Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

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

SICUREZZA DELLE INFORMAZIONI

LA SITUAZIONE IN SVIZZERA E A LIVELLO INTERNAZIONALE

Rapporto semestrale 2015/II (luglio–dicembre)

28 APRILE 2016
CENTRALE D'ANNUNCIO E D'ANALISI PER LA SICUREZZA DELL'INFORMAZIONE MELANI
http://www.melani.admin.ch

1 Indice / Sintesi

2 Editoriale

MELANI: portare avanti gli sforzi intrapresi e rinforzare i partenariati trasversali con l'economia !

Jean-Pierre Therre, Executive Vice President/ Head of Technology Risk & Business Continuity, Banque Pictet & Cie SA, Associate Fellow GCSP, Lead Lecturer UniGE.

Nel quadro della strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC), gli obiettivi strategici affidati a MELANI sono l'identificazione precoce delle minacce e dei pericoli nel cyberspazio, la riduzione dei rischi cyber in particolare legati alla criminalità informatica e al cyber-spionaggio, così come il rafforzamento della capacità di resistenza delle infrastrutture critiche. In questo contesto, essenziale per favorire la necessaria resilienza operazionale di tutti gli attori economici pubblici o privati, il team MELANI, malgrado delle risorse ancora troppo limitate, si impegna diligentemente a perseguire gli obiettivi fissati.

Inoltre MELANI si fa carico della consolidazione di iniziative settoriali miranti a rinforzare lo scambio di informazioni pertinenti così come degli scambi strutturati tra gli attori dei principali settori economici.

Un esempio sono gli incontri semestrali che riuniscono un numero importante di rappresentanti del settore bancario e finanziario, questi eventi hanno raggiunto negli anni un'importanza considerevole. È l'occasione per gli esperti presenti di ricevere una panoramica completa dello spettro delle minacce cyber osservate sia in Svizzera sia all'estero.

La medesima volontà di scambio e di collaborazione è alla base della giornata « Swiss Cyber Risks 2015 » organizzata da MELANI allo Stade de Suisse di Berna il 02.11.2015, in presenza di numerosi professionisti dell'economia e di autorità politiche e militari, che ha permesso di realizzare incontri inaspettati e vantaggiosi, quindi molto apprezzati, tra il settore pubblico e l'economia privata.

Di fatto questi sforzi incoraggiano in modo eccellente la consolidazione di un reale partenariato pubblico-privato (PPP) come auspicato da tutti i professionisti toccati dalla ormai accertata moltiplicazione della minaccia cyber, dalla sua complessità crescente e dal carattere sempre più internazionale della stessa. Le azioni di prevenzione, identificazione e reazione, così come i principi di gestione di crisi, non possono più essere assunte da istituzioni isolate ma debbono iscriversi nell'ambito di iniziative concertate e strutturate tra tutti gli attori della comunità nazionale. In questo senso il partenariato tra MELANI e l'associazione «Swiss Cyber Experts (SCE)»[1], che permette di raggruppare le conoscenze di esperti con l'obiettivo di fornire una diagnostica efficace in caso di grave attacco cibernetico, è esemplare.

Che la squadra di MELANI, sotto la direzione di Pascal Lamia, sia ringraziata per le sue molteplici iniziative di informazione e i suoi lodevoli sforzi di coordinazione intersettoriale!

[1] https://www.swiss-cyber-experts.ch/ (stato: 29 febbraio 2016).

3 Tema principale: come affrontare le falle di sicurezza

Gli utenti di Internet sono costantemente esposti, in modo diretto o indiretto, a falle di sicurezza. Nel 2015 nella banca dati di MITRE, un'organizzazione no-profit che censisce sistematicamente le vulnerabilità di programmi informatici, sono state registrate complessivamente 6 419 falle a livello internazionale[2]. Tuttavia solo pochissime di queste hanno fatto notizia, anche perché si deve partire dal presupposto che una parte delle falle non sia presente in tale banca dati in quanto, queste ultime, per le ragioni più disparate, non vengono segnalate alle ditte produttrici.

D'altro canto il ventaglio degli apparecchi collegati a Internet che attingono a componenti di un sistema operativo e alle rispettive *librerie* diventa sempre più ampio, aumentando di conseguenza gli effetti e la portata delle singole falle di sicurezza. Inoltre, generalmente molti di questi sistemi non vengono aggiornati automaticamente. In tutta sincerità, quand'è stata l'ultima volta che avete rinnovato il *firmware* del vostro *router* o che avete aggiornato il software della vostra Web radio? Gli aggiornamenti mancanti o non eseguiti rappresentano così un grande problema in relazione al numero costantemente in aumento di falle di sicurezza.

3.1.1 Mancanza di politiche di update

Se in diversi ambiti gli update automatici sono diventati uno standard, la falla di sicurezza «Stagefright», divenuta di pubblico dominio nel mese di luglio 2015, mostra che esistono ancora delle eccezioni in materia. Essa ha infatti messo in luce in modo esemplare l'assenza di un processo di aggiornamento rapido ed efficiente per il sistema Android. Ciò non desta stupore in quanto da uno studio del 2011 era emerso che il 56 per cento degli smartphone Android disponeva di un sistema operativo obsoleto.[3] Spesso trascorre molto tempo prima che gli update possano essere scaricati da Google e installati sul dispositivo del consumatore finale. Ciò è dovuto al fatto che, per la consegna degli aggiornamenti, Google dipende sia dai produttori di smartphone, come Samsung o LG, sia dai singoli operatori di telefonia mobile. Prima di poter procedere alla distribuzione, gli operatori devono testare e certificare i vari update che i produttori offrono agli utenti. Apple, invece, può distribuire i propri update direttamente ai clienti. In seguito all'episodio sopra citato Google ha annunciato un ciclo di aggiornamento mensile. Alcuni produttori di cellulari intendono seguire tale procedura e stanno discutendo in merito a ciò con i gestori di rete. Per maggiori informazioni sulla falla «Stagefright» si rinvia al capitolo 5.6.1.

Un altro ambito problematico è costituito dai *Content Management System (CMS)*, ovvero dai sistemi di gestione dei contenuti. Nonostante gli aggiornamenti di sicurezza per i grandi CMS vengano messi a disposizione rapidamente, gli operatori spesso non sono

---

2 https://www.carbonblack.com/files/info-graphic-orphan-android/ (stato: 29 febbraio 2016).

3 https://www.carbonblack.com/files/info-graphic-orphan-android/ (stato: 29 febbraio 2016).

sufficientemente motivati a installarli, come evidenziato efficacemente nell'ultimo rapporto semestrale MELANI.[4]

3.1.2 Il business redditizio delle falle di sicurezza

Prima di poter risolvere una falla di sicurezza e procedere alla creazione di un'apposita *patch*, la vulnerabilità deve essere nota al produttore. Questa premessa, apparentemente così scontata, non viene sempre soddisfatta. Il Security Business è un mercato fortemente conteso e la gestione delle informazioni relative alla sicurezza costituisce sempre un campo minato in cui entrano in gioco molti interessi, naturalmente anche di natura finanziaria.

Un esempio eloquente in tal senso è costituito dall'attacco alla società italiana di software di sorveglianza «Hacking Team» dell'estate 2015 e dalla successiva pubblicazione di dati aziendali riservati. Accanto ai software di monitoraggio e alle e-mail personali, tra i dati prelevati sono stati trovati anche vari *0-day exploit* che erano stati acquistati dalla società «Hacking Team». In un caso la ditta pagò 45 000 dollari a un hacker russo per una falla di *Flash*.[5] I nomi degli altri acquirenti di tale vulnerabilità restano ignoti.

Gli affari concreti legati ai software di monitoraggio e alle attività di spionaggio così come l'aspetto operativo della politica di potenziamento digitale nazionale non vengono discussi pubblicamente. Per questo l'entità e il volume degli 0-day in circolazione sono molto difficili da stimare. Chaouki Bekrar, ex CEO e hacker principale della società VUPEN, si oppone al principio di tale riservatezza. Già nel 2012 affermò in un'intervista che non avrebbe venduto le falle di sicurezza trovate al costruttore del software neanche per un milione di dollari, ma lo avrebbe fatto esclusivamente ai suoi clienti, segnatamente a partner e governi facenti parte della NATO. Nel frattempo Bekrar ha fondato la società Zerodium che si è specializzata nel monitoraggio di apparecchi TIC. A suo nome ha bandito nel 2015 un concorso offrendo un milione di dollari agli hacker in grado di rivelargli un metodo per violare, passando inosservati, iPad e iPhone dotati dell'ultima versione del sistema operativo iOS 9.1 tramite *jailbreak*[6]. E la sua intuizione si è rivelata vincente. Quest'esempio mostra che il mercato 0-day obbedisce alle regole correnti del mercato: quanto più una falla è esclusiva, tanto più è redditizia.

Affinché i ricercatori segnalino le falle di sicurezza ai produttori di software e non le vendano al miglior offerente si devono definire alcune regole precise e creare appositi incentivi. Nella community di sicurezza TIC sono presenti molte persone che si impegnano sul fronte della formulazione di Best-Practices del genere, senza voler trarre profitto dal loro operato. Anche da parte del produttore a cui vengono annunciate le falle e che dovrebbe conseguentemente fornire dei rimedi tramite patches, sembra non esistere ancora un modo di agire consolidato. Se i produttori non prendono sul serio le vulnerabilità segnalate o, ancor peggio, minacciano

---

[4] Cfr. rapporto semestrale 1/2015, cap. 3 https://www.melani.admin.ch/melani/it/home/dokumentation/berichte/lageberichte/halbjahresbericht-2013-2.html (stato: 29 febbraio 2016).

[5] http://arstechnica.com/security/2015/07/how-a-russian-hacker-made-45000-selling-a-zero-day-flash-exploit-to-hacking-team/ (stato: 29 febbraio 2016).

[6] https://www.zerodium.com/ios9.html (stato: 29 febbraio 2016).

di sporgere denuncia contro colui che le ha divulgate, non sorprende che tali falle vengano rese note senza preavviso o che appaiano sul mercato 0-day prima che sia disponibile un aggiornamento in grado di risolverle.

Il grado di sensibilità del *Vulnerability Reporting* o report di vulnerabilità è dimostrato dalla controversia tra FireEye, un operatore statunitense attivo nel settore della sicurezza, ed ERNW, un fornitore di servizi di sicurezza TIC con sede a Heidelberg. Un ricercatore di ERNW ha trovato cinque falle di sicurezza nel «Malware Protection System» di FireEye e le ha segnalate all'azienda, con l'intento di renderle pubbliche entro 90 giorni. Ne è scaturita una controversia giudiziaria sui contenuti dell'avvertimento relativo alla falla, detto *advisory*, che ERNW intendeva pubblicare. FireEye temeva che quest'ultimo contenesse troppe informazioni sul funzionamento del suo prodotto, mentre ERNW sosteneva che tali dati erano necessari per comprendere la falla. Inoltre il funzionamento della vulnerabilità doveva essere esposto nel corso della conferenza londinese sulla sicurezza «44CON» Tuttavia avendo ottenuto un'ordinanza del tribunale, FireEye ha potuto mostrarne solo una versione ampiamente censurata.

3.1.3 Responsible disclosure

Diversi Paesi e produttori di software hanno riconosciuto la mancanza di regole e procedure precise, reagendo a tale situazione con lo sviluppo di cosiddetti processi di «responsible disclusure» per l'individuazione responsabile di falle di sicurezza e l'organizzazione di iniziative, denominate programmi *bug bounty,* volte a identificare, risolvere e divulgare errori presenti in software. A titolo d'esempio citiamo il programma bug bounty di Microsoft e il programma di «responsible disclosure» del governo olandese già descritto nel rapporto semestrale MELANI 2/2014[7]. Sul sito Web government.nl[8] sono descritte le fasi precise che vengono predisposte in seguito a una comunicazione e l'iter previsto per l'informatore. Anche altre grandi aziende come Google, Facebook e Twitter gestiscono programmi di questo tipo. Oltre a definire le regole che disciplinano il rapporto tra ricercatore, informatore e società in questione e che si riferiscono per esempio alla gestione temporale della risoluzione degli errori, agli aspetti finanziari ma anche concettuali, per il successo della procedura è richiesta una fiducia di fondo che deve essere innanzitutto costruita.

3.1.4 Situazione giuridica in Svizzera

Accanto alle regole comportamentali opzionali sopra citate occorrono senza dubbio anche condizioni quadro legali chiare che consentano ai ricercatori attivi nel settore della sicurezza di portare avanti l'attività di ricerca di tali vulnerabilità, presupposto fondamentale per migliorare la sicurezza dei programmi. Una possibile soluzione in tal senso consiste nel focalizzare l'attenzione non sulla ricerca stessa della falla, bensì sul suo utilizzo successivo. Anche il Codice penale svizzero tiene conto della motivazione dell'attore del processo: è

---

7 Rapporto semestrale 2/2014, cap. 5.5 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/halbjahresbericht-2014-2.html (stato: 29 febbraio 2016).

8 https://www.government.nl/topics/cybercrime/contents/fighting-cybercrime-in-the-netherlands/responsible-disclosure (stato: 29 febbraio 2016).

punibile solo chiunque «mette in circolazione o rende accessibili password, programmi o altri dati, sapendo o dovendo presumere che sono utilizzati allo scopo di commettere un reato […]»[9] e chiunque «allestisce, importa, mette in circolazione, propaganda, offre o rende comunque accessibili programmi che sa o deve presumere destinati al [danneggiamento di dati], o dà indicazioni per allestirli […]»[10]. In virtù di quanto precede, la ricerca di falle di sicurezza ai fini della comunicazione al produttore non è perseguibile secondo il diritto svizzero. Anche lo scambio tra i ricercatori attivi nel settore della sicurezza dovrebbe essere consentito. Per contro la relativa pubblicazione è punibile in quanto, in questo caso, si deve prevedere che la vulnerabilità venga sfruttata in modo passibile di pena. Al pubblicatore si può rimproverare il fatto di accettare tale condizione e di agire pertanto con dolo. In Svizzera non si può minacciare un produttore di procedere a una pubblicazione (dettagliata) di una lacuna per metterlo alle strette e indurlo a risolverla. Viceversa il ricercatore è libero di riferire in termini generali sull'esistenza di una vulnerabilità scoperta su Internet e di criticare in tale sede anche un eventuale comportamento del produttore reputato insoddisfacente.

In quale misura sia possibile esigere da un produttore un compenso per l'individuazione e la segnalazione della lacuna di sicurezza è un aspetto che non è stato (ancora) definito e dovrebbe essere precisato dalla giurisprudenza, prendendo in considerazione in particolare la «gestione d'affari senza mandato»[11] e l'insorgere di un'obbligazione derivante da indebito arricchimento[12], in virtù del fatto che il produttore riceve una prestazione. Che un ricercatore avvii una causa nei confronti del produttore offrendo così a un tribunale la possibilità di prendere posizione in merito è, invece, improbabile: i ricercatori attivi nel campo della sicurezza dovrebbero perseguire obiettivi più nobili anziché affannarsi a rincorrere avvocati e giudici.

---

9 Art. 143bis cpv. 2 CP: https://www.admin.ch/opc/it/classified-compilation/19370083/index.html#a143bis (stato: 29 febbraio 2016).

10 Art. 144bis n. 2 CP: https://www.admin.ch/opc/it/classified-compilation/19370083/index.html#a144bis (stato: 29 febbraio 2016).

11 Art. 419 segg. OR: https://www.admin.ch/opc/it/classified-compilation/19110009/index.html#id-2-14 (stato: 29 febbraio 2016).

12 Art. 62 segg. CO: https://www.admin.ch/opc/it/classified-compilation/19110009/index.html#id-1-1-3 (stato: 29 febbraio 2016).

4 La situazione a livello nazionale

4.1 Spionaggio informatico in Svizzera

Il presente capitolo non contiene dettagli che consentono di identificare obiettivi o episodi specifici. Il motivo è da ricercare nell'anonimato che, nella maggior parte dei casi, viene garantito alla vittima e alla fonte d'informazione. Divulgare informazioni legate allo spionaggio informatico sarebbe controproducente anche in considerazione degli interessi della piazza economica, dello Stato e delle misure di difesa adottate. La presente panoramica offre, tuttavia, un quadro d'insieme della situazione su scala nazionale delineato grazie a una serie di informazioni raccolte attraverso vari fatti occorsi negli ultimi sei mesi.

Prima di poter definire una tipologia di obiettivi prediletti dai criminali informatici occorre stabilire che genere di informazioni potrebbero risultare preziose agli occhi di un potenziale truffatore. In questa sede ci limitiamo a un'analisi degli attacchi che presentano una certa utilità per uno Stato e possiamo pertanto presupporre che a destare interesse per quest'ultimo siano soprattutto le informazioni che potrebbero contribuire al raggiungimento degli obiettivi strategici prefissati e che, quindi, sono spesso collegate all'agenda politica (segnatamente a negoziazioni future o al monitoraggio di opposizioni politiche all'estero), a questioni di sicurezza (terrorismo), a programmi militari o, in alcuni casi, economici (in particolare innovazioni, know-how, dettagli relativi a relazioni commerciali).

La presenza sul territorio elvetico di numerose organizzazioni che possiedono interessanti informazioni da questo punto di vista rende la Svizzera un bersaglio ideale per i cyber-attacchi. Si pensi in particolare alle numerose rappresentanze estere, organizzazioni e comunità internazionali che rivestono un interesse politico per molti Paesi. Anche le conoscenze di interi settori economici e le informazioni sui relativi rapporti commerciali o sulle offerte in corso potrebbero offrire un considerevole vantaggio concorrenziale a vari attori economici di altri Paesi. In molte nazioni, inoltre, lo spionaggio economico è subordinato a un programma politico di ampio respiro e, a volte, può essere giustificato addirittura da considerazioni relative alla sicurezza.

Gli attacchi informatici che puntano a entrare in possesso di tali informazioni si rivolgono a diverse tipologie di vittime. Un hacker può decidere di colpire direttamente il proprietario dei dati ma, qualora tale obiettivo risulti per esempio difficilmente accessibile, può adottare anche una strategia articolata in due fasi e cercare dapprima di danneggiare un operatore per raggiungere in seguito il suo bersaglio effettivo. È proprio in quest'ottica che nel 2014 e nel 2015 alcune strutture alberghiere della regione del lago di Ginevra sono state utilizzate per intercettare le delegazioni ivi riunite durante le negoziazioni relative all'accordo sul nucleare con l'Iran.[13] In altri casi gli attacchi sono rivolti a società di manutenzione che hanno

[13] MELANI rapporto semestrale 1/2015, capitolo 4.1.1 https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/rapporti-di-situazione/rapporto-semestrale-2015-1.html (stato: 29 febbraio 2016).

accesso all'area riservata di un'azienda o, ancora, a operatori di telecomunicazioni, come dimostrato dall'offensiva sferrata contro BICS BELGACOM scoperta nel 2013.[14]

A volte, individui o aziende possono essere vittime «collaterali» di incidenti con i quali non hanno alcun tipo di relazione. Può succedere addirittura che soggetti terzi siano coinvolti in casi di spionaggio solo a seguito di un errore nella definizione dell'obiettivo o di altri effetti non previsti, come è successo per esempio nel 2015 a un'azienda del settore vinicolo che è stata infettata da un malware utilizzato per spionaggio informatico. Poiché le intenzioni degli hacker erano note, dagli accertamenti effettuati è emerso rapidamente che la vittima poteva essere ascritta alla categoria dei «danni collaterali».

[14] MELANI rapporto semestrale 2/2013, capitolo 4.1 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2013-2.html (stato: 29 febbraio 2016).

Conclusione e raccomandazioni:

Lo spionaggio informatico contro interessi svizzeri è una realtà, come dimostrato dai numerosi casi descritti nei precedenti rapporti semestrali MELANI e dalla panoramica delineata nel rapporto annuale del Servizio delle attività informative della Confederazione (SIC). La prevenzione rappresenta una componente importante, se non la più importante, nella lotta contro lo spionaggio. Come sottolineato da diversi casi segnalati a MELANI, il primo e principale passo in tal senso è costituito dalla presa di coscienza da parte di un'azienda di trovarsi di fronte a un rischio reale e non ipotetico. Per poter contrastare in modo efficace lo spionaggio occorre inoltre assicurare il flusso di informazioni. Se i casi di spionaggio vengono segnalati, le autorità possono adottare le misure necessarie e mettere in pratica le conoscenze acquisite in ambito legislativo o politico. Queste informazioni consentono inoltre ad altre organizzazioni di individuare eventuali attacchi ai loro sistemi. Il trattamento confidenziale dei dati resta naturalmente la massima priorità per le autorità.

MELANI è attiva da dieci anni sul fronte della lotta contro i pericoli IT in collaborazione con diversi enti privati. Per la segnalazione di incidenti legati all'ambito dell'assicurazione delle informazioni, MELANI mette a disposizione un apposito formulario sul suo sito Web:

MELANI formulario d'annuncio:

https://www.melani.admin.ch/melani/fr/home/meldeformular/formulaire.html

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

Programma Prophylax

http://www.vbs.admin.ch/internet/vbs/it/home/documentation/publication/snd_publ.html

4.2 Sistemi industriali di controllo

Con la diffusione dell'Internet delle cose, le tecnologie dell'informazione e della comunicazione (TIC) e i sistemi industriali di controllo (ICS) a esse collegate si fanno strada in settori sempre nuovi della nostra vita quotidiana. Di conseguenza i cyber-rischi acquistano rilevanza e attualità anche in tali campi. Nel presente rapporto semestrale vengono trattati i sistemi critici legati all'ambito della mobilità.

4.2.1 Gestione libera dei parcheggi

L'automazione degli edifici è un sottosettore dei sistemi di controllo in uso, di cui la maggior parte di noi si avvale quotidianamente in modo più o meno consapevole. Un campo

d'applicazione nei complessi di grandi dimensioni è costituito dalla gestione dei parcheggi. I *sistemi TIC* vengono utilizzati in molteplici ambiti, dai semplici parchimetri centrali ai più sofisticati sistemi di gestione di parcheggi estesi a intere città. A ottobre 2015 MELANI è stata informata dell'esistenza di un'interfaccia per la gestione dei parcheggi in Svizzera accessibile liberamente (Figura 1) che consentiva, quindi, a chiunque di consultare in qualsiasi momento lo stato di occupazione dei singoli parcheggi e ai potenziali scassinatori di conoscere per esempio gli orari in cui gli appartamenti erano generalmente liberi o in cui i collaboratori si trovavano fuori casa.

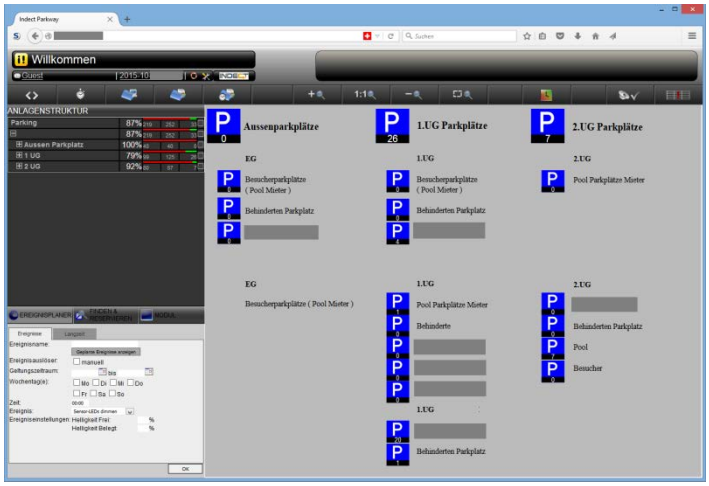

Figura 1: screenshot interfaccia web per la gestione dei parcheggi

MELANI ha informato tempestivamente l'operatore dei fatti e del potenziale pericolo.

4.2.2 Infrastruttura ferroviaria vulnerabile

Anche nell'ambito dei sistemi di trasporto e delle infrastrutture ferroviarie sempre più strettamente collegate alle TIC si utilizzano sistemi industriali di controllo, che vengono impiegati, per esempio, per comandare i segnali e azionare gli scambi. Al 32° «Chaos Communication Congress» tenutosi ad Amburgo dal 27 al 30 dicembre 2015, il gruppo russo «*SCADA*-Strangelove»[15] ha illustrato un ampio ventaglio di potenziali attacchi che possono colpire le infrastrutture ferroviarie più disparate e che, quindi, non riguardano solo i più ovvi sistemi d'informazione per i passeggeri, ma anche gli apparati centrali automatizzati, le telecamere di videosorveglianza e le stazioni solari disseminati lungo le tratte. Spesso tali sistemi sono vulnerabili in quanto l'accesso fisico a questi ultimi non è sufficientemente sicuro, i sistemi e i dispositivi di sicurezza utilizzati sono obsoleti o, ancora, perché vengono impiegate password di default di pubblico dominio. Per sensibilizzare fornitori e utenti in merito a tale problematica e convincerli a non impiegare password di default, il gruppo ha pubblicato un elenco di 37 fornitori di componenti di sistemi di controllo di utilizzo comune, quali server e *switch*, le cui password di default circolano su Internet. Tra questi figurava anche un produttore svizzero di router ferroviari e soluzioni *VPN*.

[15] https://blog.kaspersky.com/train-hack/10946/ (stato: 29 febbraio 2016).

Conclusione e raccomandazione:

Utilizziamo i mezzi pubblici per il nostro trasporto e ordiniamo merci online che, nel migliore dei casi, ci vengono recapitate il giorno successivo. Le soluzioni logistiche che impieghiamo e che ci circondano diventano sempre più efficienti, il che è possibile solo grazie all'utilizzo di sistemi di trasporto intelligenti nonché di una gestione robotizzata delle scorte. Con la crescente integrazione di oggetti d'uso quotidiano, i sistemi industriali di controllo nella loro totalità diventano una componente sempre più importante della nostra vita quotidiana.

Di conseguenza anche le persone interessate dai rischi collegati a tale sviluppo sono sempre di più. Sul suo sito Web, MELANI propone una lista di controllo delle misure di protezione dei sistemi industriali di controllo:

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

https://www.melani.admin.ch/melani/it/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-industriellen-

4.3 Attacchi a siti Web: DDoS e defacement

In Svizzera i privati e le aziende continuano a essere oggetto di diversi tipi di attacchi che colpiscono principalmente i loro siti Web. La vulnerabilità nei confronti di *attacchi DDoS* e *defacement* costituisce un problema particolarmente rilevante per le imprese per cui è importante preservare la credibilità della propria immagine online. Nel secondo semestre del 2015 sono stati osservati, sempre più di frequente, attacchi a siti web finalizzati alla successiva diffusione di malware.

4.3.1 Reti pubblicitarie

Gli hacker sono costantemente alla ricerca di nuove strategie che consentano loro di infettare il maggior numero di apparecchi di potenziali vittime servendosi di semplici espedienti. In passato lo strumento prediletto erano e-mail contenenti link o allegati infetti che potevano essere spedite senza disporre di grandi conoscenze tecniche. Oggi tuttavia le possibilità di successo di tali strumenti si sono progressivamente ridotte in quanto gli utenti di Internet sono maggiormente consapevoli dei rischi di tali attacchi e sono meno inclini a cliccare su allegati o link contenuti nei messaggi. Inoltre una campagna e-mail di questo tipo ottiene grande visibilità e il malware diffuso confluisce molto rapidamente nelle banche dati dei produttori di antivirus. Per questo attualmente le infezioni di siti Web, le cosiddette *infezioni drive-by*, acquisiscono sempre più importanza in qualità di metodo di diffusione di malware. Per ottenere una propagazione su vasta scala, i pirati informatici prendono di mira portali di ampia portata, prediligendo in particolare quelli di giornali e le cosiddette reti pubblicitarie. La specificità di queste ultime consiste nel gestire centralmente contenuti pubblicitari che vengono in seguito trasmessi a una molteplicità di clienti, come per esempio testate online. Un'infezione contratta da uno di questi sistemi centrali può avere pertanto gravi ripercussioni e portare al dilagare di infezioni.

Nel periodo in esame MELANI ha reso noti due episodi di questo tipo.

4.3.1.1 Attacco alla pagina Web di un quotidiano

Una prima infezione è stata segnalata a MELANI l'11 settembre 2015 da un ricercatore attivo a livello della sicurezza che ha scoperto che una rete pubblicitaria svizzera conduceva i visitatori all'*exploit kit* «Niteris». Poiché la medesima rete veniva sfruttata anche da una pagina che fornisce le edizioni online di diversi quotidiani, il numero delle potenziali vittime poteva essere molto elevato. Se un utente visitava un sito Web su cui appariva questo annuncio pubblicitario compromesso, il malware identificava innanzitutto la lingua impostata sul terminale. Se quest'ultima era tedesco o francese, il computer veniva sottoposto a un'analisi delle vulnerabilità in Internet Explorer (p. es. CVE-2014-6332), Firefox (p. es. CVE-2013-1710), Java (p. es. CVE-2013-2465) o Adobe Flash (p. es. CVE-2015-5119). Mentre le falle dei navigatori risalivano al 2003 e al 2004 ed erano quindi relativamente «datate», per quella di Adobe Flash era disponibile un update dal 7 luglio 2015. I computer che non avevano eseguito regolarmente gli aggiornamenti dei programmi sono stati infettati. Il malware installato era «GOZI ISFB», il noto trojan che colpisce il settore dell'e-banking e che viene utilizzato da vari gruppi di hacker per sferrare attacchi a istituti finanziari in tutto il mondo. Una settimana dopo, il 18 settembre 2015, gli hacker hanno iniziato inaspettatamente a rimuovere il malware dai computer infetti. Le motivazioni di tale scelta possono essere molteplici; probabilmente il gruppo si era reso conto che l'operazione non era andata a buon fine e intendeva così ostacolare la ricostruzione dei fatti.

Conclusione:

Oltre che dei numerosi vantaggi e dell'abbattimento dei costi reso possibile da una centralizzazione dei contenuti Web, ogni azienda dovrebbe essere consapevole anche dei rischi collegati a una simile operazione. A prescindere dal pericolo di infezioni da malware sui computer dei visitatori del sito Web, in caso di incidente, sussiste anche il rischio di una perdita di reputazione da parte dell'impresa.

È imperativo definire in precedenza la procedura da seguire in presenza di contenuti compromessi di operatori terzi. L'azienda può accedere a contenuti di terzi e, all'occorrenza, può influenzarli e bloccarli? Si dovrebbero soprattutto chiarire in precedenza i contatti con le divisioni di sicurezza TIC delle imprese terze in modo da poter informare rapidamente le persone giuste in caso di incidente e da poter avviare contromisure adeguate.

4.3.1.2 Colpito anche un portale televisivo

Un incidente simile è stato subito da un portale televisivo su cui, il 3 dicembre 2015, è stata riscontrata un'infezione che propagava l'«Angler exploit kit». Anche in questo caso la contaminazione non è rimasta circoscritta al sito Web. Il contenuto della pagina Web manipolata è stato, infatti, condiviso anche con giornalisti di altri giornali online, tra cui una rivista gratuita, il che ha aumentato notevolmente la portata e la cerchia delle potenziali vittime. Fortunatamente a essere colpita è stata solo una sottopagina. MELANI ha informato gli operatori del sito che hanno potuto così rimuovere il codice dannoso.

Le cosiddette infezioni di siti Web o infezioni drive-by fanno parte delle strategie comunemente utilizzate dagli hacker per infettare il maggior numero possibile di apparecchi. L'«Angler exploit kit» utilizzato in questo episodio ha fatto la sua prima apparizione a fine 2013 e da allora gode di crescente popolarità tra i pirati informatici. Di regola il modo di procedere adottato dai diversi gruppi di autori è quasi identico: spesso è lo stesso exploit kit a verificare il bersaglio finale, tramite JavaScript, per quanto riguarda i plugin installati e le relative versioni, allo scopo di individuare una falla e di poterla attaccare con l'exploit adeguato. È interessante osservare la velocità con cui i singoli exploit kit dispongono di exploit idonei alla comparsa di nuove vulnerabilità. Non tutti gli exploit kit dispongono degli stessi exploit; la variabilità è piuttosto ampia in questo contesto. Capita inoltre sempre più spesso che gli exploit kit stessi siano provvisti di 0-day exploit.

4.3.2 Defacement su LeMatin.ch: virus IRAQ

I contenuti di operatori terzi hanno fatto notizia anche in un altro caso: l'8 luglio 2015 sul sito Web della guida televisiva di «lematin.ch» è stata pubblicata una foto di un gruppo di hacker islamici denominato «Virus IRAQ».[16] A essere attaccato non è stato tuttavia «Le Matin» stesso, bensì l'operatore «Guide Loisirs» che fornisce contenuti di pagine Web per diversi clienti. In questo caso non si è trattato di un attacco mirato, bensì di una deturpazione generica di pagine Web, denominata *defacement*, che viene praticata migliaia di volte al giorno. Il gruppo in questione identificato come «Virus IRAQ» è attivo da tempo. Secondo il sito Web zone-h.org che recensisce questo genere di attacchi, nel 2015 il collettivo ha perpetrato azioni di questo tipo su oltre 300 pagine Web, selezionando i propri obiettivi in modo casuale: tra le pagine colpite figurano siti ucraini, neerlandesi, tedeschi, francesi, cechi e, in prevalenza, statunitensi.

Conclusione:

I siti Web vengono esaminati minuziosamente in modo continuativo e sistematico per individuare eventuali falle di sicurezza. Nel momento in cui viene scoperta una vulnerabilità essa viene anche sfruttata. Spesso nel caso dei defacement vengono inseriti contenuti politici o religiosi. Inoltre si crea una competizione tra i singoli gruppi di attivisti per chi ha sferrato il maggior numero di attacchi.

4.3.3 Acquisizione di indirizzi IP: informazioni generali relative alle problematiche BGP

Internet consta di decine di migliaia di reti (i cosiddetti «*sistemi autonomi*», in breve «AS») che sono interconnesse e che possono scambiarsi tra loro pacchetti di dati. Per lo scambio di queste informazioni viene utilizzato un protocollo denominato *Border Gateway Protocol (BGP)* che comunica ai router i percorsi o rotte attraverso le quali sono raggiungibili le varie reti. Più o meno coevo di Internet, il protocollo ha subito l'ultima revisione nel 1991 (RFC 1269) e, purtroppo, presenta da sempre alcune debolezze, come la possibilità di

[16] http://www.tagesanzeiger.ch/digital/internet/Hacker-platzieren-SchockBilder-auf-Website-von-Le-Matin/story/27762519 (stato: 29 febbraio 2016).

sferrare attacchi (cosiddetti *spoofing*) simulando false identità. Ciascun AS può sostenere, infatti, di essere proprietario di una rete anche se quest'ultima non gli appartiene affatto. Poiché tecnicamente non vi è alcuna possibilità di verificare la legittimità del percorso indicato, gli AS confidano nel fatto che l'interlocutore comunichi solo rotte corrette.

Lo scorso anno Spamhaus, uno dei maggiori provider di liste di blocco del mondo, ha segnalato a MELANI due casi di «acquisizione» di spazi di indirizzamento di AS svizzeri e successivo utilizzo da parte di spammer per l'invio di e-mail fraudolente. Il primo caso è stato notificato a MELANI a giugno 2015 quando è stato violato lo spazio di indirizzamento di un Cantone. Il secondo episodio risale invece a settembre 2015 quando un destino analogo è toccato a parti dello spazio di indirizzamento di un'azienda farmaceutica. In entrambi i casi MELANI ha informato l'organizzazione interessata.

Raccomandazione:

Se possedete un vostro spazio di indirizzamento pubblico vi consigliamo di procedere come segue:

- assicuratevi che l'oggetto all'interno dell'intervallo IP salvato presso il vostro Regional Internet Registry (RIR) p. es. RIPE sia aggiornato e che possieda un *abuse-mailbox* valido;
- diffondete il vostro spazio di indirizzamento anche se attualmente è inutilizzato in quanto ciò renderà più difficile la relativa violazione da parte degli spammer;
- attivate un monitoraggio BGP per i vostri spazi di indirizzamento per essere informati in caso di violazione da parte di un AS esterno. Qualora siate impossibilitati o non intendiate farlo direttamente, vi invitiamo a rivolgervi a società commerciali che propongono questo tipo di servizi. Per maggiori informazioni sulle problematiche relative al BGP e all'acquisizione di indirizzi IP si rinvia al blog GovCERT.ch.

GovCERT.ch Blog:

http://www.govcert.admin.ch/blog/11/cantonal-ip-space-in-switzerland-hijacked-by-spammers

4.3.4 Estorsione tramite DDoS: dopo DD4BC è la volta di Armada Collective

Anche nel secondo semestre del 2015 l'estorsione si è rivelata essere uno dei metodi privilegiati dai criminali cibernetici che mirano a realizzare un rapido guadagno finanziario. Accanto alle ormai numerose famiglie di malware di crittografia (cfr. cap. 4.5.1 del presente rapporto semestrale), si è tentato nuovamente di limitare la disponibilità di siti Web e di estorcere denaro alle vittime tramite una serie di *attacchi DDoS*. Mentre la maggior parte degli attacchi sferrati fino a metà 2015 portava la firma del gruppo «DD4BC», nel secondo semestre dell'anno il testimone è passato al gruppo «Armada Collective». Entrambi i gruppi hanno adottato la stessa strategia. Gli attacchi di Armada Collective sono stati rivolti, tra gli altri, a e-mail e hosting provider. A fare notizia, anche a livello internazionale, è stato

soprattutto l'attacco sferrato a novembre 2015 contro «Protonmail», un provider svizzero specializzato in comunicazione via e-mail cifrate.

Gli attacchi DDoS sono un fenomeno conosciuto da tempo. Nel 2015 è stata registrata un'intensificazione delle offensive a fini prettamente finanziari, rivolte principalmente a imprese con modelli aziendali che necessitano della costante reperibilità del proprio sito Internet e che quindi presentano un elevato potenziale di estorsione. Messe sotto pressione dalle minacce di inaccessibilità del loro portale Web e nella speranza di una rapida risoluzione del problema, alcune imprese considerano la possibilità di pagare un riscatto. Con tale denaro forniscono tuttavia agli estorsori i mezzi finanziari per intensificare gli attacchi e potenziarne l'infrastruttura, senza avere alcuna garanzia che, in seguito al pagamento, gli attacchi cessino. I criminali cibernetici utilizzano sovente i cosiddetti *servizi booter o stresser*, ovvero strumenti informatici che scatenano attacchi DDoS a pagamento (un «DDoS as a service»). La quantità di denaro a disposizione dell'estorsore è direttamente proporzionale al volume degli attacchi (sia in termini di intensità che di durata) che potrà sferrare tramite un fornitore di servizi simile. Per contro, se le vittime non cedono al ricatto, il modello degli estorsori non funziona più. Alla luce di quanto esposto finora, il pagamento di riscatti è tuttalpiù un palliativo temporaneo e senza garanzia. In tal modo non si contribuisce a rafforzare la propria infrastruttura a lungo termine né a proteggere Internet dagli attacchi DDoS.

Un'azienda colta alla sprovvista da un attacco DDoS, nella maggior parte dei casi non riuscirà a reagire in modo rapido ed efficace alla situazione. Le misure di sicurezza contro gli attacchi DDoS acquisiscono un'importanza ancora maggiore per quelle imprese che utilizzano internet come principale canale commerciale. In questi casi, la protezione della piattaforma di vendita dovrebbe essere considerata una priorità assoluta. Per questo si raccomanda di sviluppare una strategia da attuare nell'eventualità di un attacco di questo tipo e di reperire i nominativi dei servizi competenti in materia, sia interni che esterni, e degli altri interlocutori cui rivolgersi durante un'urgenza. Inoltre, sarebbe auspicabile che un'azienda affrontasse la problematica DDoS nel quadro della gestione generale dei rischi e che definisse una determinata strategia di difesa a livello aziendale, senza attendere di venir presa di mira. Qualsiasi organizzazione può subire un attacco DDoS! Discutete con il vostro fornitore di servizi Internet delle vostre necessità e di adeguate misure preventive. Una lista di controllo completa con l'indicazione delle misure da adottare contro gli attacchi DDoS è disponibile sul sito di MELANI al seguente link:

Liste di controllo e guide: Misure contro attacchi DDoS

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

4.3.4.1 Attacco a Protonmail

Un'eccezione sia in termini di pubblicità sia di procedura rispetto a quella sopra descritta è costituita dall'attacco DDoS sferrato a «Protonmail», il servizio di posta elettronica creato dai ricercatori del CERN che offre una *cifratura end-to-end*. L'azienda, fondata nel 2013 in

seguito alle rivelazioni di Edward Snowden, ha sede a Ginevra e viene finanziata tramite crowdfunding.[17]

Nella notte del 3 novembre 2015, Protonmail ha registrato degli attacchi DDoS sui suoi sistemi. Si è presupposto che la responsabilità degli attacchi fosse di Armada Collective. In base a quanto affermato da Protonmail, gli attacchi sono proseguiti giornalmente, il che non riflette la consueta strategia seguita dal gruppo di hacker che normalmente si limita a un solo attacco dimostrativo con il quale auspica di intimorire immediatamente la vittima costringendola a pagare. Nei primi giorni Protonmail ha supposto che si trattasse di un singolo hacker. Questi attacchi hanno avuto degli effetti collaterali su altri clienti all'intero del centro di calcolo. D'intesa con queste aziende si è deciso allora di pagare il riscatto. Solo quando gli attacchi non sono cessati in seguito al pagamento e Armada Collective stessa ha preso le distanze dalle offensive, Protonmail ha ipotizzato la presenza di un secondo estorsore.[18]

Fin dall'inizio l'azienda ha riferito i fatti con estrema franchezza e ha espresso il sospetto che dietro agli attacchi potesse nascondersi uno Stato[19], tesi che tuttavia non ha potuto essere dimostrata. Ci sono tuttavia dei buoni motivi per presupporre che vi sia stato un «approfittatore» che abbia sfruttato tale situazione. La comunicazione relativa agli attacchi DDoS, che fin dal primo istante è stata trasparente, potrebbe essere uno dei motivi per cui un fruitore clandestino sia venuto a conoscenza di questo attacco, abbia sfruttato l'occasione e abbia operato parallelamente ad Armada Collective.

4.3.4.2 Arresto all'interno di DD4BC

Molti dei tentativi di estorsione osservati nel 2015 sono attribuibili al gruppo DD4BC (DDoS for BitCoin). Il 15 e il 16 dicembre il Dipartimento High-Tech Crime della Repubblica Srpska (entità della Bosnia-Erzegovina) ha condotto un'operazione denominata «Pleiades» contro il gruppo DD4BC. L'offensiva, avviata dalle autorità austriache, è stata eseguita in collaborazione con le forze di polizia di diversi Paesi europei e di Europol e con il sostegno dell'European Cybercrime Center (EC3). Anche la Svizzera ha partecipato a tale intervento che ha portato all'arresto del presunto leader della banda, un cittadino bosniaco di 32 anni sospettato di aver giocato un ruolo chiave all'interno dell'organizzazione, e di un altro individuo.

4.3.5 Minaccia di Anonymous a Losanna

Il gruppo indipendente «Anonymous» ha ottenuto una certa notorietà a livello internazionale, in particolare in relazione a grandi battaglie, come la difesa delle attività del fondatore di WikiLeaks Julian Assang o la guerra dichiarata ai simpatizzanti dell'«ISIS» su Internet (cfr. in merito anche il cap. 5.4.2 del presente rapporto semestrale). Un clamoroso caso scoppiato

---

17 https://en.wikipedia.org/wiki/ProtonMail (stato: 29 febbraio 2016).

18 https://protonmaildotcom.wordpress.com/2015/11/05/protonmail-statement-about-the-ddos-attack/ (stato: 29 febbraio 2016).

19 https://twitter.com/ProtonMail/status/661683054866429798 4 (stato: 29 febbraio 2016).

nella Svizzera romanda nel luglio 2015 ha dimostrato tuttavia che quest'organizzazione di hacker-attivisti non è interessata solo a questioni internazionali. Un gruppo denominato «Anonymous Svizzera» ha minacciato, infatti, di violare i sistemi TIC della città di Losanna qualora non venisse mostrato un maggiore riguardo nei confronti degli abitanti del grattacielo «Tour de la Sallaz». Alla base di tale intimidazione vi erano le emissioni generate durante i lavori di costruzione che avrebbero danneggiato gli abitanti dell'edificio. Oltre a sporgere denuncia contro la minaccia, sono state adottare delle misure per proteggere la TIC della città dagli attacchi.

Conclusione:

Non trattandosi di un collettivo ben definito è difficile stabilire se quest'intimidazione sia effettivamente collegata al movimento Anonymous o se porti la firma di un altro autore che, ricorrendo al nome del famoso gruppo di attivisti, auspicava di ottenere una maggiore risonanza. La connessione non particolarmente stretta con Anonymous sfocia in una serie di annunci e attacchi non coordinati, più o meno spettacolari. Dato che per motivi inerenti alla sua struttura non esiste adesione come membro ad Anonymous, né sono presenti un portavoce ufficiale e persone responsabili dell'intero movimento, ognuno può in linea di massima eseguire attacchi o pubblicare comunicazioni a nome del gruppo.

4.4 Social engineering, phishing

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

4.4.1 Phishing: statistiche

Nel corso degli ultimi anni è notevolmente aumentato il numero di richieste relative al *phishing* che sono state evase da MELANI. Per poter elaborare in maniera più efficiente le numerose segnalazioni di phishing ricevute, nel 2015 la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione ha attivato il sito Internet «antiphishing.ch» sul quale è possibile indicare pagine sospette di phishing. Nel primo anno sono state segnalate complessivamente 2 500 pagine, per quanto il numero subisca forti variazioni nel corso del tempo per svariati motivi: oltre alle oscillazioni stagionali dovute al fatto che nei periodi di vacanza vengono effettuate meno segnalazioni (e anche gli hacker si riposano!), gli hacker cambiano regolarmente il Paese che desiderano colpire.

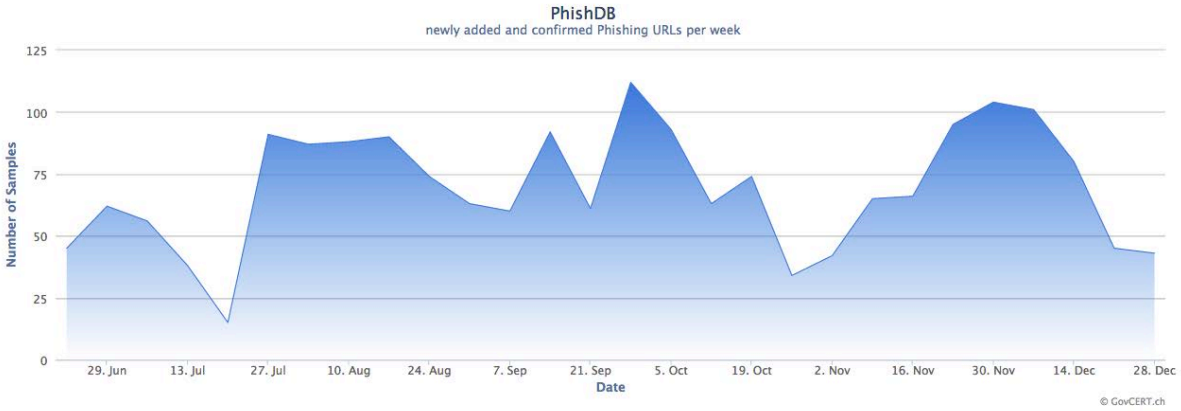

Figura 2: pagine di phishing segnalate e confermate settimanalmente su antiphishing.ch

4.4.1.1 Molteplici usi impropri del logo dell'Amministrazione federale (parte 1[a])

Il logo dell'Amministrazione federale svizzera gode di grande popolarità tra i criminali informatici che lo hanno utilizzato impropriamente già due volte per scopi di phishing e una per diffondere malware (cfr. cap. 4.5.2 del presente rapporto semestrale). Gli attacchi non sono stati sferrati contro l'Amministrazione federale. L'uso indebito del logo è stato finalizzato unicamente a creare una parvenza di serietà per ingannare le vittime.

Anche nel secondo semestre del 2015 dei truffatori hanno inviato ripetutamente e-mail a nome dell'Ufficio federale dell'energia (UFE) per tentare di impadronirsi dei dati delle carte di credito di utenti Internet. I primi casi sono stati osservati già nel 2014. I destinatari sono stati attirati da un'e-mail contenente una promessa di rimborso esigibile accedendo a un sito Web indicato, dall'aspetto identico a quello dell'Ufficio federale dell'energia, su cui i destinatari sono stati invitati a inserire non solo il loro nome e indirizzo, ma anche il numero della loro carta di credito, completo di data di scadenza e codice di sicurezza a tre cifre.

Il nome dell'Amministrazione federale delle contribuzioni (AFC) è stato utilizzato in modo improprio una seconda volta a fine settembre 2015In tale occasione, inviando un'e-mail su cui l'AFC figurava abusivamente quale mittente, i truffatori hanno tentato di procurarsi copie di passaporti nonché di accedere a informazioni su conti e carte di credito dei contribuenti.[20]

4.4.2 Phishing con pubblicità

Da aprile 2015 MELANI ha osservato un nuovo procedimento utilizzato per gli attacchi di phishing rivolti a istituti finanziari svizzeri non più basato sull'invio di e-mail, bensì sulla pubblicazione di annunci pubblicitari a pagamento su motori di ricerca come Google, Yahoo o Bing. A tale scopo i truffatori acquistano parole chiave (keyword) dai gestori dei motori di ricerca che sono in relazione con l'istituto finanziario in questione: se i phisher intendono per esempio colpire i clienti della «banca XY» pubblicano annunci pubblicitari di phishing contenenti la parola chiave «XY» o «banca XY».

[20] https://www.estv.admin.ch/estv/de/home/allgemein/aktuell/warnung--phishing.html (stato: 29 febbraio 2016).

Gli annunci pubblicitari sui motori di ricerca appaiono generalmente ben in evidenza nella parte superiore della schermata prima dei risultati veri e propri della ricerca. Di conseguenza la probabilità che un utente clicchi sull'annuncio pubblicitario anziché sul risultato effettivo della ricerca per accedere alla pagina della «banca XY» è elevata.

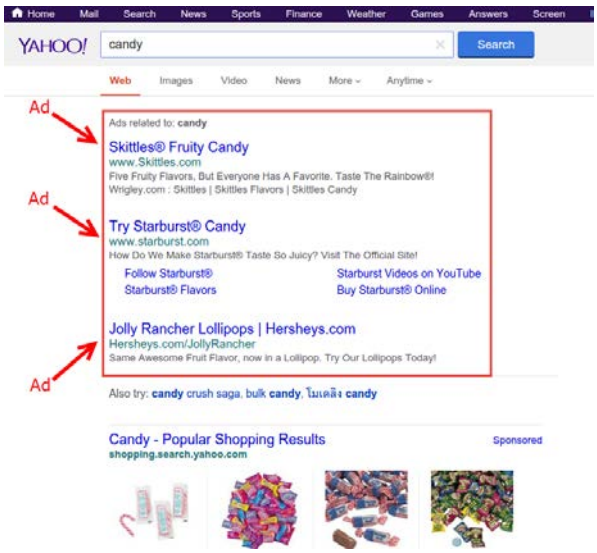

Figura 3: esempio di annuncio pubblicitario apparso su Yahoo

I malfattori sfruttano questo fatto per indirizzare utenti Internet ignari verso pagine Web di phishing. Gli attacchi di phishing tramite annunci pubblicitari su motori di ricerca noti presentano però anche altri vantaggi per gli hacker:

- per i fornitori di servizi di sicurezza TIC e i *CERT* è difficile identificare come tali gli annunci pubblicitari di phishing pubblicati su motori di ricerca;
- i cyber-criminali non devono preoccuparsi di attivare filtri anti-spam o di stilare elenchi di indirizzi e-mail affidabili in quanto questa procedura non prevede l'invio di e-mail;
- alcuni gestori di motori di ricerca non eseguono verifiche sistematiche o, comunque, non approfondite dei nuovi clienti e, di conseguenza, gli autori degli attacchi possono aprire in qualsiasi momento un nuovo account utente sulla piattaforma pubblicitaria per pubblicare annunci fraudolenti.

MELANI ha contattato i tre principali gestori di motori di ricerca svizzeri per affrontare il problema, due dei quali erano stati effettivamente colpiti dagli attacchi di phishing descritti.

Raccomandazione:

Per maggiori informazioni sul phishing tramite annunci pubblicitari si rinvia al blog GovCERT.ch:

INFO

GovCERT.ch Blog:

http://www.govcert.admin.ch/blog/16/ads-on-popular-search-engine-are-leading-to-phishing-sites

4.4.3 Phishing con file PDF

Un altro procedimento osservato più volte da MELANI nel secondo semestre del 2015 è stato il phishing tramite ricorso a file PDF, oltre ai quali vengono spedite anche le consuete e-mail di phishing che tuttavia non contengono un link HTML indirizzante alla pagina di phishing vera e propria, bensì un allegato con estensione .pdf. Tale documento contiene delle indicazioni che inducono la vittima a cliccare sul link indicato nel file PDF, il quale conduce in seguito alla pagina effettiva di phishing.

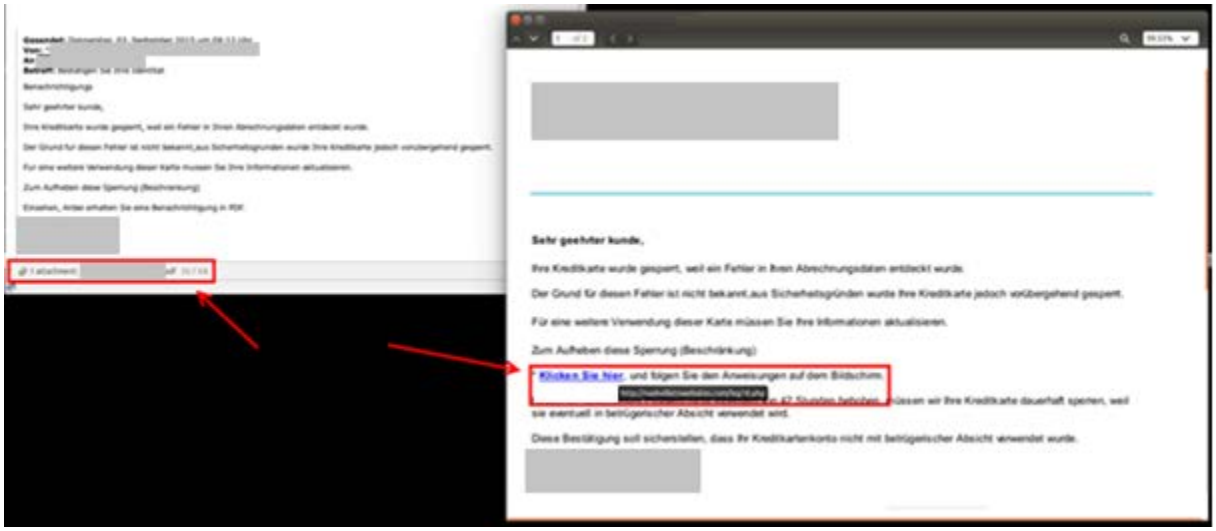

Figura 4: fac-simile di e-mail con link a un allegato con estensione .pdf

Conclusione:

Mentre per il destinatario di un'e-mail di phishing è praticamente ininfluente che il rinvio alla pagina di phishing sia celato direttamente nell'e-mail o in un allegato, questa nuova pratica comporta un importante vantaggio per gli hacker. Attraverso l'utilizzo di file PDF vengono rimossi i filtri e-mail che in genere ricercano contenuti pericolosi solo nell'e-mail stessa. I criminali informatici sembrano essersi resi conto di tale possibilità e pertanto ricorrono sempre più spesso a questo espediente.

4.5 Crimeware

Il crimeware è una forma di malware sviluppata da criminali economici che dal punto di vista criminologico rientra nel campo della criminalità informatica e giuridicamente si colloca nel settore delle truffe su Internet. In materia di crimeware sono sempre molto diffusi i trojan di e-banking, come dimostra la statistica riportata di seguito. Gran parte dei sistemi infettati in Svizzera, comunicati a MELANI, è costituita da trojan di e-banking come «Torpig», «Dyre», «Tinba», «Gozi» o «ZeuS». Mentre nello scorso semestre il malware e-banking più diffuso era stato «Tinba», nel secondo semestre del 2015 quest'inglorioso primato è spettato a «Gozi». Ciò potrebbe dipendere da vari fattori, tra cui il metodo di diffusione tramite reti pubblicitarie infette descritto nel capitolo 4.3.1. Come nel primo semestre del 2015 la maggior parte delle infezioni è da attribuire tuttavia a «Downadup» (noto anche come «Conficker»), un worm che esiste già da più di otto anni e che si diffonde tramite una falla di sicurezza rilevata nel sistema operativo Windows nel 2008 e da allora corretta.

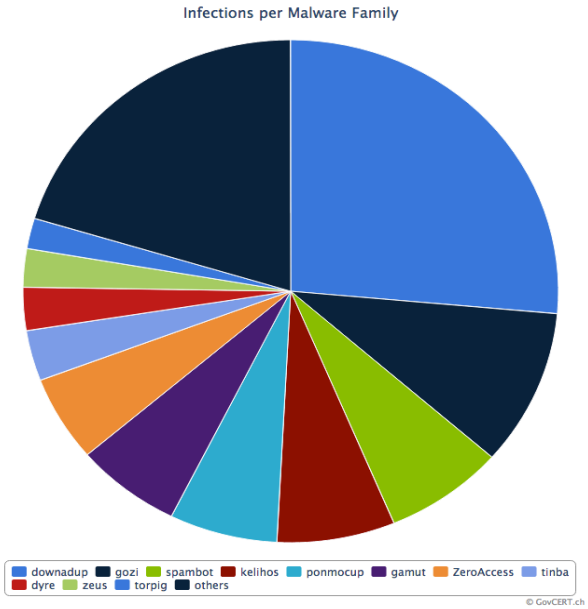

Figura 5: distribuzione del malware noto a MELANI in Svizzera. Il giorno di riferimento è il 31 dicembre 2015. Dati aggiornati sono disponibili su: http://www.govcert.admin.ch/statistics/dronemap/

Come nel primo semestre del 2015 i Cantoni di Zurigo e del Vallese hanno evidenziato una percentuale di infezioni superiore rispetto ad altri Cantoni (tenuto conto del numero di abitanti). Mentre nel caso di Zurigo il tasso più elevato potrebbe essere riconducibile a una elevata densità di computer, il motivo del tasso di infezioni registrato nel Cantone del Vallese non è attualmente chiaro.

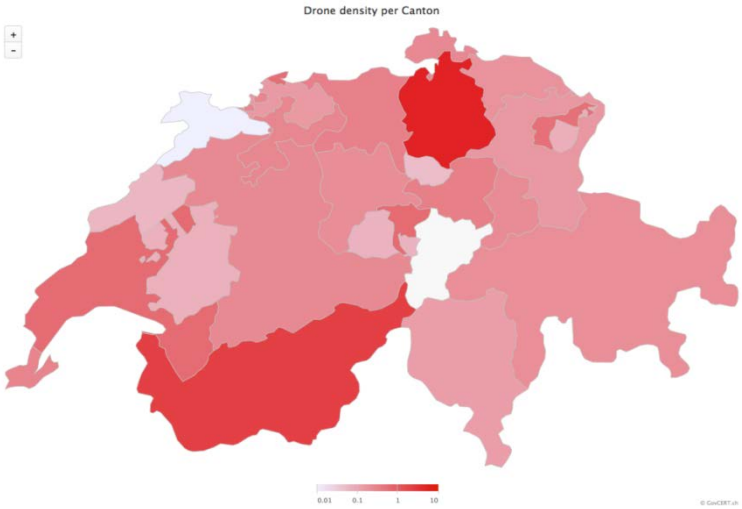

Figura 6: numero di infezioni per Cantone tenuto conto del numero di abitanti. Il giorno di riferimento è il 31 dicembre 2015. I dati aggiornati sono disponibili su: http://www.govcert.admin.ch/statistics/dronemap/

4.5.1 Trojan di crittografia sempre molto diffusi

Anche nel secondo semestre del 2015 sono stati resi noti diversi casi di dati codificati attraverso trojan di crittografia. In questi casi si è trattato generalmente del *ransomware* «Teslacrypt», ma sono stati segnalati a MELANI anche diversi episodi legati ad altre famiglie di trojan, come per esempio «Criptowall», rivolti generalmente a privati, ma anche ad aziende di tutti i settori e di tutte le dimensioni. La vittima che in caso di un attacco non ha a disposizione un backup aggiornato perde tutti i propri dati o una parte di essi.

Raccomandazione:

I dati archiviati sul computer devono essere copiati regolarmente su supporti dati esterni (*backup*) che devono essere collegati al computer solo durante il processo di backup e conservati in un luogo sicuro.

INFO

Misure contre ransomware:

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

4.5.2 Molteplici usi impropri del logo dell'Amministrazione federale (parte 2ª)

Secondo il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet SCOCI dell'Ufficio federale di polizia (fedpol), all'inizio di luglio 2015 sono state inviate delle e-mail fraudolente a nome della fedpol invitando i destinatari a scaricare dei documenti di un provvedimento giuridico fittizio da un sito Web. Un'iniziativa analoga è stata osservata a gennaio 2016. Il testo dei messaggi è stato formulato in modo tale da intimorire i destinatari mettendoli alle strette: alle persone che non avessero messo a disposizione i dati desiderati entro 15 giorni veniva intimato che il tribunale avrebbe pronunciato la sentenza senza convocarli. Il link conduceva a una pagina contraffatta del sito Internet della fedpol. Gli utenti venivano in seguito invitati a inserire un codice di sicurezza (*captcha*) e a scaricare dei file. Chi seguiva le indicazioni riportate sul sito e contenute nel testo dell'e-mail procedeva tuttavia, involontariamente, all'installazione del malware di crittografia «Cryptolocker» sul suo apparecchio.

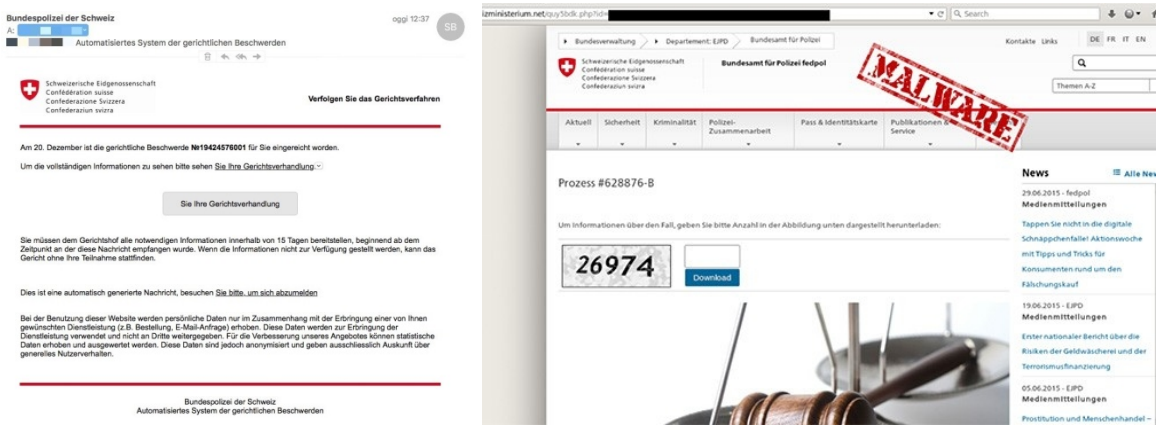

Figura 7: uso improprio del sito dell'Ufficio federale di polizia per la diffusione del trojan di crittografia «Cryptolocker» Fonte: SCOCI/fedpol

All’inizio di febbraio 2016 il logo dell’Ufficio federale di polizia è stato nuovamente utilizzato per un’iniziativa fraudolenta che, a seguito della visita di un sito compromesso, portava al blocco del navigatore e alla comparsa di un messaggio che accusava la vittima di aver scaricato dei file illegali. Dietro pagamento di un’ammenda via paysafecard i truffatori promettevano lo sblocco del navigatore e l’abbandono del procedimento penale. Negli ultimi anni questi casi si sono intensificati sempre di più. Diversamente dal trojan di crittografia citato in precedenza, quella utilizzata in questo caso è una variante di frode non molto professionale che, a seconda del sistema operativo e del navigatore, consente di richiudere la finestra del navigatore ed evitare che le ultime pagine visitate vengano riaperte automaticamente (evitando così che la procedura si ripeta). Vi invitiamo a consultare le istruzioni del software in uso; per Windows, per esempio, la chiusura avviene attraverso il Task Manager (Ctrl-Alt-Canc). Non solo i computer fissi e portatili sono colpiti da varianti nocive del navigatore. Si constata un aumento di codici con le stesse funzionalità anche per navigatori mobili come smartphone e tablet

Figura 8: falsa schermata di blocco con il logo dell’Ufficio federale di polizia Fonte: SCOCI/fedpol

4.5.3 Trojan di e-banking: Retefe e Tinba

A fine novembre 2015 MELANI ha deciso, previo accordo con i partner e gli istituti finanziari interessati, di disattivare l’*infrastruttura Command & Control* utilizzata dal trojan di e-banking «Retefe». MELANI è intervenuta presso gli hosting provider e i centri di registrazione esteri, invitandoli a disattivare i server e i nomi di dominio utilizzati da Retefe. Il takedown ha interessato più di 30 server e nomi di dominio in tutta Europa. Nelle settimane successive MELANI non ha più riscontrato nuove infezioni né nuove ondate di spam collegate a Retefe. La disattivazione della *botnet* ha avuto un esito positivo fino a fine dicembre 2015, quando sono state registrate nuove ondate di spam identiche a quelle osservate nei mesi precedenti e collegate a Retefe. Un’analisi degli allegati ha fornito tuttavia risultati sorprendenti: il software nocivo utilizzato (malware) non era Retefe, ma un altro trojan di e-banking di gran lunga più noto chiamato «Tinba» (anche noto come «Tiny Banker»). Evidentemente il gruppo responsabile di Retefe ha deciso di adottare un nuovo strumento, utilizzando da dicembre 2015 Tinba e, di conseguenza, una nuova infrastruttura Command & Control.

I due trojan Retefe e Tinba presentano notevoli differenze: mentre il primo è stato, a quanto pare, ideato direttamente dagli hacker e utilizzato esclusivamente per truffe e-banking in Svizzera, Austria, Svezia e, in alcuni casi isolati, anche in Giappone, il secondo è un noto «*crimeware kit*» che viene venduto su forum underground. Un’altra differenza è

rappresentata dal funzionamento dei due cavalli di Troia: mentre Retefe modifica le impostazioni DNS o Proxy del computer infettato, Tinba si annida nel sistema e comunica regolarmente con un'infrastruttura di Command & Control centrale, il che consente ai truffatori di accedere in qualsiasi momento al computer della vittima e di perpetrare una truffa e-banking attraverso quest'ultimo.

4.5.4 Botnet: Dridex / Bugat

Nel mese di ottobre 2015 il Dipartimento di giustizia statunitense e l'FBI hanno sferrato un attacco contro la botnet «Bugat». Meglio conosciuto con il nome di «Dridex», Bugat è un trojan di e-banking che colpisce i clienti di dozzine di istituti finanziari di tutto il mondo. Le autorità statunitensi hanno accusato un trentenne moldavo di aver amministrato la rete infetta. Nonostante i tentativi dell'intelligence americana di smantellare la botnet Bugat e di arrestarne le persone coinvolte, quest'ultima è ancora attiva e cerca quotidianamente di infettare apparecchi di ignari utenti Internet in America e in Europa attraverso campagne di spam.

Raccomandazione:

MELANI raccomanda agli utenti Internet di non aprire nessun allegato e-mail sospetto anche se i messaggi provengono da mittenti apparentemente affidabili e di assicurarsi che sul proprio computer sia installato un antivirus che venga tenuto costantemente aggiornato.

Regole di comportamento: E-Mail

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

4.5.5 Retata contro gli acquirenti di Droidjack

I *Remote Access Tool* per Android (RAT) sono sempre più popolari tra i cyber-criminali. Oltre a consentire di controllare uno smartphone[21], questi strumenti permettono di monitorare il traffico dati, di intercettare di nascosto telefonate e rumori ambientali, di assumere il controllo della fotocamera del telefono e di localizzare l'apparecchio. Su iniziativa delle autorità di perseguimento penale tedesche a fine ottobre è stata avviata una retata contro i venditori del RAT «Droidjack». Contemporaneamente nel Regno Unito, negli Stati Uniti, in Francia, Germania, Belgio e anche in Svizzera sono state eseguite delle perquisizioni domiciliari. Gli acquirenti del malware, che veniva venduto online al prezzo di 210 dollari statunitensi, sono stati accusati di spionaggio illecito di dati e di frode informatica. Con l'aiuto degli indizi raccolti si auspica di ottenere delle informazioni sulla paternità del malware, aspetto passato in secondo piano nell'ambito della retata. Le tracce lasciate dagli autori del crimine porterebbero in India.

[21] http://www.symantec.com/connect/blogs/droidjack-rat-tale-how-budding-entrepreneurism-can-turn-cybercrime (stato: 29 febbraio 2016).

4.6 Altri temi

4.6.1 La gestione dei domini come processo cruciale per le imprese

I nomi di dominio non sono solo indirizzi ai quali è possibile raggiungere un sito Web. In ambito aziendale essi costituiscono generalmente anche l'ultima parte degli indirizzi e-mail dei collaboratori e possono per esempio essere parte dell'infrastruttura implementata per consentire gli accessi remoti degli impiegati alle reti interne. In qualità di elementi d'indirizzo impiegati nel settore delle telecomunicazioni, i nomi di dominio presentano una molteplicità di utilizzi e, non da ultimo, fungono anche da marchi aziendali. Alla luce delle diverse funzioni per le quali vengono utilizzati, soprattutto dalle aziende, la relativa gestione può costituire un processo cruciale per l'impresa stessa, per esempio in quanto il sito Internet e le e-mail sono fondamentali per l'attività svolta o perché la configurazione dell'infrastruttura TIC può essere adattata ad altri nomi di dominio solo con sforzi notevoli.

I nomi di dominio, tuttavia, non possono essere «acquistati», ma vengono registrati. Ciò significa che il *registrant*, ovvero colui che richiede la registrazione, ottiene un diritto di utilizzo dell'elemento di indirizzo corrispondente, divenendone titolare per un periodo di tempo limitato. Tale diritto deve essere rinnovato periodicamente; qualora si ometta di farlo, il sito diviene improvvisamente irraggiungibile e anche l'invio delle e-mail viene sospeso – tanto per citare solo le conseguenze tecniche palesi.

Nel 2015, con la riorganizzazione dell'assegnazione dei nomi di dominio in Svizzera,[22] l'obbligo del gestore del registro o *registry* di assegnare nomi di dominio del primo livello (*Top Level Domain*) «.ch» direttamente al cliente finale (titolare del dominio o *registrant*) è stato abolito. Inoltre si è stabilito che dopo un periodo di transizione il gestore del registro dovrà cessare completamente le attività svolte con i clienti finali. Il gestore del registro deve limitarsi alla gestione tecnica del dominio .ch, mentre l'assegnazione dei nomi di dominio e l'amministrazione dei clienti finali nell'ottica di una disaggregazione completa del mercato dei domini compete unicamente al cosiddetto *registrar* o centro di registrazione. Di conseguenza i registrant che fino a questo momento avevano acquistato i nomi di dominio direttamente dal gestore del registro SWITCH hanno dovuto cercare un registrar in grado di gestire la registrazione del dominio per loro conto. Nella scelta del registrar, i registrant dovevano essere consci delle proprie esigenze e selezionare un'offerta adeguata.

A fine 2015 MELANI ha ricevuto diverse lamentele da parte di registrant che dichiaravano di non essere stati informati in tempo utile e forma adeguata sull'imminente scadenza del loro contratto di registrazione. Ciò che ha portato alla disattivazione dei loro nomi di dominio con le conseguenze sopra descritte per la loro attività. Fortunatamente i nomi .ch scaduti non vengono immediatamente sbloccati per una nuova registrazione e pertanto, con alcuni oneri amministrativi e con l'ausilio dei loro registrar, i (precedenti) registrant possono riottenerli.

---

[22] Separazione dei compiti nella gestione degli indirizzi Internet.ch: http://www.bakom.admin.ch/themen/internet/00468/04167/04981/index.html?lang=it (stato: 29 febbraio 2016).

Raccomandazione:

Un’azienda deve sapere quanti e quali nomi di dominio ha registrato, lo scopo per cui li utilizza e, in particolare, quando rinnovare le varie registrazioni. Discutete con il centro di registrazione responsabile delle vostre esigenze e delle offerte proposte. Definite dei processi e meccanismi per la protezione dei vostri nomi di dominio da modifiche intenzionali e non, sia a livello tecnico che amministrativo.

Promemoria sulla sicurezza informatica per le PMI.

https://www.melani.admin.ch/melani/it/home/dokumentation/liste-di-controllo-e-guide/promemoria-sulla-sicurezza-informatica-per-le-pmi.html

5 La situazione a livello internazionale

5.1 Spionaggio

5.1.1 Hacking Team nel mirino degli hacker

La società italiana «Hacking Team» che produce software di monitoraggio ha subito un grande furto di dati a seguito di un attacco hacker. Il 5 luglio 2015 sono stati pubblicati oltre 400 gigabyte di materiale prelevato. La società milanese elabora programmi di sorveglianza per autorità giudiziarie, servizi segreti e aziende private e annovera tra i suoi clienti anche la Polizia cantonale di Zurigo.[23] L'offerta di prodotti include un software di monitoraggio per Windows, MacOS, Linux e tutti i sistemi operativi per smartphone che consente di accedere a smartphone e computer e, per esempio, di leggere SMS o intercettare telefonate e conversazioni Skype.

Nelle attività legate al monitoraggio la confidenzialità costituisce la massima priorità. L'attacco non ha comportato pertanto soli enormi danni di reputazione per l'azienda colpita, ma anche una serie di conseguenze per i clienti. Tra i dati pubblicati sono apparsi per esempio e-mail, elenchi di clienti e altri documenti confidenziali che, con ogni probabilità, non sono stati setacciati minuziosamente solo da giornalisti e fornitori di servizi di sicurezza, ma anche da gruppi intenzionati a trarre profitto dalle falle di sicurezza e dalle backdoor ormai note. In alcuni casi i programmi impiegati e pagati dai clienti sono stati fortunatamente disattivati in modo tempestivo, mentre in altri, purtroppo, hanno potuto essere utilizzati anche da terzi non autorizzati. Di conseguenza la società ha messo in guardia contro l'uso improprio del software da parte di criminali e terroristi.[24] Diversi provider di software hanno pertanto iniziato a chiudere le falle di sicurezza sfruttate. La Polizia cantonale di Zurigo, che aveva acquistato il software «Galileo» prodotto dalla società Hacking Team per circa mezzo milione di franchi, ha dichiarato inoltre di voler sospendere l'utilizzo di tale programma. L'episodio sopra descritto illustra molto chiaramente la difficoltà e la pericolosità di gestire falle di sicurezza e backdoor (cfr. in merito i cap. 3 e 5.1.2 Juniper).

L'elenco dei Paesi di provenienza dei clienti è lungo[25] e contiene, accanto a Stati come la Svizzera, gli Stati Uniti e la Germania, anche Paesi come il Sudan, in cui vige effettivamente un embargo sulle armi imposto dall'ONU, il che potrebbe a sua volta ravvivare la discussione circa la misura in cui un programma informatico possa rientrare nel concetto di «esportazione di armi».

Anche a livello politico la pubblicazione dei dati interni della società Hacking Team ha generato alcune turbolenze: il capo dell'intelligence cipriota, Andreas Pentaras, ha

---

23 http://www.heise.de/newsticker/meldung/Hacking-Team-Kantonspolizei-kaufte-Ueberwachungssoftware-trotz-Bedenken-des-Bundesgerichts-2911887.html (stato: 29 febbraio 2016).

24 http://www.heise.de/newsticker/meldung/Hacking-Team-Terroristen-koennten-geleakte-Schnueffeltechnik-nutzen-2746071.html (stato: 29 febbraio 2016).

25 http://www.watson.ch/Digital/Best%20of%20watson/477908232-Die-uns%C3%A4glich-peinliche-Geschichte-der-gehackten-Hacker-(und-Kapo-ZH-Lieferanten)-in-25-Tweets-erz%C3%A4hlt (stato: 29 febbraio 2016).

rassegnato le proprie dimissioni nel momento in cui è stato reso noto l'acquisto da parte sua di un software di Hacking Team. Sull'isola greca il monitoraggio delle comunicazioni è vietato. Cinque anni prima, infatti, il Parlamento cipriota aveva rivisto la costituzione in tal senso, consentendo lo svolgimento di tali attività solo in determinate condizioni.[26] Nonostante le basi legali non fossero state ancora applicate, Pentaras ha dichiarato che tutte le disposizioni erano state rispettate, pur decidendo comunque di abbandonare il suo incarico per evitare possibili danni ai servizi segreti nazionali.

A finire sotto accusa, in Svizzera, è stato Mario Fehr, capo della Polizia cantonale di Zurigo, che aveva dato il proprio benestare all'ordinazione di un software della società Hacking Team. L'acquisto del software è stato effettuato seguendo la procedura ordinaria tramite un'ordinanza della Direzione della sicurezza ed esclusivamente nell'ambito del perseguimento penale.[27] Per contro l'adozione di misure tecniche di monitoraggio è avvenuto su disposizione del giudice dei provvedimenti coercitivi responsabile dell'autorizzazione alla sorveglianza. La Gioventù socialista (GISO) zurighese ha sporto denuncia contro Fehr, sostenendo che l'acquisto avrebbe violato il diritto costituzionale alla libertà personale e alla protezione della sfera privata. Il pubblico ministero di Zurigo non ha aperto tuttavia alcun procedimento contro il consigliere di Stato.

5.1.2 Spionaggio con Juniper, Synful Knock e un certificato esportabile

Nel corso di una revisione software interna, il fornitore di servizi di rete Juniper ha scoperto la presenza di «righe di programma non autorizzate» nel sistema operativo «ScreenOS». La società, che ha sede negli Stati Uniti, si configura come il secondo maggiore service provider del mondo dopo Cisco e produce router high-end che vengono impiegati per *dorsali Internet*. Prima di Natale 2015 sono state pubblicate due falle di sicurezza e, contemporaneamente, anche il rispettivo update. Le versioni in questione in realtà non sono così diffuse, ma vengono impiegate per la comunicazione aziendale di massima sicurezza.

Una falla comprendeva l'implementazione di una master password nel codice di programmazione ed era evidentemente presente nel sistema operativo dal 2013. Mentre prima dell'update solo pochi (hacker) sarebbero stati in possesso di questo passepartout, in seguito alla pubblicazione è stato possibile risalire, senza grandi sforzi, al luogo in cui era salvato. Dopo poche ore, tale informazione è stata resa di pubblico dominio anche su Internet e gli attacchi non hanno tardato a seguire.

La seconda falla è più complessa: in concreto si tratta di una backdoor nella cifratura che consente a un hacker di intercettare connessioni VPN, permettendo così di decodificare anche dati di rete salvati in un secondo tempo. La falla si basa sul generatore di numeri pseudo-casuali «EC_DRBG», già noto dai tempi di Snowden, che in realtà non fornisce le sequenze numeriche in modo così fortuito come dovrebbe. Anziché sostituire questo

[26] https://intelnews.org/tag/cyprus-intelligence-service/ (stato: 29 febbraio 2016).

[27] http://www.kapo.zh.ch/internet/sicherheitsdirektion/kapo/de/aktuell/medienmitteilungen/2015_07/1507071c.html (stato: 29 febbraio 2016).

generatore in toto, Juniper ha cambiato unicamente i lucchetti sotto accusa che sono stati nuovamente modificati senza troppe esitazioni da un hacker a proprio vantaggio.

Conclusione:

Soprattutto nel caso della seconda falla è evidente che il reato sia imputabile a un attore statale. Queste falle mostrano ancora una volta l'enorme interesse degli hacker nei confronti di componenti TIC centrali. Un ulteriore aspetto evidenziato da questo esempio è il rischio collegato a un blocco consapevole di backdoor e falle. Terzi possono infatti scoprire in qualsiasi momento queste backdoor e utilizzarle per i propri scopi.

In base a quanto riportato da FireEye, anche Cisco, il maggiore provider di servizi di rete del mondo, ha subito un attacco a livello di hardware di rete.[28] Nell'ambito del caso divenuto noto con il nome di «SYNful Knock» sono stati compromessi almeno 14 router in Ucraina, nelle Filippine, in Messico e in India e sono state installate backdoor. Tuttavia, la quantità di dispositivi infetti è probabilmente molto più elevata.[29] Diversamente dall'incidente Juniper, in questo caso per accedere ai sistemi non è stata sfruttata nessuna falla di sicurezza, ma semplicemente una password di amministrazione. In seguito parti del *firmware* sono state sovrascritte con il malware. Gli hacker hanno acquisito le password attraverso diversi canali e in vari casi hanno utilizzato password standard, il che evidenzia, ancora una volta, la sovente carenza di considerazioni di base relative alla sicurezza.

Il 23 novembre 2015 si è scoperto che Dell salva un proprio *root CA certificate* nell'archivio certificati di Windows come «Autorità di certificazione radice attendibile», con il quale chiunque può emettere certificati validi per apparecchi Dell. Il problema consiste nel fatto che, pur non essendo contrassegnato come esportabile, tale documento può essere tuttavia esportato senza grandi difficoltà, il che consente di intercettare con semplicità collegamenti cifrati di programmi che utilizzano le funzioni API di crittografia (*CryptoAPI*) di Dell mediante «*Man in the Middle*». Ciò è possibile per quasi tutti i programmi Windows. In questo modo, però, è possibile installare facilmente anche malware su un computer Dell. La presenza di una firma non valida impedisce normalmente l'installazione di software non affidabili o, per lo meno, genera un messaggio in cui si chiede all'utente se desidera effettivamente eseguire l'operazione. Questo meccanismo di sicurezza decade nel momento in cui l'hacker è in possesso del certificato root CA e di conseguenza può contrassegnare con una firma valida qualsiasi software (dannoso). Dell ha reagito a tale attacco fornendo un update in grado di rimuovere il certificato.

[28] https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html (stato: 29 febbraio 2016).

[29] http://www.theregister.co.uk/2015/09/22/synful_knock_spreads_embaddened_boxen_in_31_countries/ (stato: 29 febbraio 2016).

Conclusione:

Gli esempi riportati mostrano due concetti fondamentali: in primo luogo gli Stati continueranno a tentare di intercettare comunicazioni per scopi legati ai servizi di informazione. Secondariamente esistono di base due approcci distinti per fare ciò. Da una parte, gli Stati possono assicurarsi un accesso sui nodi e i canali principali delle comunicazioni importanti a livello mondiale. Dall'altro raccolgono informazioni attraverso operazioni mirate, adattate personalmente al fine che si intende raggiungere (ad esempio per infiltrare il computer di un sospettato). A prescindere dai problemi giuridici e politici che il primo metodo innegabilmente comporta (vedi RS 2013 I e II), l'utilizzazione della cifratura delle comunicazioni diminuisce l'utilità dei dati intercettati. L'unica via per salvare in futuro il primo approccio sarebbe proibire o diminuire l'efficacia dei sistemi di cifratura o delle componenti. Il secondo approccio che mira a intercettare l'informazione prima della codificazione o dopo la decodifica, de facto è però autoregolante e autolimitante a causa del dispendio di risorse e della complessità, inoltre comporta dei rischi operativi. Ciò aumenta automaticamente il costo dell'intercettazione che ne limita così il numero possibile.

La discussione sui pro e contro dell'indebolimento della cifratura è già tema di discussione a livello internazionale e si può prevede un aumento della tensione. Proprio in questo senso gli Stati di diritto che, nel quadro della sicurezza sia interna che esterna, non vogliono rinunciare alla possibilità di intercettare delle comunicazioni, dovranno

5.2 Furto di dati

5.2.1 Talk Talk

TalkTalk è un fornitore di servizi di telefonia, Internet e pay-TV britannico. Il 21 ottobre 2015 l'azienda ha subito un attacco informatico attraverso il quale sono stati prelevati dati di quasi 157 000 clienti, in oltre 15 000 casi anche di carattere bancario. Quella descritta non è stata tuttavia la prima aggressione sferrata alla società inglese che già nel dicembre 2014 e nel febbraio 2015 era stata vittima di tentativi di frode realizzati adottando tecniche di social engineering e sfociati nella sottrazione indebita di dati dei clienti.

L'azienda è stata duramente criticata non solo per la gestione dell'episodio in esame e dei suoi processi interni, ma anche per il fatto di non aver tratto alcun insegnamento dagli attacchi precedenti. A essere stigmatizzata è stata soprattutto la mancata codifica dei dati personali al momento del salvataggio.

Diversi esperti sono giunti alla conclusione che l'attacco sia partito da un'iniezione SQL, inviata in contemporanea a un attacco DDoS. Si è ipotizzato che quest'ultima offensiva sia stata utilizzata come «manovra diversiva» al fine di consentire agli hacker di compromettere il sistema mentre l'azienda era impegnata a ripristinare la disponibilità del servizio.[30]

[30] Nonostante non vi sia conferma di ciò, si è accennato a un possibile coinvolgimento di fini estorsivi.

Secondo la prassi normalmente seguita in questi casi, i dati prelevati sono stati successivamente venduti sul mercato nero e utilizzati per frodi mirate ai danni di utenti di TalkTalk.

Quest'episodio sottolinea l'importanza dell'esecuzione dell'analisi del rischio da parte delle aziende che salvano dati personali. In tale ambito queste ultime devono interrogarsi sui mezzi con i quali un criminale potrebbe accedere a queste informazioni e sui rischi che un incidente simile potrebbe comportare per i clienti interessati. Alla luce di tali considerazioni si devono adottare misure di protezione, come la codifica dei dati. Inoltre si dovrebbe definire una procedura chiara da seguire nell'eventualità di un attacco, volta a disciplinare, in particolare, le modalità di comunicazione con le vittime (ovvero con i clienti) e con le autorità competenti.

5.2.2 Altri furti di dati

Il 5 agosto 2015 è stato scoperto un episodio di furto di dati eseguito da un gruppo di hacker che, a quanto pare, sarebbe riuscito a prelevare dati di clienti del gruppo di telecomunicazioni britannico «Carphone Warehouse» per due settimane, copiando illecitamente all'incirca 2,4 milioni di dati, tra cui quasi 90 000 relativi a carte di credito, dai portali come ad esempio OneStopPhoneShop.com, e2save.com e mobiles.co.uk della società di telefonia mobile. I clienti colpiti sono stati informati. Per rispondere alle richieste e ai timori dei clienti è stata istituita una hotline dedicata.

In un altro attacco sferrato contro Experian Irlanda, un'azienda di servizi che verifica la solvibilità di clienti T-Mobile, sembra che tra il 1° settembre 2013 e il 16 settembre 2015 siano stati prelevati complessivamente 15 milioni di dati. Tra le informazioni trafugate figuravano numeri di assicurazioni sociali o di licenze di condurre che, pur essendo criptati, sono stati decodificati. Non sono stati rinvenuti, invece, dati relativi a conti bancari e carte di credito.

Il 28 settembre 2015 anche la piattaforma di crowdfounding «Patreon» è stata vittima di un'acquisizione illecita di dati, attraverso la quale sembra siano stati copiati password, dati fiscali e numeri di assicurazioni sociali cifrati. Per contro gli indirizzi e-mail sono stati sottratti in chiaro. Tra le informazioni prelevate erano contenuti, inoltre, messaggi provenienti dal sistema di messaggeria interno. Pur avendo assicurato agli utenti di aver salvato le password solo criptate, il gestore ha consigliato loro di modificarle. A rendere possibile l'attacco è stato un backup delle banche dati dei sistemi produttivi salvato su un server di test. A quanto pare, in seguito, è stato possibile accedere a tale server attraverso un'applicazione Web che è stata sfruttata dagli hacker. I 2,3 milioni di indirizzi e-mail rubati sono stati pubblicati su Internet. In questo contesto va segnalata, inoltre, un'e-mail di ricatto con la quale i truffatori hanno minacciato i destinatari di pubblicare altri dati sensibili qualora non avessero ricevuto il pagamento di un *bitcoin* entro 48 ore. Non è chiaro se gli hacker possedessero veramente tali dati o se avessero scritto a caso agli indirizzi e-mail resi pubblici.

5.3 Sistemi industriali di controllo

Il pericolo derivante da sistemi industriali di controllo (*denominati ICS o anche SCADA*) che non ricevono una sufficiente protezione viene segnalato da tempo. Attraverso i *controllori a logica programmabile o Programmable Logic Controller (PLC o SPS),* che possono costituire parte di un sistema SCADA collegato in rete e che sono spesso accessibili liberamente da Internet, agli hacker vengono offerte diverse possibilità di contrabbandare malware, per esempio per spiare sistemi industriali. Il software richiesto a tale scopo può essere scaricato liberamente. Spesso tali avvisi vengono liquidati come pericoli in grado di funzionare solo in un ambiente di laboratorio. L'organizzazione di verifica tecnica TÜV-Süd ha mostrato mediante una centrale idroelettrica fittizia esposta su Internet come *honeynet* che anche sistemi apparentemente insignificanti possono subire attacchi di ogni genere[31]. I risultati sono stati pubblicati a fine luglio 2015.

Quasi contemporaneamente all'attivazione di questo sistema esca è stato eseguito il primo accesso alla centrale idroelettrica fittizia. Durante gli otto mesi di sperimentazione gli esperti di TÜV-Süd hanno registrato oltre 60 000 accessi da oltre 150 Paesi. Gli *indirizzi IP* della maggior parte dei tentativi provenivano dalla Cina, dagli USA e dalla Corea del Sud, anche se questi ultimi non hanno permesso di risalire alla sede effettiva dell'utente che effettuava l'accesso. In base alle esperienze raccolte finora in tali casi gli accessi vengono effettuati di norma attraverso indirizzi IP nascosti o falsificati.

I tentativi di accesso a protocolli standard sono molto diffusi. NeI tentativo sopra descritto sono state tuttavia osservate richieste presentate attraverso protocolli industriali come Modbus/TCP o S7Comm. L'episodio in esame mostra ai gestori di tali impianti che le falle di sicurezza presenti nella configurazione vengono ricercate, individuate e in seguito sfruttate.

L'esempio descritto nel capitolo 5.3.1 che segue si riferisce al primo blackout di vaste proporzioni imputabile principalmente a un attacco cibernetico e dimostra che l'interesse degli hacker non è rivolto solo a sistemi fittizi, ma anche ad altri ambiti, come per esempio quello degli apparecchi medici (cap. 5.3.3) o delle automobili (cap. 5.3.4), che in futuro verranno presi maggiormente di mira.

5.3.1 Blackout in Ucraina – malware sotto accusa

Poco prima di Natale nella regione ucraina «Ivano-Frankivsk Oblast» 80 000 utenti sono rimasti senza energia elettrica. Diversi fornitori regionali hanno segnalato che i loro sistemi erano stati colpiti da un attacco informatico, a seguito del quale sette sottostazioni da 110 kV e 23 da 35 kV sono state scollegate dalla rete[32].

---

31 http://www.tuev-sued.de/tuev-sued-konzern/presse/pressearchiv/potenzielle-angreifer-sind-ueberall (stato: 29 febbraio 2016).

32 http://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid (stato: 29 febbraio 2016).

12/24/2015

Dear customers!

Dec. 23, 2015, from 15:35 - 16:30, third parties were made illegal entry into information-technological system of remote access to equipment telecontrol substations of 35-110 kV JSC "Kyivoblenergo."

As a result, it was disconnected 7 (seven) 110 kV substations and 23 (twenty three) substation 35 kV. This led to the repayment of about 80,000 different categories of customers on the reliability of electricity supply.

Electricity was restored to all consumers employees of the Company at **18:56** the same day.

We apologize for the situation and thank you for your understanding.

PJSC "Kyivoblenergo"

Figura 9: informazione inviata da un fornitore locale ucraino ai clienti

L'attacco alle centrali elettriche è stato sferrato a più livelli: grazie al supporto internazionale, il CERT ucraino (CERT-UA) è riuscito a identificare sui computer delle società elettriche colpite diverse versioni (BE2 e BE3) del malware «BlackEnergy» (BE). Il blackout non può essere, tuttavia, imputato unicamente alla presenza di tale software dannoso[33].

Allo stato attuale delle conoscenze, l'iter più probabile seguito dai malfattori pare essere il seguente: i computer della rete delle società elettriche in questione sono stati infettati tramite *spear phishing* e allegati Office appositamente creati a tale scopo. Con l'aiuto del malware BlackEnergy gli hacker hanno setacciato la rete, procurandosi così l'accesso ad altri apparecchi, compresi quelli degli operatori, su cui erano installate le consolle SCADA per la gestione delle sottostazioni. Il blackout è stato probabilmente causato dall'azionamento degli interruttori all'interno di tali consolle, eseguito esattamente come avrebbe fatto un operatore legittimo in loco per scopi di manutenzione. Per impedire il ripristino della fornitura d'energia i truffatori si sono serviti anche del malware «*KillDisk*», che ha reso inutilizzabili gli hard disk dei computer sabotati e ha eliminato le possibilità di trovare delle tracce e, contemporaneamente, hanno sovraccaricato il sito Web e il call center dell'azienda con *attacchi DDoS* per ostacolare la segnalazione degli incidenti e la comunicazione con i clienti.[34]

Poco dopo i fatti sopra descritti, i rappresentanti del governo ucraino hanno attribuito la colpa dell'accaduto alla Russia, reiterando la stessa accusa anche a gennaio 2016, in seguito al ritrovamento, pur senza danni, di BlackEnergy nella rete dell'aeroporto «Boryspil» di Kiev. Non esistono tuttavia prove a sostegno di tali accuse. L'agenzia di sicurezza «iSight Partners» presuppone che dietro l'attacco si nasconda il team «Sandworm» che in episodi di sabotaggio precedenti aveva agito in modo analogo nell'interesse del governo russo.

---

33 https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B (stato: 29 febbraio 2016).

34 http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/ (stato: 29 febbraio 2016).

BlackEnergy, tuttavia, è un malware molto utilizzato e inoltre è disponibile in parte anche sul mercato nero, il che complica ulteriormente l'attribuzione della paternità degli attacchi.

Conclusione e raccomandazione:

L'episodio descritto è il primo massiccio blackout da ricondurre principalmente a un cyber-attacco. I gestori delle infrastrutture colpite possono sfruttare quanto appreso attraverso tale episodio per potenziare le proprie reti e apparecchiature rendendole più forti contro offensive analoghe.

MELANI mette a disposizione una lista di controllo per la protezione dei sistemi industriali di controllo. Le misure indicate dovrebbero essere integrate in un processo di sicurezza sovraordinato che ne garantisca l'applicazione, una verifica regolare e un costante miglioramento. È altresì importante che il gestore di questo impianto conosca la propria situazione attuale di minaccia, la verifichi regolarmente e faccia confluire gli insegnamenti nell'implementazione e nel miglioramento delle misure di sicurezza. A tale scopo è necessaria una stretta collaborazione tra gli ambiti della gestione dei rischi, della engineering e della gestione aziendale.

DOCU

Misure di protezione dei sistemi industriali di controllo (ICS)

https://www.melani.admin.ch/melani/it/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-industriellen-kontrollsystemen--ics-.html

5.3.2 Manipolazioni tramite automazione basata su dati nella fornitura di gas e petrolio

Il timore di attacchi a sistemi di gestione di processi critici si è diffuso fin da prima dell'avvento di Stuxnet. Come già supposto nel precedente capitolo su BackEnergy, non deve essere necessariamente il sistema di gestione a essere violato in modo diretto: i processi possono essere, infatti, influenzati anche attraverso la manipolazione di dati in sistemi contigui. Nel novembre 2015, alla conferenza «Black Hat Europe», Alexander Polyakov e Mathieu Geli della società di sicurezza «ERPScan» hanno illustrato come le valvole degli oleodotti utilizzati nell'industria del gas e del petrolio possano essere influenzate mediante la manipolazione di *sistemi ERP*.[35] Secondo gli esperti ERP, l'ambiente di sistema complesso e in molti settori automatizzato (cfr. in merito fig. 10) può essere attaccato in tre modi.

Uno di questi prevede la falsificazione di variabili come temperatura e pressione all'interno di un'applicazione per la gestione delle risorse, il che comporta un oneroso invio di team di manutenzione, nella peggiore delle ipotesi verso una piattaforma petrolifera posizionata in mezzo all'oceano. Inoltre la modifica mirata dei livelli e capacità dei serbatoi può provocare,

[35] https://www.blackhat.com/docs/eu-15/materials/eu-15-Polyakov-Cybersecurity-For-Oil-And-Gas-Industries-How-Hackers-Can-Manipulate-Oil-Stocks-wp.pdf (stato: 29 febbraio 2016).

nell'eventualità più catastrofica, esplosioni. Per aumentare l'efficienza è consentito inviare determinati comandi da sistemi terzi al livello di controllo. Di conseguenza, in questo caso, per eseguire un sabotaggio non è necessaria nemmeno la presenza di falle di sicurezza all'interno del sistema di controllo.

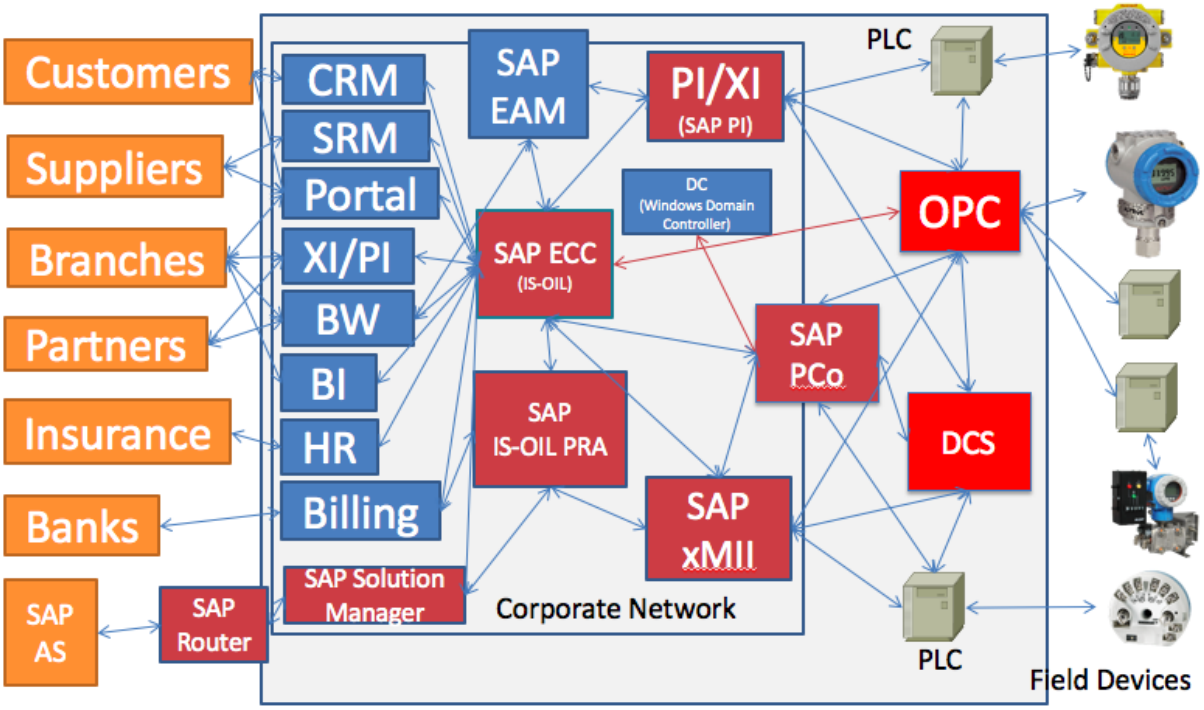

Figura 10: esempio di ambiente di sistema nell'industria del gas e del petrolio. Fonte: Alexander Polyakov e Mathieu Geli

Conclusione:

L'esempio illustra la problematica legata all'automazione basata su dati. La diffusione sempre più ampia dei contatori intelligenti («smart meter») non solo apre la strada a processi commerciali più efficienti, ma anche a vettori di attacco più efficaci in caso di utilizzo improprio.

5.3.3 Possibili attacchi via Internet di migliaia di apparecchi medici

Negli ospedali spesso bisogna agire in fretta. La vita delle persone dipende da decisioni basate su dati diagnostici e di laboratorio che devono essere immediatamente a disposizione del personale curante. Anche in relazione alla configurazione delle apparecchiature mediche e delle rispettive interfacce per amministrare i dati dei pazienti, sembra che, spesso, si tenda a dare maggior importanza alla velocità e alla facilità d'uso a discapito degli aspetti tecnici di sicurezza.

Alla conferenza sulla sicurezza «Derbycon 2015»[36] i ricercatori Scott Even e Mark Collao hanno presentato i risultati di uno studio in base al quale presso una sola impresa attiva nel campo della sanità oltre 68 000 apparecchi medici sarebbero accessibili via Internet e quindi preda di possibili attacchi. Il fatto che simili attacchi si verifichino concretamente è stato dimostrato dai risultati di dieci sistemi *honeypot* che sono stati spacciati per defibrillatori o sistemi RM. Gli apparecchi-esca sono stati attaccati 299 volte da malware e, in 24 casi, gli attacchi sono riusciti.

I rischi in campo medico non si limitano tuttavia agli accessi non autorizzati alle apparecchiature mediche. Negli ultimi tempi si è parlato molto spesso anche dell'accesso a dati sanitari degni di particolare protezione[37]. In alcuni casi sono i pazienti stessi a mettere ea repentaglio la sicurezza dei propri dati servendosi di app non sicure. Pur essendo state autorizzate dall'autorità sanitaria britannica NHS, 23 delle 79 app testate dall'«Imperial College»[38] non sono dotate di alcun meccanismo di cifratura[39]. In quattro applicazioni i dati sanitari sono stati trasmessi addirittura in chiaro.

5.3.4 L'auto intelligente – la responsabilità dell'industria automobilistica

La scena potrebbe essere tratta da un film dell'orrore: viaggiando in macchina in una giornata estiva, il riscaldamento inizia a funzionare a pieno regime, la radio si sintonizza improvvisamente su un canale specializzato, il tergicristalli si mette in azione e sul display di navigazione appare un volto ignoto che annuncia di aver preso il controllo del veicolo. Poco dopo non è più possibile né accelerare né frenare.

Anche se finora nella realtà attacchi di questo tipo non si sono mai verificati, essi non sono il frutto di pura fantasia: una falla nel sistema di infotainment «Uconnect» ha consentito a due ricercatori in sicurezza informatica, Miller e Valasek, di assumerne il controllo a distanza[40]. Per farlo è bastato loro conoscere l'*indirizzo IP* del sistema. Una volta assunto il controllo del sistema, hanno potuto inserire il loro codice nel firmware di Uconnect per accedere ai processori più vicini alle componenti elettroniche di controllo. Servendosi della rete di comunicazione interna, il cosiddetto Controller Area Network *Bus*, hanno quindi potuto impartire ordini al motore e ai freni e sottrarre al conducente il controllo del veicolo manovrandolo a distanza.

I ricercatori hanno presentato i loro risultati alla «Conferenza Black Hat 2015» insieme al *patch*[41] elaborato in collaborazione con l'azienda «Fiat-Chrysler» e il partner di

---

36 http://www.irongeek.com/i.php?page=videos%2Fderbycon5%2Fbreak-me14-medical-devices-pwnage-and-honeypots-scott-erven-mark-collao (stato: 29 febbraio 2016).

37 http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720 (stato: 29 febbraio 2016). http://www.huffingtonpost.com/2015/03/17/premera-blue-cross-cybera_n_6890194.html (stato: 29 febbraio 2016).

38 https://www.imperial.ac.uk (stato: 29 febbraio 2016).

39 http://www.theguardian.com/society/2015/sep/25/nhs-accredited-health-apps-putting-users-privacy-at-risk-study-finds (stato: 29 febbraio 2016).

40 http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (stato: 29 febbraio 2016).

41 https://ics-cert.us-cert.gov/advisories/ICSA-15-260-01 (stato: 29 febbraio 2016).

telecomunicazioni coinvolto «Sprint». Questo scenario ha destato grande scalpore nell'industria automobilistica e presso l'opinione pubblica, anche se l'episodio è stato presto dimenticato, perché i consumatori apprezzano la possibilità di controllare alcune funzioni del proprio veicolo in tutta comodità servendosi della relativa app per smartphone.

Resta da sperare che vengano prese sul serio le preoccupazioni in materia di separazione tra sicurezza dell'elettronica d'intrattenimento e quella dell'elettronica di controllo, poiché di giorno in giorno emergono nuovi vettori di potenziali attacchi. Per esempio, è già possibile neutralizzare gli immobilizzatori delle chiavi elettroniche[42] o assumere il controllo dei comandi tramite i sistemi di intrattenimento manipolando i segnali[43].

Conclusione:

Affidare responsabilità sempre maggiori alle auto intelligenti fa sorgere necessariamente nuovi problemi. Per quel che riguarda gli autoveicoli autonomi e intelligenti in grado di autoregolarsi come i sistemi Car2X, i confini tra sicurezza fisica e sicurezza dell'informazione si fanno sempre più labili, il che nella migliore delle ipotesi porterà l'intensità dei test sui sistemi TIC agli stessi livelli dei crashtest.

5.3.5 Piratato per rappresaglia il controllo di una diga di sbarramento

Pare che nel 2013 presunti hacker iraniani siano riusciti a entrare nei sistemi di controllo di una diga di sbarramento nei pressi di New York. È quanto riportato dal Wallstreet Journal[44] nel dicembre 2015 in riferimento a due persone incaricate delle indagini. La diga, di piccole dimensioni, dovrebbe essere stata attaccata nell'ambito delle azioni di rappresaglia adottate in seguito alla scoperta del sabotaggio Stuxnet. È importante imparare dall'analisi di simili «casi marginali» e continuare a migliorare nel campo delle misure preventive delle infrastrutture di importanza critica.

5.4 Attacchi a siti Web: DDoS e defacement

5.4.1 Il gruppo New World Hacking si spinge oltre gli obiettivi prefissati dall'attacco test alla BBC

Per molti cittadini britannici che la sera di San Silvestro avrebbero voluto guardare la trasmissione preferita sulla BBC prima di dare inizio alle festività o magari beneficiare dell'accompagnamento dell'app di radio BBC la delusione è stata grande. Sulle pagine web della BBC appariva unicamente un messaggio di errore (cfr. fig. 11).

---

42 http://www.heise.de/make/meldung/Wegfahrsperre-VW-Hack-ist-offen-2778194.html (stato: 29 febbraio 2016).

43 http://www.bbc.com/news/technology-33622298 (stato: 29 febbraio 2016).

44 http://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559 (stato: 29 febbraio 2016).

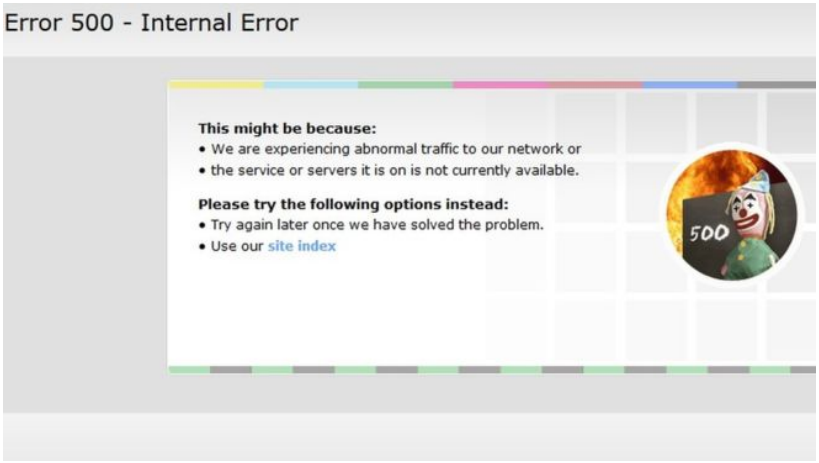

Figura 11: messaggio di errore apparso sul sito Web della BBC la sera di San Silvestro del 2015[45]

Secondo il gruppo «New World Hacking», il guasto di varie ore non era dovuto a un problema tecnico, bensì a un test che il gruppo aveva eseguito per mettere alla prova le proprie capacità. Uno degli hacker che si fa chiamare «Ownz» avrebbe raccontato al corrispondente in tecnologia della BBC Rory Cellan-Jones di essere uno dei responsabili dei presunti cyber-attacchi DDoS. In realtà le attività del gruppo miravano a contrastare la presenza online dello Stato islamico. Il gruppo aveva scelto la BBC come obiettivo per una dimostrazione allo scopo di sperimentare il suo nuovo strumento «Bangstresser». Secondo le affermazioni degli hacker non era loro intenzione provocare un'interruzione di simili proporzioni. La portata dell'infrastruttura offensiva ha sorpreso i suoi stessi autori.

5.4.2 Anonymous contro ISIS – La guerra della propaganda in rete

Già in seguito agli attacchi terroristici contro il giornale satirico «Charlie Hebdo» nel gennaio 2015 il collettivo di hacker «Anonymous» aveva lanciato la campagna «#OpISIS», nella quale cercava soprattutto di sabotare i canali di comunicazione online dei presunti terroristi e di ostacolare il reclutamento di nuovi membri. All'indomani del nuovo attacco di Parigi, il gruppo di hacker ha diffuso in Internet un videomessaggio in cui dichiarava guerra allo Stato islamico[46].

Poiché Anonymous non dispone di una struttura chiaramente definita, le misure che hanno fatto seguito agli attacchi non sono state ben coordinate. Per esempio si è discusso a lungo della necessità di dare avvio, accanto all'attuale #OpISIS, ad un'operazione separata denominata «#OpParis». Altre divergenze di opinione in merito al senso di una dichiarazione di guerra e di altri annunci di sottogruppi hanno spinto il collettivo di hacker a pubblicare un comunicato stampa il 18 novembre 2015[47]. In tale documento erano presentati gli obiettivi del gruppo in merito alle attività correnti nonché consigliati i canali di comunicazione preferiti. Il sottogruppo «Ghost Security (GhostSec)» ha puntato sull'identificazione e sul blocco di conti sui social media in relazione con l'organizzazione terroristica. La cooperazione

[45] http://www.bbc.com/news/technology-35213415 (stato: 29 febbraio 2016).
[46] https://www.youtube.com/watch?v=RwGGcZoRs-k (stato: 29 febbraio 2016).
[47] https://www.docdroid.net/hUQ7Ez2/anonymous-operations-isis-11-2015.pdf.html (stato: 29 febbraio 2016).

sporadica di GhostSec con autorità statali non è stata approvata da tutti i membri di Anonymous.

Oltre a un appello[48] a partecipare al «Trolling Day» l'11 dicembre 2015, nel corso del quale ci si faceva beffa dei terroristi dell'IS, sono state soprattutto le attività di «*Doxing*» del gruppo GhostSec ad attirare l'attenzione della stampa. Con il doxing vengono svelate pubblicamente le vere identità e i luoghi di residenza delle persone che si celano dietro ai conti dei social media e dietro ai siti Web. Oltre a una serie di istruzioni[49] per proteggersi meglio online, non è stata osservata alcun'altra reazione da parte dell'IS. Nelle istruzioni l'IS raccomanda, oltre a molte applicazioni, anche gli operatori svizzeri «Swisscom IO» e «Threema» nonché le soluzioni di comunicazione della ditta ginevrina «Silent Circle». È possibile che queste ditte o i loro clienti diventino un obiettivo degli hacker per via di questa pubblicità.

5.4.3 Codici QR manipolati

I codici a barre e, negli ultimi tempi, anche i codici bidimensionali QR sono usati negli ambiti più disparati. Tutti conoscono i codici a barre presenti sugli imballaggi dei prodotti, che non contengono unicamente indicazioni sul prezzo, ma anche molte altre informazioni. Il codice QR viene impiegato anche nei trasporti aerei per identificare i passeggeri durante le operazioni di imbarco.

Il rischio finora sollevato dall'impiego di tali codici è stato soprattutto quello relativo all'uso improprio delle informazioni in essi contenute. Tuttavia il ricercatore in sicurezza informatica Yang Yu ha potuto dimostrare che i codici stampati possono essere usati anche come strumento per attaccare i sistemi computerizzati di lettura dei dati[50]. Il ricercatore ha pubblicato vari video intitolati «Badbarcode» e presentato i propri risultati alla conferenza «PacSec» 2015 di Tokyo. Yang Yu ha usato una serie di falle presenti nei programmi usati per scansionare i codici. Stampando i codici a barre da lui manipolati, il ricercatore è riuscito a spingere i sistemi di scansione non solo a leggere informazioni, ma anche a eseguire dei comandi.

Nonostante finora non siano note applicazioni malevole di questo tipo, il ricercatore sottolinea il fatto che queste falle costituiscono un potenziale rischio.

5.5 Crimeware

5.5.1 Nuovi TLD e malware

Vari Top Level Domain (TLD) presentano livelli di sicurezza diversi. Quindi non c'è da stupirsi se i gruppi criminali prediligono alcuni TLD rispetto ad altri. Con l'introduzione di TLD generici i cybercriminali hanno trovato nuove opportunità per avere accesso a domini a

---

48 https://ghostbin.com/paste/ucsf3 (stato: 29 febbraio 2016).

49 http://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/ (stato: 29 febbraio 2016).

50 http://motherboard.vice.com/read/badbarcode-project-shows-customized-boarding-passes-can-hack-computers (stato: 29 febbraio 2016).

basso costo e privi di controllo. Le loro infrastrutture di comando e controllo si trovano quindi in questi domini. Tuttavia anche i domini più noti (p.es. .com o .biz) sono molto spesso preda della cybercriminalità.

Secondo ntldstats.com, i seguenti TLD generici contengono il numero più elevato di malware:

* .science
* .click
* .link
* .party
* .xyz

I nomi a dominio di alcuni Paesi sono regolarmente sfruttati in maniera fraudolenta da gruppi di cybercriminali. Le ragioni sono molteplici: per esempio, il centro di registrazione «freenom.com» ha offerto la possibilità di registrare gratuitamente vari TLD di Paesi africani, il che ha provocato un forte aumento delle registrazioni di nomi di domini a scopi criminali in questi Paesi.

Domini di Paesi con un'elevata quota di malware sono per esempio:

.gq (Guinea Equatoriale)
.tk (Tokelau)
.ga (Gabon)
.cf (Repubblica Centrafricana)
.ml (Mali)

Tuttavia i registri e i centri di registrazione devono disporre di regole chiare contro gli abusi che determinino in maniera chiara a che cosa si va incontro in caso di uso improprio di un dominio. Va da sé che essi devono essere responsabili anche dell'applicazione di tali regole. Per fare ciò servono processi collaudati e appositi abuse team in grado di occuparsi dei casi e di risolverli rapidamente. Nel capitolo 6.2 sono riportate maggiori informazioni sulla lotta contro l'uso improprio di nomi di dominio svizzeri.

5.6 Altri temi

5.6.1 Sudori freddi per Android

Il 27 luglio 2015 è stata resa nota una falla scoperta dall'agenzia di sicurezza «Zimperium» che consentiva agli hacker di accedere ai dati degli smartphone Android tramite MMS e senza alcuna interazione da parte degli utenti. In base alle stime, sarebbero stati colpiti fino al 95 per cento di tutti gli smartphone Android. Per sfruttare questa falla, gli hacker dovevano semplicemente inviare alle vittime un apposito messaggio MMS che non aveva neppure bisogno di essere aperto, visto che lo smartphone risultava colpito non appena il messaggio veniva elaborato dal sistema. Fino alla pubblicazione e all'impiego del relativo aggiornamento, l'unico rimedio possibile era quello di disattivare la funzione di ricezione dei messaggi MMS. «Deutsche Telekom» aveva persino sospeso temporaneamente il recapito di messaggi MMS al fine di proteggere la clientela da potenziali attacchi.

6 Tendenze e prospettive

6.1 Mobile Payment

La Svezia si accinge a diventare il primo Paese ad abolire l'uso delle banconote. Mentre fino a una decina di anni fa sarebbe stato impensabile ipotizzare che le carte di credito o di debito avrebbero sostituito il denaro contante, oggi, in Scandinavia, perfino ai mercatini di Natale vengono accettati quasi unicamente pagamenti digitali. Le previsioni odierne vedono lo smartphone come sostituto delle suddette carte di pagamento e il Mobile Payment come il metodo di pagamento del futuro. In America quattro acquirenti su dieci hanno affermato di averlo già utilizzato almeno una volta e, secondo il sito «The Statistic Portal», la tendenza seguirà una crescita progressiva del 20 per cento annuo circa. La Svizzera fatica, invece, a introdurre i dispositivi di *Mobile Payment*, anche se il pagamento senza contanti è una realtà già consolidata da tempo all'interno del Paese che offre tale servizio già dal 2011, anno dell'introduzione sul mercato del brand «Mobino».

Tale argomento è divenuto d'attualità solo da qualche mese con l'entrata in campo dei pezzi da novanta. Dalla fine del 2015 presso oltre 3000 casse delle «Coop» di tutto il Paese si può trovare l'esagono verde di «Twint», il servizio di «PostFinance» che permette di effettuare pagamenti tramite cellulare in alcuni punti vendita dotati di appositi terminali *Bluetooth.* «Paymit», l'alternativa offerta da «UBS» in collaborazione con «SIX» e con la «Zürcher Kantonalbank», ha vinto nel 2015 il premio come migliore applicazione svizzera e, con oltre 170 000 download, si posiziona come il servizio di pagamento tramite smartphone più diffuso in Svizzera. Anche altri operatori continuano a sfornare proposte sempre nuove: «Migros», «Manor» e «Starbucks» permettono ora ai propri clienti di saldare il proprio conto tramite cellulare e di recente ha visto la luce «Swiss One Wallet», la piattaforma per pagamenti digitali in negozi online e mezzo di pagamento tramite smartphone, gestita dalle aziende «Aduno», «Swisscard» e «Netcetera». Ai servizi citati si aggiungono poi i prodotti di aziende come Apple, Facebook e Google. Per il momento, però, nonostante le molteplici offerte, l'utilizzo di questi servizi sembra faticare a prendere piede. A prescindere dal fatto che gli individui tendono a modificare le proprie abitudini molto lentamente, alcuni dei motivi che determinano questo procedere flemmatico sono: il numero e la scarsa visibilità dei fornitori, il timore dei clienti per la sicurezza dei propri dati e, infine, la scelta da parte di alcuni fornitori di servizi di tecnologie poco diffuse o mal supportate dalla telefonia cellulare. Il fallimento di «Tapit», l'app per i pagamenti di Swisscom, potrebbe dipendere per esempio anche dal fatto che il metodo di comunicazione *Near Field Communication (NFC)* utilizzato, è stato a lungo disponibile solo per possessori di Android ma non per utenti Apple. Il colosso dell'informatica infatti, ha introdotto questa tecnologia solo a partire dall'IPhone 6.

Ogni app offre un servizio leggermente differente, con tecnologie diverse e indirizzate a una clientela eterogenea. Le analisi che seguono si limitano pertanto a quelli che si prevede essere i principali protagonisiti di questo business in Svizzera: Paymit e Twint.

Il debutto di Paymit presso i primi commercianti è avvenuto nel mese di febbraio di quest'anno e, a partire dal secondo trimestre del 2016, l'app potrà essere utilizzata anche per acquisti online. L'applicazione consente di effettuare anche pagamenti mobili tra privati. Per iscriversi a Paymit non è necessario essere un cliente UBS, ma occorre possedere un numero telefonico e un conto bancario svizzeri e una carta di credito o prepagata. Le

transazioni vengono effettuate direttamente sul conto bancario e vengono controllate dalla banca, proprio come per i pagamenti classici. In caso di furto l'applicazione è protetta da un codice di sicurezza, mentre non viene richiesta alcuna autorizzazione supplementare per effettuare un pagamento. Inoltre, per limitare i rischi, è stato fissato un limite di prelievo giornaliero di 500 franchi che può essere, tuttavia, aumentato.

Oltre a consentire l'esecuzione di pagamenti in centri commerciali tramite Bluetooth, Twint è un sistema peer-to-peer che permette di effettuare pagamenti tra privati e presso alcuni e-shop. Twint non è appannaggio dei clienti PostFinance, anche se il collegamento diretto con un conto bancario può essere effettuato solo con sei banche partner. A differenza di Paymit non è necessario possedere una carta di credito, in quanto la somma di denaro desiderata viene caricata direttamente sul «portafoglio digitale» dell'app tramite carta PostFinance, addebito diretto (LSV), bollettino di versamento o carta prepagata Twint. Per quanto riguarda le prescrizioni di sicurezza l'importo massimo è limitato a 3 000 franchi e l'età minima per l'utente è fissata a dodici anni.

Pur essendo di per sé abbastanza sicura in quanto supporta sia l'uso dell'autenticazione tramite password sia l'uso della crittografia, la tecnologia Bluetooth non è totalmente priva di pericoli. «Cabir», il primo virus per smartphone, si diffuse proprio tramite questo canale e il programma di spionaggio «Flame» scoperto da Kaspersky Lab nel maggio del 2012 era in grado, tra l'altro, di accedere alla rubrica telefonica tramite Bluetooth.

Il Mobile Payment è quindi un servizio semplice e pratico che, pur presentano la stessa percentuale di rischio di cadere fisicamente in mani sbagliate che ha un portamonete fisico, gode in più della precauzione di un codice PIN che al borsellino classico manca. Questo portamonete moderno ha però lo svantaggio di attirare anche malfattori ben più scaltri dei tipici borseggiatori. Sulla rete si muovono criminali informatici che studiano sempre nuovi metodi per ottenere accesso remoto a qualsiasi tipo di apparecchio collegato a Internet e redditizio per i loro scopi. Limiti di prelievo bassi potrebbero scoraggiare temporaneamente gli attacchi, ma non appena il guadagno dovesse diventare più allettante non si escludono tecniche quali «*Man in the Middle*» o tramite ingegneria sociale che dirottino il saldo richiesto su un ricevente diverso da quello auspicato.

Raccomandazione:

- Disattivare il Bluetooth quando non viene utilizzato.
- Mantenere ridotti i limiti di prelievo.
- Attivare le impostazioni di sicurezza del telefono cellulare (p. es. il codice PIN).

Protezione di base, Periferia e strumenti:

https://www.melani.admin.ch/melani/it/home/schuetzen/sekundaere-grundschutz.html

6.2 Lotta contro l'uso improprio di numeri di telefono e nomi di dominio svizzeri

Con l'avvento di Internet il settore delle telecomunicazioni si è arricchito di nuovi elementi d'indirizzo: i nomi di dominio e gli indirizzi IP. Mentre questi ultimi non vengono gestiti da autorità statali, a ogni Stato è stato assegnato un dominio di primo livello (Top Level Domain) costituito dalle due lettere della rispettiva abbreviazione ISO con il quale può conferire nomi di dominio. Alla Svizzera è stato assegnato il dominio nazionale «.ch» che viene amministrato da e per conto dell'Ufficio federale delle comunicazioni (UFCOM). La Svizzera ha scelto un regime molto libero per l'attribuzione dei nomi di dominio che consente sostanzialmente a chiunque di registrare e utilizzare un nome di dominio «.ch» in tutto il mondo. Tuttavia per contrastare con efficacia gli utilizzi impropri sono state adottate diverse misure di sostegno tra cui, per esempio, quella che prevede la possibilità per un'autorità svizzera, nell'ambito dell'esecuzione dei suoi compiti, di richiedere a un registrant estero di indicare un indirizzo postale in Svizzera[51] al fine di consentire il recapito di lettere ufficiali. Tutto ciò con lo scopo di evitare procedure amministrative o d'assistenza giudiziaria, il più delle volte lunghe e complesse e non generare controversie sulla competenza e sul diritto applicabile. Sui domini svizzeri si applica il diritto svizzero che può essere fatto valere attraverso il meccanismo sopra indicato. Questo processo richiede tuttavia del tempo (occorre indicare un termine al registrant per poter adempiere all'invito). Pertanto per i casi in cui, con l'ausilio di nomi di dominio svizzeri, vengono create minacce acute per gli utenti Internet è stata istituita una competenza per il blocco immediato di domini in presenza di *phishing* e *malware*.[52] L'applicazione coerente di quest'ultima, in particolare a livello di gestore del registro, ha portato a un comprovato consolidamento della buona reputazione e della sicurezza nell'ambito del dominio .ch.[53]

Anche gli elementi d'indirizzo tradizionali beneficiano di nuovi impulsi: la *telefonia via Internet*, infatti, non è rimasta a lungo l'unica a utilizzare il Web. Inoltre per quasi tutti i collegamenti telefonici tradizionali le chiamate vengono effettuate attraverso *reti IP* non appena è stato superato l'«ultimo miglio» che collega il cliente alla rete dell'operatore. Di conseguenza sussistono diverse possibilità per utilizzare le interfacce tra Internet e la rete telefonica: attraverso la telefonia via Internet è possibile per esempio effettuare telefonate verso linee telefoniche di Paesi lontani pagando la tariffa locale in quanto l'operatore dispone di un collegamento in tale Paese. O ancora un operatore internazionale può offrire ai propri clienti una hotline alla tariffa locale in quanto ha attivato un numero in ciascun Paese.

Tuttavia, per poter effettuare telefonate in uscita tecnicamente non è più necessario disporre di un numero di chiamata proprio. Il numero che viene visualizzato in caso di chiamata può essere definito liberamente e può essere oggetto di *spoofing*. Negli ultimi anni la Segreteria di Stato dell'economia (SECO) ha registrato un netto aumento dei reclami dovuti a telefonate

---

51 Art. 23 cpv. 3 ODIn: https://www.admin.ch/opc/it/classified-compilation/20141744/index.html#a23 (stato: 29 febbraio 2016).

52 Art. 15 ODIn: https://www.admin.ch/opc/it/classified-compilation/20141744/index.html#a15 (stato: 29 febbraio 2016).

53 https://www.switch.ch/it/news/cybercrime/ (stato: 29 febbraio 2016).

pubblicitarie indesiderate,[54] contro le quali non è possibile intervenire in alcun modo attraverso misure amministrative a livello di numeri telefonici. Per poter procedere contro questi mittenti è necessario avviare una procedura internazionale generalmente lunga e complessa, tipicamente contro i fornitori dei prodotti e dei servizi che vengono reclamizzati per telefono. È pressoché impossibile contrastare e perseguire gli autori di chiamate fraudolente, come per esempio coloro che si spacciano per collaboratori del supporto Microsoft[55]. Il ricorso all'assistenza giudiziaria internazionale costituisce un grande ostacolo.

Spesso la telefonata viene interrotta dopo il primo squillo in modo da indurre il destinatario a richiamare. Per farlo è necessario un numero di telefono valido. Disporre di un numero svizzero rispetto a uno estero aumenta notevolmente la probabilità che una persona richiami. Spesso i truffatori indicano sui siti Web utilizzati per sferrare i loro attacchi dei numeri svizzeri funzionanti per guadagnarsi la fiducia delle potenziali vittime.

La Segreteria di Stato dell'economia (SECO) contrasta le telefonate pubblicitarie sleali intraprendendo azioni penali (spesso contro ignoti) e civili in rapporto a fornitori del servizio di preselezione.[56] Del resto in diversi casi la minaccia di adire le vie legali ha fatto sì che diverse società di telecomunicazioni revocassero numeri di telefono utilizzati in modo indebito.

Al livello più elevato i numeri di telefono vengono amministrati dall'UFCOM che li assegna in blocchi da 10 000 a società di telecomunicazioni (anche estere che devono disporre unicamente di un indirizzo postale in Svizzera) che, a loro volta, li trasmettono in blocchi più piccoli o singolarmente ai propri clienti (finali) in Svizzera o all'estero. Alla luce del maggior numero di segnalazioni ricevute inerenti l'utilizzo improprio di numeri di telefono svizzeri, l'anno scorso le possibilità di revoca dell'attribuzione da parte dell'UFCOM sono state ampliate.[57]

Inoltre l'11 dicembre il Consiglio federale ha avviato la consultazione relativa al progetto di modifica della legge sulle telecomunicazioni e della legge federale contro la concorrenza sleale (LCSI). La modifica si prefigge, tra le altre cose, di migliorare l'insieme degli strumenti tecnici e giuridici da utilizzare contro le telefonate pubblicitarie indesiderate. In questo modo, come per la lotta agli spam, i fornitori di servizi di telecomunicazioni dovranno essere tenuti a filtrare le telefonate pubblicitarie.

---

54 http://www.seco.admin.ch/themen/00645/00653/05456/index.html?lang=de; cfr. anche opuscolo «Stop alle telefonate pubblicitarie indesiderate»: https://www.seco.admin.ch/seco/it/home/Publikationen_Dienstleistungen/Publikationen_und_Formulare/Werbe_und_Geschaeftsmethoden/Unlauterer_Wettweberb/ruhe-vor-unerbetenen-werbeanrufen_seco.html (stato: 29 febbraio 2016).

55 Cfr. bollettino d'informazione MELANI https://www.melani.admin.ch/melani/it/home/themen/fake_support.html (stato: 29 febbraio 2016).

56 http://www.seco.admin.ch (stato: 29 febbraio 2016).

57 Cfr. art. 11 dell'Ordinanza concernente gli elementi d'indirizzo nel settore delle telecomunicazioni (ORAT): https://www.admin.ch/opc/it/classified-compilation/19970410/index.html#a11 (stato: 29 febbraio 2016).

Conclusione:

Quanto più l'assegnazione degli elementi d'indirizzo è libera, tanto più semplice deve essere l'organizzazione delle competenze e delle misure in caso di revoca per uso improprio, in modo da poter salvaguardare la fiducia negli elementi d'indirizzo di un'autorità di assegnazione. Questo principio è stato riconosciuto anche da alcuni operatori di nuovi ambiti di nomi di dominio (new gTLDs): per i nomi di dominio che possono essere acquistati in modo semplice e conveniente e che pertanto attirano anche potenziali criminali, i centri di registrazione procedono in parte in modo piuttosto aggressivo in caso di revoca. Diversamente la reputazione del loro TLD potrebbe crollare. Gli utenti Internet potrebbero evitare gli indirizzi con tale suffisso o addirittura filtrarli a livello tecnico. Di conseguenza ciò potrebbe dissuadere anche attori seri dalla registrazione di tali indirizzi.

Questo problema non pare interessare i numeri di telefono; si deve tuttavia considerare che nei confronti dei numeri di telefono svizzeri viene riposta tradizionalmente un'ampia fiducia (per lo meno all'interno del Paese). Per preservare tale situazione l'abuso deve essere il più possibile evitato e, all'occorrenza, contrastato in modo efficace.

6.3 Quando gli hacker entrano nella sala giochi

Svariati sono i giocattoli attraverso i quali, negli anni, i bambini si sono approcciati al mondo degli adulti: bambolotti da cullare e nutrire, macchinine da lanciare a tutta velocità, casette da arredare, cucinette per sfornare leccornie in plastica. In una realtà digitale anche le preferenze dei bambini subiscono delle variazioni: se i genitori passano buona parte del loro tempo tra computer e smartphone, i bambini provano il desiderio di emularli e il mercato del giocattolo si adegua producendo tablet per i più piccoli e bambole hi-tech. L'Internet delle cose si apre all'infanzia portando con sé i suoi pregi e i suoi pericoli.

A metà novembre 2015 il produttore di applicazioni tecnologiche per bambini e di giochi digitali «VTech Holdings Ltd», con sede a Hong Kong, è stato vittima di uno dei più grandi attacchi hacker di tutti i tempi. A essere violati sono stati il database dell'App Store «Learning Lodge», negozio online da cui gli utenti possono scaricare app, giochi, video, e-book, i database del social network «Kid Connect», con cui genitori e figli possono comunicare tra di loro tramite tablet e smartphone, e la banca dati «PlanetVTeach».

Il responsabile, dopo aver ottenuto l'accesso root tramite *SQL injection* ed essere entrato in possesso di 5 milioni di account di adulti e di 6,3 milioni di dati di minori, ha contattato il sito del magazine online «Motherboard» rivelando l'accaduto e affermando che l'attacco avrebbe avuto lo scopo di mettere in luce le scarse misure di sicurezza della ditta. L'azienda, che ha ammesso di non aver protetto la propria rete in modo ottimale, non si è espressa apertamente sull'accusa mossa da Motherbroad, secondo cui foto e video chat dei bambini sarebbero finite nelle mani sbagliate, ma ha confermato il furto di nomi, indirizzi di casa, e-mail e IP, password e relative risposte segrete dei genitori nonché nome, sesso e data di nascita dei bambini, specificando che numeri di previdenza sociale, di patente e di carte di credito non sono stati rubati.

Nel mirino degli hacker è finita anche «Sanrio», ditta giapponese proprietaria del famoso marchio «Hello Kitty», dal cui database, a fine novembre, sono stati sottratti dati personali di 3,3 milioni di utenti. Anche in questo caso non sarebbero state prese misure di sicurezza adeguate.

I casi di VTech e Kittyleaks non sono isolati. «Mattel» e la start-up «Toy-Talk» hanno colmato delle falle che, secondo alcuni esperti di sicurezza informatica, avrebbero potuto trasformare la bambola interattiva «Hello Barbie» in un mezzo di spionaggio. Il giocattolo, collegato a Internet tramite WLAN, è in grado di colloquiare con i bambini, a tale scopo è dotata di un microfono e confronta i dati via WLAN con un server di una ditta terza. Sfruttando questa falla di sicurezza sarebbe stato possibile per esempio assumere il controllo del microfono.

Questi esempi dimostrano che nella società odierna la consapevolezza di quali siano i dati da proteggere con particolare attenzione non sia ancora sviluppata ovunque, in modo omogeneo. Sono proprio i dati dei bambini a essere particolarmente sensibili e a richiedere una protezione adeguata. I giocattoli collegati direttamente a Internet sono un'invenzione relativamente recente e sono destinati a svilupparsi fortemente nei prossimi anni. L'auspicio è che non si investa solo nell'integrazione di nuove funzioni, ma anche nella relativa sicurezza.

Raccomandazione:

- Cambiare di frequente le password.
- Considerare che ogni apparecchio collegato a internet può comportare dei rischi.
- Insegnare la sicurezza ai bambini.
- Per ordinazioni e pagamenti di prodotti dedicati all'infanzia non utilizzare i dati del bambino.

Protezione di base, regole di comportamento:

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

7 Politica, ricerca, policy

7.1 Atti parlamentari

Atto parlamentare	Numero	Titolo	Depositato da	Data del deposito	CN/CS	Ufficio	Stato delle deliberazioni & link
Interpellanza	15.4073	L'esercito è realmente in grado di proteggere il cyberspazio svizzero?	Derder Fathi	25.09.2015	CN	DDPS	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20154073
Postulato	15.5064	Dibattito sul servizio pubblico. Rispondere alle sfide della società dell'informazione e impedire che i canali mediatici innovativi siano discriminati	Balthasar Glättli	25.09.2015	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20154064
Postulato	15.3980	Valutare le opportunità e i rischi dell'Industria 4.0	Gruppo dei verdi	24.09.2015	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153980
Mozione	15.3979	Una piattaforma per l'Industria 4.0	Adèle Thorens Goumaz	24.09.2015	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153979
Postulato	15.3957	Misure contro il commercio illegale on line di specie minacciate	Guillaume Barrazone	24.09.2015	CN	DFI	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153957
Interpellanza	15.3917	Crowdfunding. Conflitti d'interesse tra innovazioni economiche e tutela degli investitori	Konrad Graber	23.09.2015	CS	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153917
Mozione	15.3903	Nessun ulteriore ritardo per i casinò on line	Peter Schilliger	23.09.2015	CN		https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153903
Iniziativa parlamentare	15.482	Parità di trattamento tra emittenti radiotelevisive private e offerenti on line privati	Thomas Matter	22.09.2015	CN	CTT-CN	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20150482
Interpellanza	15.3959	Mantenimento dei servizi e-mail per un periodo limitato in seguito a disdetta	Anita Fetz	24.09.2015	CS	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153959
Interpellanza	15.3882	Rischi per la salute legati all'impiego delle TIC nella società dell'informazione	Thomas Böhni	22.09.2015	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153882
Domanda	15.5466	Engagement der Post bei der Entwicklung einer E-Voting Plattform	Cédric Wermuth	15.09.2015	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20155466

Interrogazione urgente	15.1059	Aiuto finanziario urgente della Confederazione in seguito all'attacco informatico contro TV5 Monde	Didier Berberat	10.09.2015	CS	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20151059
Interpellanza	15.3822	Occorre correggere rapidamente i difetti di gioventù del nuovo abbonamento dei trasporti pubblici "Swiss Pass"	Jean Christophe Schwaab	09.09.2015	CN	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153822
Mozione	15.3799	Decreto concernente la rete delle strade nazionali e vignetta elettronica	Commissione dei trasporti e delle telecomunicazioni CS	18.08.2015	CS	DATEC	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153799
Interpellanza	15.4062	Attuare rapidamente dei progetti per snellire la burocrazia	Hans Grunder, gruppo BD	25.09.2015	CN	DEFR	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20154062
Interpellanza	15.3994	Misure per garantire il successo dei progetti TIC dell'amministrazione federale. Eccessivo impiego di personale	Thomas Maier, Martin Bäumle	24.09.2015	CN	DFF	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20153994
Postulato	15.4045	Diritto all'utilizzo dei dati personali. Diritto alla copia	Derder Fathi	25.09.2015	CN	DFGP	https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20154045

7.2 La legge sulla sicurezza informatica della Germania

Il 25 luglio 2015 è entrata in vigore in Germania la tanto discussa «Legge per il miglioramento della sicurezza dei sistemi informatici (legge sulla sicurezza informatica)» che ha lo scopo di alzare considerevolmente il livello di sicurezza TIC contribuendo anche alla sicurezza dell'economia e dell'utenza privata[58]. La legge si rivolge soprattutto agli operatori di infrastrutture d'importanza critica nonché a quelli di siti non esclusivamente privati. Per gli operatori di infrastrutture d'importanza critica la legge prevede alcuni obblighi di messa in sicurezza dei rispettivi TIC secondo lo stato della tecnologia e di notifica degli incidenti di sicurezza TIC di una certa entità. Con la creazione della «centrale per la sicurezza della tecnologia dell'informazione di infrastrutture d'importanza critica» è stato istituito l'organo incaricato del controllo presso l'Ufficio federale della sicurezza della tecnologia dell'informazione (BSI). Le violazioni degli obblighi sanciti dalla legge (p. es. notifica non effettuata, non effettuata correttamente, non completa o non tempestiva) in futuro verranno puniti con multe pecuniarie fino a 100 000 euro.

Mentre lo scopo generale della legge sulla sicurezza informatica è stato chiaramente identificato con il significativo miglioramento della sicurezza dei sistemi di tecnologia dell'informazione della Germania e con la protezione delle infrastrutture d'importanza critica,

[58] http://dipbt.bundestag.de/extrakt/ba/WP18/643/64396.html (stato: 29 febbraio 2016).

gli obiettivi concreti del decreto molto lontano dalla prassi dal diritto penale non si distinguono in maniera immediata. Non si capisce chiaramente se l'accento dell'attuazione sia posto sulla verifica dei soggetti sottoposti al rispetto delle prescrizioni in materia di protezione delle diverse categorie di dati degni di protezione (relativi a persone) o piuttosto sul rispetto dell'obbligo di notifica di incidenti TIC (o su entrambi). In particolare, i servizi responsabili dovranno stabilire dapprima una prassi e i relativi criteri di valutazione in materia di proporzionalità e in merito all'impreciso termine giuridico di «stato della tecnologia».

La legge tedesca sulla sicurezza informatica non ha nessuna ripercussione diretta sulla Svizzera poiché si tratta di diritto vigente in tale Paese. Tuttavia sono in corso lavori in tal senso con l'elaborazione di una direttiva europea sulla sicurezza della rete e dell'informazione (Direttiva NIS, p.es. con l'introduzione di un obbligo di notifica), il che potrebbe spingere la Svizzera a riprendere ampiamente questi propositi nell'ambito del recepimento autonomo del diritto europeo in quello svizzero. Del resto, le aziende svizzere che hanno delle filiali in Germania sottoposte alla nuova legge sulla sicurezza informatica devono già confrontarsi a questa tematica. Non è escluso che indagini avviate contro filiali di aziende svizzere per presunte violazioni di questa legge possano avere ripercussioni sulle case madri in Svizzera.

7.3 Conferenza SNPC

Il 2 novembre 2015 lo «Stade de Suisse» di Berna ha ospitato la seconda conferenza sulla «Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)». Oltre 250 partecipanti provenienti dal mondo dell'economia, della politica, dell'amministrazione e della società civile sono stati informati sullo stato della SNPC e hanno ottenuto una panoramica generale delle misure adottate dalla Svizzera in questo campo. I relatori nazionali e internazionali intervenuti hanno discusso i diversi aspetti legati a tali rischi. Il GovCERT.ch ha illustrato, in particolare, il funzionamento concreto di un'analisi di eventi, mentre MELANI ha presentato il prototipo di un quadro della situazione sviluppato nell'ambito della SNPC. Un altro punto centrale analizzato nel corso dell'incontro è stato quello della lotta alla cybercriminalità. Il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet (SCOCI) ha presentato lo stato dei lavori stilando una panoramica dei casi su scala nazionale, mentre il Ministero pubblico di Zurigo ha fornito una serie di esempi tratti dall'attività quotidiana delle autorità di perseguimento penale. Grande interesse è stato suscitato anche dalla dimostrazione live di un hacker che ha illustrato la strategia che gli consente di identificare sistematicamente impianti di controllo per sistemi industriali e le relative falle.

Dalla conferenza è emerso che la protezione contro i cyber-rischi continua a costituire una grande sfida per la Svizzera, anche se è stato sottolineato che negli ultimi anni sono stati compiuti importanti passi avanti in tal senso. La chiave del successo è rappresentata da un buon coordinamento tra i numerosi soggetti coinvolti. Il rafforzamento di questa collaborazione costituirà l'obiettivo principale della SNPC anche nel corso del prossimo anno.

8 Prodotti MELANI pubblicati

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

8.1 GovCERT.ch Blog

8.1.1 TorrentLocker Ransomware targeting Swiss Internet Users

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

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

8.1.2 Ads on popular Search Engine are leading to Phishing Sites

23.11.2015 - GovCERT.ch and Reporting and Analysis Centre for Information Assurance (MELANI) are aware of an ongoing phishing campaign that is targeting a large credit card issuer in Switzerland. What makes this phishing campaign somehow unique is the way how the phishers are advertising their phishing sites: while traditionally phishing sites are being promoted through phishing emails that are usually being sent to a large audience, the phishers are using advertisements (Ads) on a popular search engine to promote their phishing sites.

➔ http://www.govcert.admin.ch/blog/16/ads-on-popular-search-engine-are-leading-to-phishing-sites

8.1.3 Update on Armada Collective extort Swiss Hosting Providers

08.11.2015 - During the recent days and weeks, various Hosting Providers in Switzerland have been blackmailed by a hacking group that calls themselves Armada Collective. As the Distributed Denial of Service (DDoS) attacks carried out by the Armada Collective have grown in terms of intensity and frequency, we have decided to publish an update to our previous blog post about Armada Collective, providing a short overview on the current situation in Switzerland and some additional information.

➔ http://www.govcert.admin.ch/blog/15/update-on-armada-collective-extort-swiss-hosting-providers

8.1.4 Armada Collective blackmails Swiss Hosting Providers

22.09.2015 - Earlier this year, we warned about DD4BC, a hacker group that tried to extort money from high value targets in Switzerland and abroad. While DD4BC is still around, MELANI / GovCERT.ch as well as the Cybercrime Coordination Unit Switzerland (CYCO) did receive several independent reports from hosting Providers in Switzerland recently that they are being blackmailed by a hacker group that calls themselves Armada Collective.

➔ http://www.govcert.admin.ch/blog/14/armada-collective-blackmails-swiss-hosting-providers

8.1.5 Swiss Advertising network compromised and distributing a Trojan

22.09.2015 - On September 11, 2015, MELANI / GovCERT.ch got informed by security researcher Kafeine about a popular advertising network in Switzerland that obviously got compromised by cybercriminals, leading to an exploit kit called Niteris.

➔ http://www.govcert.admin.ch/blog/13/swiss-advertising-network-compromised-and-distributing-a-trojan

8.1.6 Analysing a new eBanking Trojan called Fobber

11.09.2015 - Some weeks ago we read an interesting blog by Malwarebytes about Fobber, a new e-banking focussed malware in the arena that seems to be a Tinba spinoff. We decided to have a closer look at it to find out whether Swiss critical infrastructures are targeted by it. We'd like to share our findings with you, because it contains some interesting advanced techniques that at the same time are implemented in a comparably simple way; we think this makes Fobber an ideal case study.

➔ http://www.govcert.admin.ch/blog/12/analysing-a-new-ebanking-trojan-called-fobber

8.2 Bollettino d'informazione

8.2.1 TeslaCrypt: Rimangono sempre attuali i software nocivi che cifrano i vostri dati e richiedono un riscatto (ransomware)

03.12.2015 - Diverse segnalazioni riguardanti il software nocivo chiamato TeslaCrypt ricevute negli ultimi giorni dalla Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI testimoniano un aumento della diffusione di questa variante di ransomware che, una volta installato, cifra i files e intima l'utente a pagare un riscatto per poterli ripristinare.

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

8.2.2 Il pagamento di riscatti rafforza l'infrastruttura degli attacchi DDoS

19.11.2015 - Attualmente l'estorsione è uno dei metodi privilegiati dai criminali cibernetici che mirano a realizzare un rapido guadagno finanziario. Per estorcere denaro a una vittima

possono essere utilizzati diversi tipi di attacchi, tra i quali figurano anche gli attacchi DDoS («Distributed Denial of Service»), che mirano a limitare la disponibilità di siti o servizi in rete. Quest'anno MELANI ha informato a più riprese sulla realtà di simili attacchi e sulle conseguenti estorsioni operate dai gruppi Armada Collective e DD4BC, i quali hanno destato l'attenzione dei media in Svizzera. MELANI sconsiglia vivamente di cedere alle richieste degli estorsori.

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

8.2.3 Il 21o rapporto semestrale MELANI è incentrato sul tema principale della «sicurezza dei siti Web»

29.10.2015 - Il 21o rapporto semestrale MELANI è incentrato, tra l'altro, sugli attacchi di spionaggio che hanno colpito anche la Svizzera, sugli attacchi di phishing tuttora presenti e sul tema principale della «sicurezza dei siti Web». Quest'ultima tematica è una delle numerose novità del rapporto semestrale.

➔ https://www.melani.admin.ch/melani/it/home/dokumentation/bollettino-d-informazione/MELANI-21-rapporto-semestrale.html

8.2.4 Portale di segnalazione contro il phishing

29.07.2015 - Nel corso degli ultimi anni è notevolmente aumentato il numero di richieste relative al phishing che sono state elaborate dalla Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI. Nella maggioranza dei casi sono state segnalate e-mail e pagine web create a scopo di phishing che prendono di mira clienti di istituti finanziari in Svizzera, ma anche piattaforme Internet di fama internazionale (come ad es. social network, servizi e-mail o fornitori di servizi di pagamento online). Per poter elaborare in maniera più efficiente le numerose segnalazioni di phishing in entrata, la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI ha attivato un sito Internet sul quale è possibile segnalare pagine sospette di phishing.

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

8.3 Liste di controllo e guide

Nel seconda metà dell'anno 2015 MELANI non ha pubblicato né nuove liste di controllo né nuove guide.

9 Glossario

Termine	Spiegazione
Application programming interface (API)	Una application programming interface (in italiano «interfaccia di programmazione di un'applicazione», acronimo API) è una parte di programma che un sistema software mette a disposizione di altri programmi per il collegamento al sistema stesso.
Attacco DDoS	Attacco Distributed-Denial-of-Service Un attacco DoS in cui la vittima è attaccata simultaneamente da numerosi sistemi diversi.
Backdoor	Backdoor (in italiano: porta posteriore) designa una parte del software che consente agli utenti di accedere al computer eludendo le normali protezione di accesso oppure un'altra funzione altrimenti protetta di un programma per computer.
Backup	Backup (in italiano: salvaguardia dei dati) designa la copia di dati nell'intento di poterli ricopiare in caso di perdita.
Bitcoin	Sistema di pagamento decentrato disponibile a livello mondiale nonché il nome di un'unità di moneta digitale.
Bluetooth	Una tecnologia che consente la comunicazione senza fili tra due apparecchi finali e utilizzata soprattutto in ambito di telefonia mobile, di laptop, di PDA e di dispositivi di immissione (ad es. il mouse del computer).
Border Gateway Protocol (BGP)	Protocollo di routing utilizzato in Internet per connettere tra loro diversi sistemi autonomi.
Bot / Malicious Bot	Trae origine dalla parola slava per lavoro (robota). Designa un programma che esegue autonomamente una determinata azione alla ricezione di un comando. I cosiddetti malicious bot possono pilotare a distanza i computer compromessi e indurli a eseguire qualsiasi azione.
Bug bounty	Un programma bug bounty è un'iniziativa organizzata da aziende, gruppi di interesse, privati o enti governativi volta all'identificazione, risoluzione e divulgazione di errori presenti in software dietro

	corresponsione di premi in natura e/o denaro a coloro che scoprono tali vulnerabilità.
Bus	Sistema di trasmissione dei dati tra diversi utenti mediante un canale condiviso in cui la trasmissione viene eseguita attraverso uno strato di comunicazione uniformato indipendente dal mittente e dal destinatario.
Captcha	CAPTCHA è un acronimo di Completely Automated Public Turing test to tell Computers and Humans Apart. I CAPTCHA sono utilizzati per determinare se si è di fronte a un essere umano o a una macchina.
Cavalli di Troia	I cavalli di Troia (sovente chiamati troiani) sono programmi che eseguono di nascosto operazioni nocive, camuffandosi in applicazioni e documenti utili per l'utente.
CERT	Un Computer Emergency Response Team (CERT), in italiano «squadra per la risposta a emergenze informatiche», è un gruppo di esperti di sicurezza che interviene nella risoluzione di incidenti relativi alla sicurezza IT offrendo indicazioni e suggerimenti pratici.
Certificate	Un certificato digitale è in un certo qual senso l'equivalente di una carta d'identità a livello di cyberspazio ed è destinato all'assegnazione di una determinata chiave pubblica a una persona o a un'organizzazione. Tale assegnazione è autenticata dal servizio di certificazione che provvede a tale scopo apponendovi la propria firma digitale.
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.
Command & Control Server	La maggior parte dei bot possono essere sorvegliati da un botmaster e ricevere comandi attraverso un canale di comunicazione. Tale canale di comunicazione è denominato Command and Control Server.
Content Management Systems	Un «Content Management System» (acronimo CMS, in italiano «sistema di gestione dei contenuti») è un

(CMS)	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).
Crimeware kit	Modulo che consente anche a utenti inesperti di creare un malware in tutta semplicità.
Crittografia end-to-end	Metodo che consente la codifica/decodifica dei dati trasmessi solo al mittente e al destinatario.
Defacement	Deturpamento di pagine Web.
Dorsale	Rete di telecomunicazione ad alta velocità di trasmissione. La dorsale Internet costituisce il «cuore» di Internet.
Doxing	Pratica basata su Internet che consiste nella raccolta e successiva pubblicazione di dati personali, generalmente con intenti malevoli nei confronti delle vittime.
Exploit-Kit	kit che consente a criminali di generare programmi, script o righe di codice mediante i quali è possibile sfruttare le vulnerabilità dei sistemi di computer.
Firmware	Dati di comando per il controllo di un apparecchio (ad es. scanner, carte grafiche ecc.), memorizzati in un chip. Questi dati possono di norma essere modificati per il tramite di Upgrades (aggiornamenti).
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.
Honeypot	In ambito di sicurezza dei computer si designa come hone-ypot (italiano: vaso di miele) un programma informatico o un server che simula i servizi di rete di un computer, un'intera re-te di computer oppure il comportamento di un utente. Gli honeypot sono utilizzati per ottenere informazioni sui modelli di attacco e sui comportamenti degli aggressori.
Infezione da «drive-by-	Infezione del computer mediante malware

download»	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.
IP-Adresse	Indirizzo che identifica il computer in Internet (o su una rete TCP/IP; esempio: 172.16.54.87).
Jailbreak	Con il termine jailbreaking (dall'inglese evasione dalla prigione) si intende il superamento delle limitazioni di uso dei prodotti Apple per il tramite di un apposito software.
JavaScript	Un linguaggio di script orientato sugli oggetti per lo sviluppo di applicazioni. Gli JavaScripts sono elementi di programma integrati nel codice HTML, che consentono determinate funzioni nel navigatore di Internet. Ne può essere un esempio il controllo dei dati immessi dall'utente in un modulo Web. È così possibile verificare se tutti i caratteri immessi alla richiesta di un numero telefonico corrispondono effettivamente a delle cifre. Come gli ActiveX Controls, gli JavaScripts sono eseguiti sul computer del visitatore di pagine Internet. Oltre a funzioni utili, è però anche possibile programmare funzioni nocive. Diversamente dagli ActiveX Controls, gli JavaScripts sono supportati da tutti i navigatori.
KillDisk	Formattazione a basso livello per la cancellazione sicura e definitiva di dati da un disco rigido.
Librerie	Nell'ambito della programmazione, una libreria software indica una raccolta di sottoprogrammi/subroutine che offrono soluzioni a problemi tematicamente collegati tra loro.
Macro	Nello sviluppo software una macro è costituita da una sequenza di istruzioni o dichiarazioni che vengono raggruppate in modo da poter essere eseguite con un semplice richiamo.
Malware	Termine generico per software che esegue funzioni nocive su un computer. Rientrano tra l'altro in questo gruppo i virus, vermi informatici, cavalli di Toia, nonché le Logic Bombs.
Man-in-the Middle	Attacco Man-in-the-Middle Attacco nel corso del quale l'aggressore si insinua inosservato su un canale di comunicazione tra due partner, in modo da essere in

	grado di seguire o di modificare lo scambio di dati.
Mobile Payment	Termine utilizzato per designare processi di pagamento in cui almeno il debitore si avvale di tecnologie elettroniche mobili per avviare, autorizzare o effettuare le transazioni.
NFC (Near Field Communication)	La Near Field Communication è uno standard di trasmissione secondo gli standard internazionali per lo scambio senza contatto di dati su corte distanze.
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.
Programmable Logic Controller (PLC)	Designazione inglese dei controllori logici programmabili (CLP).
QR Code (o codice QR)	Metodo per annotare informazioni in modo che possano essere reperite e scansionate meccanicamente in modo particolarmente rapido.
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
Remote Administration Tool	Il software di manutenzione a distanza (in inglese: Remote Administration Tool) costituisce un'applicazione nell'ambito del concetto di manutenzione a distanza di qualsiasi computer o sistema di computer.
Routers	Apparecchiature del settore delle reti di computer, della telecomunicazione o anche di Internet che collegano o separano più reti di computer. I router sono ad esempio utilizzati nelle reti domestiche per effettuare il collegamento tra la rete interna e Internet.
Servizi booter o stresser	Servizio che consente anche a utenti tecnicamente non esperti di eseguire attacchi DDoS.

Sistema crittografico	Un sistema crittografico è un sistema utilizzato per la cifratura. Crittografia significa originariamente scienza di cifratura di informazioni.
Sistema ERP	L'enterprise resource planning (letteralmente «pianificazione delle risorse d'impresa», abbreviato in ERP) identifica l'attività aziendale di pianificazione e gestione tempestiva e commisurata alle esigenze di risorse come capitale, personale, mezzi d'esercizio, materiali, tecnologia dell'informazione e della comunicazione, sistemi TIC conformemente all'oggetto sociale.
Sistemi autonomi	Un sistema autonomo è un insieme di reti IP che vengono amministrate come unità e che sono collegate attraverso un protocollo di routing interno comune.
Sistemi industriali di controllo (ICS)	I sistemi di controllo e di comando constano di una o più apparecchiature che guidano, regolano e/o sorvegliano il comportamento di altre apparecchiature o sistemi. Nella produzione industriale il concetto di «sistemi industriali di controllo» (inglese: Industrial Control Systems, ICS) è corrente.
Sistemi SCADA	Supervisory Control And Data Acquisition Sistemi utilizzati per la sorveglianza e il comando di processi tecnici (ad es. approvvigionamento energetico e idrico).
SmartMeter	Uno SmartMeter (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.
Smartphone	Lo smartphone è un telefono mobile che mette a disposizione una maggiore funzionalità di computer di quella di un telefono mobile progredito usuale.
SMS	Short Message Service Servizio per l'invio di messaggi brevi (160 caratteri al massimo) agli utenti di telefonia mobile.
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. 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.
Spearphishing	Attacco mirato di phishing. Si fa ad esempio credere alla vittima di comunicare tramite e-mail con una persona di fiducia.
Spoofing	Nel tecnica informatica si designano come spoofing di-versi tentativi di inganni sulle reti di computer per camuf-fare la propria identità.
SQL-Injection	SQL-Injection (introduzione clandestina SQL) designa lo sfruttamento di una lacuna di sicurezza nel contesto di una banca dati SQL, ossia di una lacuna che insorge a causa della mancata verifica delle variabili da trasmettere. L'aggressore tenta di intro-durre clandestinamente i suoi propri comandi di banca dati per modificare i dati nel proprio senso o per assumere il controllo del server.
Streaming	Streaming media descrive la trasmissione simultanea dei dati video e audio attraverso una rete.
Switch	Commutatore usato per connettere segmenti di rete.
Top Level Domain	Ogni nome di dominio in Internet consta di una successione di serie di caratteri separate da un punto. La designazione Level-Domain si riferisce all'ultimo nome di questa successio-ne e costituisce il livello più elevato della risoluzione del no-me. Se ad esempio il nome completo di dominio di un compu-ter, rispettivamente di un sito Web, è de.example.com, l'elemento a destra (com) rappresenta il Top-Level-Domain di questo nome.
TOR	Sistema di anonimizzazione del traffico Web.
Ufficio abuse	Ufficio a cui possono essere inviati reclami (p. es. per utilizzo improprio di un sito Web).
USB Memory Stick	Piccoli dispositivi di memoria che possono esser raccordati al computer per il tramite di un'interfaccia USB.
VoIP	Voice over IP Telefonia tramite il protocollo Internet (IP). I protocolli utilizzati con maggiore frequenza sono: H.323 e SIP.
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).
Watering Hole Attack	Attaque du trou d'eau, attaque ciblée par un maliciel n'infectant que des sites supposés être visités par un groupe spécifique d'utilisateurs.
Zero-Day Exploits	Vulnerabilità non conosciuta pubblicamente.