comunicazione si unisce a questa logica un ulteriore elemento di inasprimento: la stragrande maggioranza degli offerenti di tecnologie di informazione e di comunicazione – che si tratti di produttori di software o di hardware, di offerenti di *cloud* o di servizi di trasmissione dei dati – hanno la loro sede principale negli USA e sottostanno pertanto primariamente alla legislazione e alla giurisprudenza statunitensi. La centralizzazione della forza di mercato di un ramo settoriale in un Paese determina anche una concentrazione delle possibilità di un solo Stato di accedere agli offerenti di infrastrutture di base della rete mondiale in virtù della propria legislazione. Sembra chiaro che in un simile caso l'applicazione di leggi nazionali abbia sempre una ripercussione globale. Visto in questo senso gli USA dispongono de facto, nel settore delle imprese TIC e del loro ruolo come motori e fautori della messa in rete globale, di una posizione unipolare ed egemonistica nel mondo. Si potrebbe invero obiettare che in ambito di produzione di elementi di hardware anche la Cina accumula in suo seno una forza di mercato schiacciante – parola chiave Supply Chain. In futuro proprio questo tema comporterà la necessità di alcuni chiarimenti. Infatti la gestione finale di questo hardware all'esterno della Cina, lo sviluppo di firmware che comanda queste componenti ecc. non è sovente in mani cinesi. Con riguardo specialmente agli offerenti di motori di ricerca, alle soluzioni di posta elettronica o ai media sociali, la Cina persegue soluzioni locali che non comportano quindi implicazioni globali e non entrano in concorrenza con la posizione di egemonia delle imprese di questo settore situate negli USA.

Dal punto di vista della politica di sicurezza, nel corso della storia le posizioni di egemonia hanno sempre comportato un strascico di questioni scabrose per gli altri Stati, la loro economia e la loro popolazione. Intorno al nocciolo di questa problematica ruota sempre la questione della misura in cui un egemone è disposto a cessare la propria dominanza sugli altri, rispettivamente se l'egemone è in chiaro sulla propria predominanza e sulle implicazioni globali che ne derivano. Tutte queste questioni riguardano in definitiva la prevedibilità dell'egemone nel senso di una protezione contro l'arbitrio, rispettivamente l'abuso di potere, ciò che costituisce un importate fattore degli altri Stati nei loro rapporti con l'egemone. Questa prevedibilità costituisce in definiva il fondamento (nel senso di una certezza di pianificazione e di diritto) dell'economia nelle sue relazioni con i partner indispensabili a livello di influsso legale sull'egemone.

Dovrebbe essere nell'interesse di ogni Stato che dispone di una simile egemonia chiarire presto e definitivamente queste questioni. In merito non si tratta di un problema di sovranità legale, ma anzitutto di chiarire (politicamente) quali obiettivi persegue con la sua legge e come intende emanarla e applicarla a favore dei propri interessi (personali) a spese degli interessi esteri. In altri termini in quale misura intende perseguire – nel quadro del proprio ordinamento giuridico e quindi influenzando l'industria nazionale (se del caso attiva a livello globale) – i propri interessi di strategia politica (e possibilmente economica) a scapito degli altri Stati oppure rinunciarvi esplicitamente. È però anche compito della comunità internazionale degli Stati lanciare il dibattito internazionale su queste questioni e ricercare un chiari-

mento nell'una o nell'altra direzione. La Svizzera è attiva al riguardo nel quadro di forum multilaterali e bilaterali.

La conseguenza immancabile di una fase di incertezza e di imprevedibilità che perdurasse nel tempo sarebbe che gli Stati dovrebbero ricorrere a soluzioni TIC proprie e indipendenti, questo non nel quadro del concorso sportivo di economia di mercato, ma come strumento di politica di sicurezza e come demarcazione nei confronti dei prodotti del Paese egemone. Il fatto che il tutto sia vincolato a inefficienze e costi inopportuni per l'economia e specialmente per le infrastrutture critiche è ovvio, ragione per la quale ciò dovrebbe sempre essere la peggiore delle soluzioni.

La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) propugna da sempre un approccio basato sul rischio in ambito di sicurezza dell'informazione e di protezione delle infrastrutture TIC, approccio che è ora stato integrato nella «Strategia nazionale per la protezione della Svizzera contro i rischi informatici (NCS)», questo al posto di un approccio meramente tecnico, basato sulle possibilità TIC. Alternative in merito nel campo dei prodotti router e dei programmi di economia di mercato indotti in questo settore, all'infuori degli USA e della Cina, esistono già attualmente e sono anche utilizzate[40].

Affinché l'approccio di questi rischi informatici possa poi anche riuscire è essenziale che la minaccia possa essere valutata e compresa nella sue molteplici sfaccettature. In questo ambito svolgono un ruolo non soltanto gli attori, le vulnerabilità tecniche e le più recenti conoscenze in merito agli incidenti, ma anche fattori non tecnici nel settore della struttura fisica, personale e organizzativa, come pure delle condizioni quadro legali e degli interventi sovrani nel Paese del fabbricante del prodotto, degli offerenti di prestazioni di servizi e delle memorie di dati utilizzate. Al riguardo ogni impresa deve essere lasciata libera di ponderare in maniera più o meno forte i fattori di rischio che corrispondono al meglio al suo profilo, ai suoi processi critici e alla sua possibilità di esposizione all'estero, nonché alla sua attività.

Per offrire in questo settore un più forte sostegno alle imprese e specialmente alle infrastrutture critiche si è provveduto – nel quadro della «Strategia nazionale per la protezione della Svizzera contro i rischi informatici (NCS)» – a potenziare le risorse che devono assicurare le posizioni della Svizzera e della sua economia nel settore internazionale della politica di sicurezza, questo oltre a un rafforzamento di MELANI fino al 2017.

5.2 Manuale di Tallinn

Nel marzo del 2013 è stato pubblicato il «Manuale di Tallin» (titolo originale: Tallinn Manual on the International Law Applicable to Cyber Warfare)[41]. Si tratta nella fattispecie di uno studio sulle modalità con le quali il diritto internazionale – in particolare il «diritto di fare la guerra» (ius ad bellum) e il diritto internazionale umanitario («diritto nella guerra», ius in bello) – possa trovare applicazione nelle operazioni informatiche.

---

[40] http://www.fp7-ofelia.eu/about-ofelia/ (stato: 31 agosto 2013).
http://www.change-project.eu (stato: 31 agosto 2013).
http://www.openflow.org/wk/index.php/MPLS_with_OpenFlow/SDN (stato: 31 agosto 2013).
http://www.heise.de/ix/artikel/Alles-fliesst-1643457.html (stato: 31 agosto 2013).

[41] http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381 (stato: 31 agosto 2013).

Il Manuale di Tallinn analizza tra l'altro nel quadro del commento di 95 norme questioni di sovranità nazionale, di giurisdizione e di responsabilità, come pure implicazioni del diritto di neutralità. Si ricerca a quale momento uno hacker civile può essere considerato un partecipante attivo alla guerra («combattente»), divenendo un bersaglio legittimo di attacco, rispettivamente in quale misura le sue attività possono essere attribuite a uno Stato. Sono inoltre tematizzati la protezione delle infrastrutture critiche civili, nonché gli attacchi a centrali nucleari e dighe di sbarramento[42].

Il manuale è stato elaborato tra il 2009 e il 2012 da un gruppo internazionale di circa 20 esperti di diversi settori su invito del NATO Cooperative Cyber Defence Center of Excellence con sede a Tallinn, la capitale dell'Estonia. Non si tratta di un documento ufficiale della NATO, bensì di una pubblicazione accademica, non giuridicamente vincolante, che illustra approcci e pareri (in parte discordanti) sulle modalità con le quali il diritto internazionale potrebbe essere applicato al nuovo contesto «ciber». Dato che si tratta di una prima pubblicazione completa in questo settore, ci si deve aspettare che nonostante il suo carattere non ufficiale diversi Stati e organizzazioni osservino i pareri che vi sono rappresentati nella formulazione delle loro posizioni e dei loro manuali.

5.3 Prossimo alla fine il supporto a Microsoft Windows XP SP3 e a Microsoft Office 2003

L'8 aprile 2014 prende fine il supporto a Microsoft Windows XP SP3 e a Microsoft Office 2003. A tutte le imprese che lavorano con queste versioni si raccomanda urgentemente un aggiornamento alle più recenti versioni ulteriormente supportate del sistema operativo e del software.

Dopo l'8 aprile 2014 non saranno più liberamente disponibili presso il produttore supporto, *patch* di sicurezza o eliminazioni dei problemi per Windows XP SP3 e Office 2003. Le vulnerabilità dei sistemi operativi e delle applicazioni non più supportati non saranno soppresse, circostanza che potrebbe essere sfruttata in maniera mirata per attacchi informatici ai computer sui quali girerebbero ulteriormente Windows XP SP 3 e/o Office 2003. Le chance di riuscita di simili attacchi aumentano, mentre cresce in maniera corrispondente il rischio di sicurezza nel caso degli utenti che utilizzano le vecchie versioni.

Le più recenti versioni del software offrono miglioramenti in ambito di sicurezza perché contemplano le più attuali tecnologie di sicurezza. Il produttore elimina inoltre ulteriormente le vulnerabilità che vengono rese note. L'utilizzazione del sistema operativo e del software più recenti è il mezzo più efficace in ambito di sicurezza, a parte la gestione dei *patch*.

Alle imprese che non possono effettuare l'aggiornamento entro l'8 aprile 2014 rimane la possibilità di concludere un contratto di servizio di supporto con Microsoft. I costi del servizio di supporto sono sensibilmente superiori a quelli del supporto normale e aumentano successivamente. Anche chi opta a favore del servizio di supporto deve presentare come parte del contratto con Microsoft un piano di passaggio da Windows XP SP3 e Office 2003 ai prodotti più recenti.

[42] http://ccdcoe.org/249.html (stato: 31 agosto 2013).

Il supporto di Microsoft Exchange Server 2003 e Microsoft Office SharePoint Server 2003 prende anch'esso fine l'8 aprile 2014[43].

5.4 Problematica del Content Management System (CMS)

Nel corso degli ultimi anni il numero di siti Web su Internet è pressoché esploso. Questo tra l'altro per il motivo che anche utenti senza dimestichezza con la tecnica possono aprire un sito Web su Internet facendo capo a strumenti di facile utilizzazione e grazie a prezzi sempre più bassi. A tale scopo si ricorre sovente ai cosiddetti *Content Management Systems (abbr. CMS*), per il tramite dei quali un sito Web può essere creato e messo su Internet in un paio di clic e senza conoscenze approfondite del Webdesign. Attualmente esistono dozzine di simili CMS che possono essere utilizzati dai gestori per hobby di siti Web e dai criminali informatici. La diffusione crescente di simili sistemi li rende interessanti anche per i cibercriminali, che profondono tanto più energia e denaro nelle lacune di sicurezza quanto più un software è diffuso e offre un numero corrispondentemente maggiore di possibili bersagli di attacco. Non soltanto i CMS, ma ogni software ha lacune potenziali di sicurezza – non esiste alcun software la cui sicurezza sia garantita. Gli sviluppatori di software implementano inoltre sempre nuove funzionalità. Ogni riga supplementare di codice non dota soltanto il software di nuove funzioni, ma ne accresce la complessità e quindi il rischio che comporti da qualche parte una lacuna di sicurezza.

Generalmente le lacune di sicurezza non rimangono a lungo nascoste agli sviluppatori di software e sovente trascorrono pochi giorni dalla scoperta di una lacuna di sicurezza fino alla fornitura di un aggiornamento di sicurezza corrispondente da parte del produttore, destinato appunto a eliminare tale lacuna di sicurezza. Dato che simili aggiornamenti di sicurezza non sono installati automaticamente sul sistema si richiede l'azione del gestore del sito Web. Poiché nel frattempo numerosi siti Web sono gestiti da laici in materia tecnica – ossia da persone alle quali è stata agevolata la creazione di un sito Web, ma alle quali non sono state spiegate le misure necessarie a una manutenzione sicura del sito – esiste un numero corrispondentemente grande di siti Web che utilizzano un CMS che non è stato aggiornato da mesi, se non da anni, e che presentano a seconda delle circostanze dozzine di (note) lacune di sicurezza.

Siffatti siti Web vulnerabili possono essere rintracciati e attaccati da corrispondenti tool automatizzati. Per i criminali è relativamente facile manipolare un grande numero di siti Web in modo da infettare con software nocivo i loro visitatori.

Gli attacchi ai CMS possono essere ridotti in misura massiccia grazie a *patch* corrispondenti (effettuazione attuale degli aggiornamenti di sicurezza). Esiste nondimeno tutta una serie di misure ulteriori per contribuire alla sicurezza dei CMS. Troverete spiegazioni sulle misure elencate sul sito Web di MELANI sotto «Liste di controllo e guide»[44].

---

[43] Indicazioni precise sul MS Support Lifecycle: http://support.microsoft.com/lifecycle (stato: 31 agosto 2013). Indicazioni precise sulla fine del supporto di Windows XP SP3 und Office 2003: http://www.microsoft.com/endofsupport (stato: 31 agosto 2013).

[44] Liste di controllo e guide: http://www.melani.admin.ch/dienstleistungen/00132/index.html?lang=it (stato: 31 agosto 2013).

1. Effettuazione attuale degli aggiornamenti di sicurezza
2. Autenticazione a due fattori
3. Limitazione degli accessi di amministratore a determinati indirizzi IP
4. Limitazione degli accessi di amministratore mediante file .htaccess
5. Securizzazione del computer del Webmaster
6. Web Application Firewall
7. Individuazione tempestiva delle lacune di sicurezza

5.5 Dove ci si incontra (e ci si infetta) – la pozza d'acqua

Nelle regioni aride tutti gli animali si ritrovano prima o poi alla pozza d'acqua per bere. Questo fenomeno dà il proprio nome a un tipo di attacco sempre più osservato negli ultimi tempi: l'«attacco pozza d'acqua» (inglese *Watering-Hole Attack*). Anche in Internet esistono posti dove gli utenti si soffermano regolarmente, non per procurarsi cibo e bevande, ma per procacciarsi informazioni. Se i motori di ricerca, i portali di informazioni e le reti sociali attirano un grande numero di persone, esistono anche siti Web di offerenti specializzati in temi di informazione regolarmente visitati da utenti che manifestano interessi corrispondenti. Questa circostanza può essere sfruttata da un aggressore che prende di mira determinati gruppi professionali o di interessi. Posto che possa hackerare un simile sito Web e collocarvi *software nocivo* gli si presenterà un pubblico mirato.

Nella primavera del 2013 ad esempio il sito Web del Ministero statunitense del lavoro è stato hackerato e vi è stata collocata un'infezione *drive-by* che sfruttava una lacuna di sicurezza fino ad allora sconosciuta di Internet Explorer 8. Sul sito in questione gli impiegati dei gruppi energetici possono informarsi sui programmi di indennità dopo essere stati in contatto con l'uranio. I computer degli interessati che hanno acceduto a questa pagina sono stati infettati da un programma di spionaggio. Questo collocamento mirato lascia presumere che gli aggressori abbiano preso di mira persone del settore dell'energia – in particolare dell'energia nucleare – e collaboratori del Governo in questo settore. Sono anche prese di mira dagli aggressori le persone che lavorano con armi nucleari.

Nel corso del periodo in esame sono aumentate le comunicazioni relative a simili attacchi di Watering-Hole. Rispetto alle infezioni drive-by usuali – nel cui ambito i criminali colpiscono indiscriminatamente siti Web mal protetti in vista della diffusione del loro software nocivo su qualsiasi computer – nel caso degli attacchi di Watering-Hole si pone in atto un dispendio maggiore per hackerare siti Web specifici a prescindere dalla sicurezza esistente.

Sebbene questi attacchi siano diretti primariamente contro i computer d'ufficio, a seconda dell'impresa colpita è possibile procurarsi, oltre a segreti aziendali, anche altre informazioni degne di protezione (piani di rete, indirizzi e dati di accesso ai sistemi di controllo ecc.), utilizzabili per altri ulteriori attacchi. Gli hacker possono accedere anche da sistema a sistema a una rete aziendale non sufficientemente segmentata, fino a raggiungere il sistema di controllo che comanda i processi fisici per poterlo manipolare.

Prima o poi una *lacuna di sicurezza* appare in ogni browser. Il capitolo 5.1 del rapporto semestrale MELANI 2012/2[45] illustra le possibilità di riduzione dei rischi quando divengono note lacune di sicurezza dei browser. Esiste tuttavia sempre la possibilità che vengano perpetrati attacchi di Watering-Hole attraverso lacune di sicurezza (anche *plug-in*) non ancora note a quel momento.

5.6 Cavalli di Troia per Smartphone

Nel corso dell'ultimo semestre è proseguita la tendenza del software nocivo per smartphone, con una forte progressione negli ultimi mesi. Tale tendenza si accentra soprattutto sul sistema operativo Android. Ne è motivo la forte diffusione di Android, la sua struttura aperta già oggetto di discussione nell'ultimo rapporto semestrale[46], ma anche il fatto che numerosi produttori di aggiornamenti di sicurezza non li forniscano oppure solo molto tempo dopo la notizia della lacuna di sicurezza.

I bersagli degli aggressori sono molto diversi:

- Attacchi ai conti bancari: furto di *mTAN*
- Invio di SMS a pagamento
- Attacchi ad applicazioni mobili di Micropayment
- Furto di dati di accesso alle reti sociali e ai conti di posta elettronica
- Dati di indirizzo: nomi, numeri di telefono, indirizzi e-mail e date di nascita dei contatti
- Furto di identità
- Furto generico di dati

Molto sovente si utilizzano componenti di social engineering per la diffusione di malware. In questo senso ad esempio note app sono «troianizzate» e messe in circolazione per il tramite di app store non ufficiali. In precedenza vengono inviate e-mail con link corrispondenti, ad esempio e-mail falsificate di una banca che informano in merito alla nuova app necessaria per effettuare il banking online. Sono parimenti state osservate *infezioni drive-by* nel cui ambito basta in genere visitare un sito Web per infettare il dispositivo. Una nuova dimensione verrà raggiunta con la creazione della prima rete bot composta esclusivamente da dispostivi Android. Essa sarà ad esempio utilizzata per l'invio di e-mail di spam.

È interessante il fatto che gran parte del *malware* in circolazione poggi sul medesimo codice di base. È stata ad esempio rintracciata una biblioteca (libvadgo) in diverse varianti di malware, destinata alla comunicazione con i *Command and Control Server.* Questa biblioteca può inoltre nascondersi ai tool di analisi, nel senso che termina diversi processi o manipola determinati comandi.

---

[45] Rapporto semestrale MELANI 2012/2, capitolo 5.1: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=de (stato: 31 agosto 2013).

[46] Rapporto semestrale MELANI 2012/2, capitolo 4.8: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=de (stato: 31 agosto 2013).

La maggior parte del malware per dispositivi mobili è al momento scritta per Android. Ma anche le altre piattaforme sono attaccabili. Se si tratta di perpetrare attacchi ai danni di determinate imprese o persone anche un iPhone un Windows-Phone costituiscono una zona di attacco analoga a un dispositivo Android. I dispositivi mobili – in particolare nel caso di ambienti altrimenti ben securizzati – possono fungere da portone di entrata per penetrare nelle reti interne. Questa problematica deve in particolare essere presa in considerazione nei progetti *Bring Your Own Device (BYOD)*.

MELANI raccomanda le seguenti norme di comportamento per utilizzare i dispositivi mobili in maniera sicura:

1. Inserite correttamente i meccanismi di sicurezza del vostro smartphone (p.es. immissione del PIN e bloccaggio automatico dello schermo).
2. Installate unicamente applicazioni provenienti da app store ufficiali. Confrontate su di essi le valutazioni e le comunicazioni degli utenti. Non installate mai applicazioni via link di e-mail.
3. Prima di un'installazione verificate i diritti che esige l'applicazione e chiedetevi se essi siano effettivamente necessari, rispettivamente se intendete concederli (p. es. accesso ai contatti o lettura o invio di SMS). In caso di dubbio rinunciate preferibilmente all'installazione.
4. Siate prudenti nell'utilizzazione di hotspot WiFi sconosciuti. Configurate il vostro smartphone in maniera che non si colleghi automaticamente a nuove reti wireless.
5. Dispositivi Android a contare dalla versione 4.2: Sincerateví che il servizio reputazione di Google sia attivo; esso protegge il vostro dispositivo da minacce sconosciute (app maligne). Questo servizio può essere configurato nella rubrica di menu «Confermare app». Il parametro «Verificare app» deve essere attivato.
6. Dispositivi Android: Sincerateví che l'installazione di app sia consentita soltanto a partire dal Google Play Store ufficiale (deve essere disattivata l'opzione «Fonti sconosciute» del parametro di configurazione -> Sicurezza -> Gestione del dispositivo).

Nell'allegato 7.1 è pubblicata un'analisi dei cavalli di Troia per Android apparsi in Svizzera nel corso del primo semestre del 2013.

5.7 Utilizzo abusivo e attacco ai danni della telefonia in Internet (VoIP)

I rischi nell'utilizzazione delle tecnologie VoIP e le possibilità di utilizzo abusivo riguardano sia le persone private che le imprese. Il potenziale di danno dell'utilizzo abusivo di una infrastruttura VoIP è tuttavia molto più grande nel caso delle imprese. In definitiva i vantaggi incontestabili della telefonia VoIP vanno sempre ponderati con i possibili inconvenienti in ambito di sicurezza. Attualmente le truffe perpetrate integralmente o parzialmente mediante il telefono sfruttano in ampia misura la tecnologia VoIP. Il capitolo 3.6 descrive un evento che si è verificato in Svizzera. Ulteriori tipi di attacco sono descritti qui sotto:

Attacco alla disponibilità (Telephony Denial of Service)

All'inizio del 2013 le autorità statunitensi hanno segnalato il pericolo di attacchi di *Telephony Denial of Service*, ovvero di attacchi alla disponibilità dei servizi telefonici. Nel loro contesto una centrale telefonica viene sommersa di chiamate affinché non possa più essere raggiun-

ta. Queste chiamate sono automatizzate da un impianto VoIP (compromesso) ed effettuate senza grandi costi. Nella maggior parte dei casi un simile attacco è accompagnato da una richiesta di denaro. Il gestore della linea deve pagare una determinata somma per fare cessare l'attacco. Il fenomeno è particolarmente preoccupante se concerne servizi pubblici, segnatamente i numeri di emergenza medica.

Spionaggio

Nel contesto della telefonia VoIP le conversazioni sono convertite in dati digitali. In maniera analoga a quanto avviene nel caso degli altri dati digitali gli aggressori possono tentare di accedere anche a questi dati. Esistono diversi metodi di intercettazione: alcuni programmi nocivi sono concepiti in maniera tale da poter essere installati direttamente sul computer e di potere captarvi i segnali prima che questi siano cifrati e trasmessi mediante il *protocollo IP*. Ulteriori attacchi sono effettuati direttamente sui server VoIP per spiare il traffico corrente di comunicazioni. Si rammenta inoltre che in alcuni casi l'asporto di dati derubati è camuffato come traffico VoIP.

1. Una prima regola di base per ridurre a un minimo i rischi nell'utilizzazione di questa tecnologia è – per quanto possa sembrare semplice – la modifica del codice iniziale di accesso mediante password complesse.

2. Come nel caso di tutti gli altri prodotti anche in ambito di VoIP i programmi utilizzati devono essere costantemente aggiornati.

3. Una misura di sicurezza più concreta consiste nella configurazione della telefonia VoIP in maniera tale che siano possibili soltanto le chiamate a partire da determinati settori di numeri e che le chiamate ai numeri a valore aggiunto siano per quanto possibile bloccate.

6 Glossario

Advanced Persistent Threats (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.
App	Il concetto di app (dall'abbreviazione inglese di Application) designa in generale ogni forma di programmi di applicazione. Nell'uso linguistico si fa nel frattempo perlopiù riferimento alle applicazioni per i moderni smartphone e tablet computer.
Attacchi di Watering-Hole	Infezioni mirate con software nocivo per il tramite di siti Web che vengono visitati di preferenza da un gruppo specifico di utenti.
Attacco DDoS	Attacco Distributed-Denial-of-Service. Un attacco DoS in cui la vittima è attaccata simultaneamente da numerosi sistemi diversi.
Attacco di riflessione DNS	Cfr. attacco di amplificazione DNS.
Autentificazione a due fattori	A tal fine sono necessari almeno due dei tre fattori di autenticazione: 1. una cosa che si conosce (ad es. passwort, PIN ecc.); 2. una cosa che si ha (ad es. certificato, token, elenco da cancellare ecc.); 3. una cosa che si è (ad es. impronte digitali, scanner della retina, riconoscimento vocale ecc.)
Bring Your Own Device (BYOD)	Bring Your Own Device (BYOD) è una direttiva di organizzazione destinata a disciplinare le modalità secondo le quali i collaboratori possono utilizzare le loro proprie apparecchiature d'ufficio a scopi di servizio.
Brute Force	Il metodo Brute-Force-Methode è un metodo di soluzione di problemi nei settori dell'informatica, della criptologia e della teoria dei giochi, fondato sulla sperimentazione di tutti i casi possibili (o almeno di numerosi casi).
Cloud Computing	o «cloud computing» (sinonimo: «cloud IT», in italiano: «calcolare tra le nuvole»); concetto della tecnica dell'informazione (IT). Il pae-saggio IT non è più esercitato/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 dit-ta, ma in una nuvola («cloud»). L'accesso a questi sistemi a distanza è effet-tuato per il tramite di una rete.
Content Management System	Un «Content Management System» (acronimo CMS, in italiano «sistema di gestione dei contenuti») è un sistema che rende possibile e organizza la produzione e l'elaborazione comune di contenuti, consistenti in documenti di testo e multimediali, in genere destinati al World Wide Web. Un autore può servirsi di un simile sistema anche senza conoscenze di programmazione o di HTML. In questo caso il contenuto informativo da presentare è detto «content» (contenuto).
DNS	Domain Name System. Con l'ausilio del DNS, Internet e i suoi servizi sono di agevole utilizzazione, perché al posto dell'indirizzo l'utente possono utilizzare nomi (ad es. www.melani.admin.ch).
Attacco di amplificazione DNS	Attacco di Denial of Service (DoS), che sfrutta abusivamente server DNS accessibili al pubblico e li utilizza come amplifier (amplificatore).
Firewall	Un firewall (termine inglese per designare un muro tagliafuoco) protegge i sistemi di computer, nel senso che sorveglia i collegamenti entranti e uscenti e se del caso li rifiuta. Diversamente da quest'ultimo, il personal firewall (detto anche desktop firewall) è concepito per la protezione di un singolo computer ed è installato direttamente sul sistema da proteggere – ossia sul vostro computer.
Flash	Adobe Flash (abbr. Flash, già Macromedia Flash) è un ambiente proprietario e integrato di sviluppo per la produzione di contenuti multimediali. Attualmente Flash è utilizzato in numerose applicazioni Web, sia come insegna pubblicitaria, sia come parte di una pagina Web, ad esempio come menu di comando o sotto forma di pagina Flash completa.
FTP	File Transfer Protocol FTP è un protocollo di rete per la trasmissione di dati tramite reti TCP/IP. FTP può ad esempio essere utilizzato per caricare pagine Web su un server Web.
Gateways	Un gateway congiunge reti di calcolatori che possono essere basate su protocolli di rete totalmente diversi.
Geolocazione	La geolocazione ordina gli indirizzi IP in funzione della loro provenienza geografica.

Honeypots	In ambito di sicurezza dei computer si designa come honeypot (italiano: vaso di miele) un programma informatico o un server che simula i servizi di rete di un computer, un'intera rete di computer oppure il comportamento di un utente. Gli honeypot sono utilizzati per ottenere informazioni sui modelli di attacco e sui comportamenti degli aggressori.
Hyperlink	Un hyperlink, o più brevemente un link, o rinvio elettronico, è un rinvio incrociato in un ipertesto che esegue dal profilo funzionale un salto su un'altra posizione all'interno del medesimo o di un altro documento elettronico.
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.
Interfaccia	L'interfaccia o interface è una parte di un sistema destinata alla comunicazione. Cfr. interfaccia Web.
Interfaccia Web	L'interfaccia Web è una parte di un sistema destinata alla comunicazione tra applicazione e utente, generalmente attuata graficamente.
Internet Service Provider (ISPs)	Internet Service Provider. Offerente di prestazioni Internet, che offre generalmente contro retribuzione diverse prestazioni indispensabili per l'utilizzazione o l'esercizio di servizi Internet.
Intrusion Detection Systeme	Intrusion Detection System Sistemi che consentono di individuare accessi non autorizzati ai dati o all'elaboratore.
IP address spoofing	Nel tecnica informatica si designano come spoofing diversi tentativi di inganni sulle reti di computer per camuffare la propria identità.
IP-Adresse	Indirizzo che identifica il computer in Internet (o su una rete TCP/IP; esempio: 172.16.54.87).
Java	Java è un linguaggio di programmazione orientato sugli oggetti e una marca registrata dell'impresa Sun Microsystems (acquisita nel 2010 da Oracle).
Command and 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.
Lacuna Zero-Day	Lacuna di sicurezza per la quale non esiste ancora alcun patch.
Lacune di sicurezza	Vulnerabilità dell'hardware o del software, tramite la quale gli aggressori possono accedere a un sistema.
Malware	Termine composto dalle parole inglesi «Malicious» e "Software". 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.
Mobile Banking	Con il concetto di mobile banking si designa il disbrigo di operazioni bancarie effettuato con l'ausilio di dispositivi finali mobili come i telefoni mobili e i PDA.
Modbus/DNP3	Modbus e DNP3 (Distributed Network Protocol) sono protocolli di comunicazione dei sistemi di automazione dei processi.
mTAN	Password unica inviata mediante SMS e utilizzata prevalentemente in ambito di banking online.
Open DNS resolvers	Server DNS raggiungibili e utilizzabili da tutti gli utenti di Internet.
Open Source	L'Open Source è una gamma di licenze di software il cui testo fonte è liberamente accessibile e che per il tramite della licenza ne promuove lo sviluppo ulteriore.
Pacchetto di dati	In ambito di elaborazione dei dati si designano generalmente pacchetto di dati unità di dati chiuse in sé stesse che il mittente o un processo mittente invia al destinatario.
Packer	Programma di compressione o algoritmo di compressione di un programma. Ideato in origine per ottimizzare le dimensioni di un programma sul disco rigido. Il malware si avvale sovente di packer a monte per impedire la propria individuazione da parte dei software antivirus e per ostacolare l'analisi del malware (reverse engineering).
Patch	Un software che sostituisce le componenti di un programma affette da errori, sopprimendo così per esempio una lacuna di sicurezza.
Phishing	Nel caso del phishing i truffatori tentano di accedere ai dati confidenziali di ignari utenti di Internet. Si

	può trattare per esempio di informazioni sui conti di offerenti di aste online (ad es. eBay) o di dati di accesso a servizi bancari via Internet. I truffatori sfruttano la buona fede e la disponibilità delle loro vittime inviando loro e-mail nei quali l'indirizzo del mittente è falsificato.
PHP-Script	PHP è un linguaggio script che viene principalmente utilizzato per l'allestimento di pagine Web dinamiche e di applicazioni Web.
PLC	Un controllore logico programmabile (PLC) è un'apparecchiatura utilizzata per comandare o regolare una macchina o un impianto, che viene programmata su base digitale.
Plug-In, Plugin	Un software di complemento che amplia le funzioni di base di un'applicazione. Esempio: i Plug-In di Acrobat per i browser di Internet consentono la visualizzazione diretta di file PDF.
Point of Sales	Un terminale POS (in Svizzera terminale EFT/POS) è un terminale online per il pagamento senza contanti presso un punto di vendita («point of sale»).
Protocollo Internet (IP)	Protocollo di rete molto diffuso nelle reti di computer che costituisce la base di Internet. Si tratta dell'implementazione dello strato di trasmissione (inglese «Network Layer») del modello TCP/IP, rispettivamente dello strato di trasmissione del modello OSI.
QR-Code	Il QR-Code è un codice a barre bidimensionale che consta di una matrice quadrata di punti neri e bianchi che rappresentano in maniera binaria i dati codificati.
Ransomware	Malware tramite il quale i proprietari dei computer infettati sono ricattati (ransom: termine inglese per riscatto). Nel caso tipico i dati sono cifrati e nuovamente messi a disposizione dall'aggressore dopo il pagamento del riscatto per la chiave di decodificazione necessaria al loro ripristino.
Remote Administration Tool (RAT)	Il software di manutenzione a distanza (in inglese: Remote Administration Tool) costituisce un'applicazione nell'ambito del concetto di manutenzione a distanza di qualsiasi computer o sistema di computer.
Rete Bot	Un insieme di computer infettati da Malicious Bot. Essi possono essere interamente comandati a distanza da un aggressore (il proprietario della rete

	bot). A seconda delle dimensioni, una rete può constare di poche centinaia fino a milioni di elaboratori infettati.
Serial-Port Server	Un Serial-Port Server è un'apparecchiatura che trasferisce dati tra un'interfaccia seriale ed Ethernet.
Server Web	Un server Web è un server che trasmette documenti a client, come ad esempio i browser Web.
sFTP	sFTP è un metodo di cifratura del File Transfer Protocol (FTP), descritto in RFC 4217.
Smart-Meter	Uno Smart-Meter (in italiano: contatore intelligente) è un contatore dell'energia che mostra al singolo utente del collegamento il consumo effettivo di energia e il tempo effettivo di utilizzazione, dati che possono anche essere trasmessi all'impresa di approvvigionamento energetico.
SMS	Short Message Service Servizio per l'invio di messaggi brevi (160 caratteri al massimo) agli utenti di telefonia mobile.
Software di manutenzione	Il software di manutenzione a distanza (in inglese: Remote Administration Tool) costituisce un'applicazione nell'ambito del concetto di manutenzione a distanza di qualsiasi computer o sistema di computer.
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..
Spam Score	Sistema di punti utilizzato dai filtri per individuare le e-mail come spam.
Spear Phishing	Attacco mirato di phishing. Si fa ad esempio credere alla vittima di comunicare tramite e-mail con una persona di fiducia.
Telephony Denial of Service	Attacco alla disponibilità dei sistemi di telefonia, prevalentemente in ambito di VoIP.
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.
Voice-Phishing	Forma di truffa in Internet con uno stratagemma e prende il nome dal concetto inglese di pescare

	(fishing) e dal metodo di telefonia VoIP utilizzato.
VoIP	Voice over IP Telefonia tramite il protocollo Internet (IP). I protocolli utilizzati con maggiore frequenza sono: H.323 e SIP.
VoIP Toll Fraud	Utilizzo abusivo di un impianto VoIP per chiamare numeri a valore aggiunto appartenenti all'aggressore.
VPN	Virtual Private Network Consente per il tramite della cifratura del traffico di dati una comunicazione sicura tra computer su una rete pubblica (ad es. Internet).
Web Application Firewall (WAF)	Un Web Application Firewall (WAF) è una procedura destinata a proteggere le applicazioni Web da attacchi attraverso l'Hypertext Transfer Protocol (HTTP).
Web Hosting	Per Webhosting o anche Nethosting si intende l'approntamento di spazio Web e il collocamento (hosting) di siti Web sui server Web di un Internet Service Provider.
zip-Datei	Zip è un algoritmo e un formato di file per la compressione dei file, destinato a ridurre lo spazio di memorizzazione dei file per l'archiviazione e la trasmissione.

7 Allegato

7.1 Analisi di un software nocivo per Android, destinato a danneggiare la clientela e-banking svizzera

Le funzioni

- Il malware trasmette un SMS a un numero di telefonia mobile nell'area linguistica russa.
- L'obiettivo è il furto di mTAN.
- All'atto dell'installazione esso richiede l'autorizzazione di lettura e scrittura di SMS, nonché il diritto di scrittura sulla scheda SD.
- Si camuffa come applicazione di certificazione di Metaforic.
- Nel frattempo il malware viene individuato da numerosi scanner antivirus (Android/TrojanSMS.Agent.NV).

L'infezione

L'infezione segue le seguenti fasi:

1. Il cliente è invitato da un sito a installare un'applicazione sul proprio dispositivo mobile. Deve scegliere un sistema operativo.
2. Viene visualizzato un QR-Code che rinvia alla pagina dove si trova effettivamente il malware. Il malware è un normale pacchetto di installazione per Android (un file APK).
3. Il cliente deve disattivare determinati parametri di sicurezza affinché l'installazione funzioni.
4. Non appena l'installazione è eseguita il malware diviene attivo e sorveglia l'entrata degli SMS. L'applicazione stessa si camuffa come applicazione di sicurezza.
5. Gli SMS sono trasmessi a un numero di telefonia mobile in Russia.

L'obiettivo dell'aggressore è di captare mTAN per utilizzarli in vista di attacchi ai danni dei conti di e-banking.

Il malware

Dopo l'installazione il malware si presenta come applicazione di sicurezza di Metaforic. Metaforic è in realtà un fornitore di servizi di sicurezza, specializzato nel campo dei dispositivi

mobili. Spacciarsi per un prodotto degno di fiducia nel settore della sicurezza ai fini di accattivarsi la fiducia della vittima è un trucco che si osserva frequentemente, non soltanto nel caso del malware mobile. È vistosa la cattiva traduzione. L'utente deve scegliere una password (Wort Dordine) e immetterla nuovamente a titolo di conferma:

Figura 7: Schermata di login visualizzata per l'immissione della password (=Wort Dordine).

Dopo l'installazione del malware l'applicazione pretende di aver installato con successo un certificato.

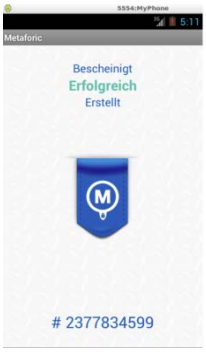


Figura 8: Conferma dell'installazione del certificato.

Il malware esige le seguenti autorizzazioni dallo smartphone:

```
In [19]: a.get_permissions()
Out[19]:
['android.permission.WRITE_EXTERNAL_STORAGE',
 'android.permission.RECEIVE_SMS',
 'android.permission.SEND_SMS']
```

Figura 9: Attribuzione dell'autorizzazione al malware.

Il fatto in particolare che un'applicazione esiga diritti di lettura e scrittura di SMS sta a indicare che non persegue buone intenzioni. In sottofondo l'applicazione esegue i seguenti processi:

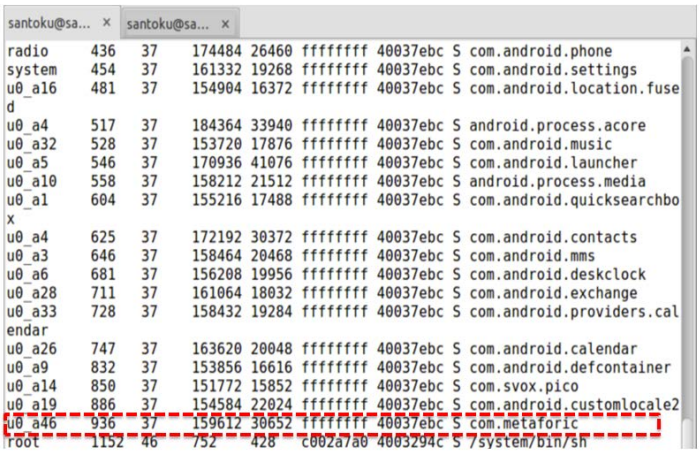


Figura 10: Sono contrassegnati in rosso i processi che il malware esegue in sottofondo.

Il codice di programma induce alle seguenti conclusioni:

- L'applicazione era originariamente redatta in olandese ed è stata successivamente tradotta in tedesco (peggio che male).

- Il numero al quale sono trasmessi gli SMS derubati figura in testo chiaro nel malware. Esso è localizzabile nell'area di lingua russa.

```
geben Sie das Passwort
Passwort best
tigen
Metaforic
Ya TuT :)
Wachtwoord komen niet overeen
^L^L+[redacted]
^L^LVerladung...
Wort Dordine:
^LBest
tigen:
Zertifikat erstellen
Erstellen eines Zertifikats...
Bescheinigt
Erfolgreich
Erstellt
```

Figura 11: Testo fonte con programmazione del numero telefonico al quale deve essere trasmesso l'SMS captato.

Le applicazioni Android sono sempre firmate digitalmente. In questo caso l'applicazione è stata firmata con un Debug Certificate, circostanza che non consente alcuna distribuzione attraverso l'app store ufficiale e la cui utilizzazione è di per sé riservata esclusivamente agli sviluppatori e ai collaudatori di applicazioni Android.

Da un punto di vista generale il malware è strutturato in maniera molto semplice e non dispone né di una funzionalità Rootkit per nascondersi, né di cifratura o di offuscazione per rendere difficile un'analisi. Essa persegue il solo e unico obiettivo di derubare mTAN. Esiste un grande numero di cavalli di Troia paragonabili per la piattaforma Android. Il tasso di identificazione da parte dei diversi scanner antivirus era inizialmente molto cattivo ed ha raggiunto successivamente il 50% circa (stato: inizio luglio 2013).