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**
https://www.melani.admin.ch/

# SICUREZZA DELLE INFORMAZIONI

## LA SITUAZIONE IN SVIZZERA E A LIVELLO INTERNAZIONALE

Rapporto semestrale 2019/2 (luglio–dicembre)


30 APRILE 2020
CENTRALE D'ANNUNCIO E D'ANALISI PER LA SICUREZZA DELL'INFORMAZIONE MELANI
https://www.melani.admin.ch/

# 1 Indice

# 2 Editoriale

**Delegato federale alla cibersicurezza**

Florian Schütz è Delegato federale alla cibersicurezza e direttore del Centro nazionale per la cibersicurezza.

MELANI diventa «Centro nazionale per la cibersicurezza». Così titolava un contributo sulla homepage di MELANI all'inizio del 2020. Si tratta di un ulteriore passo avanti verso la definizione delle competenze a livello federale, come stabilito dal Consiglio federale il 30 gennaio 2019 (cfr. fig. 1). L'organizzazione del Centro nazionale per la cibersicurezza è parte integrante dei lavori in corso e non è ancora stata approvata in via definitiva. Una cosa però è già chiara: MELANI è una componente chiave del nuovo centro e in futuro sarà ulteriormente rafforzata e ampliata. Ecco perché in questo editoriale desidero ripercorrere le esperienze che ho maturato con MELANI nel secondo semestre 2019 e discutere di tre sfide future.

Fin dalla fondazione di MELANI, il 1° ottobre 2004, le tecnologie dell'informazione e della comunicazione (TIC) hanno pervaso in modo crescente l'economia, la ricerca e la società. Le TIC sono il fulcro dei processi digitalizzati e permeano il nostro quotidiano. Oggi un'analisi generale della situazione non è più adeguata di fronte alla diversificazione delle minacce, che richiede approfondimenti specifici per settori economici, ambiti della politica, ricerca e società. Nel quadro di un progetto pilota, attualmente è al vaglio una prima misura che prevede una rappresentazione della situazione specifica per il settore finanziario.

La seconda sfida è data dal forte aumento dei casi. Se durante il primo anno di attività di MELANI, nel 2005, sono state registrate complessivamente meno di 500 segnalazioni, nel solo mese di gennaio di quest'anno ne sono pervenute più di 500. Per far fronte a un tale volume, come prima misura nel secondo semestre del 2019 è stato istituito il Servizio nazionale di contatto per la cibersicurezza, che riceve e analizza le segnalazioni assicurandone il trattamento da parte dei servizi competenti.

Un altro compito importante consisterà nell'automatizzazione dell'analisi, nel trattamento e nell'integrazione dei servizi interessati – ad esempio delle autorità di perseguimento penale.

«Sei stato pesato, sei stato misurato e sei stato trovato mancante» recita la citazione tratta del film «Il destino di un cavaliere». Benché MELANI goda di un'eccellente reputazione sul piano internazionale, nelle discussioni pubbliche, di tanto in tanto, capita di sentire che MELANI non è ritenuta abbastanza valida. Posto che il potenziale di miglioramento è indubbio, il buon lavoro svolto dal team non merita questa critica generica. Crediamo che sia data dal fatto che l'assenza di indicatori chiave di prestazione («key performance indicator», KPI) rende difficile formulare considerazioni articolate e pertanto può capitare di giungere a conclusioni errate in alcune situazioni. Definiremo quindi dei KPI per consentire critiche più puntuali e misurare meglio i risultati raggiunti.

Una di queste critiche l'abbiamo già presa sul serio: secondo alcuni il rapporto semestrale MELANI non era abbastanza tecnico. Per continuare a comunicare con il gruppo target formato da politici, dirigenti e privati interessati, senza rinunciare a offrire qualcosa agli esperti,

per la prima volta abbiamo realizzato un allegato tecnico. Saremo molto lieti di ricevere eventuali suggerimenti al riguardo. Vi invitiamo a scriverci comunicandoci se vorreste che in futuro fosse ampliato o meno.[1]

Dalla sua creazione nel 2005, MELANI ha ottenuto e dato molto, come mostra anche il presente rapporto semestrale. Nei prossimi anni le sfide legate alla sicurezza sono destinate ad aumentare ancora. Ritengo tuttavia che sapremo venirne a capo e che, grazie alla nuova organizzazione del Centro nazionale per la cibersicurezza, getteremo solide basi per il futuro.

Florian Schütz

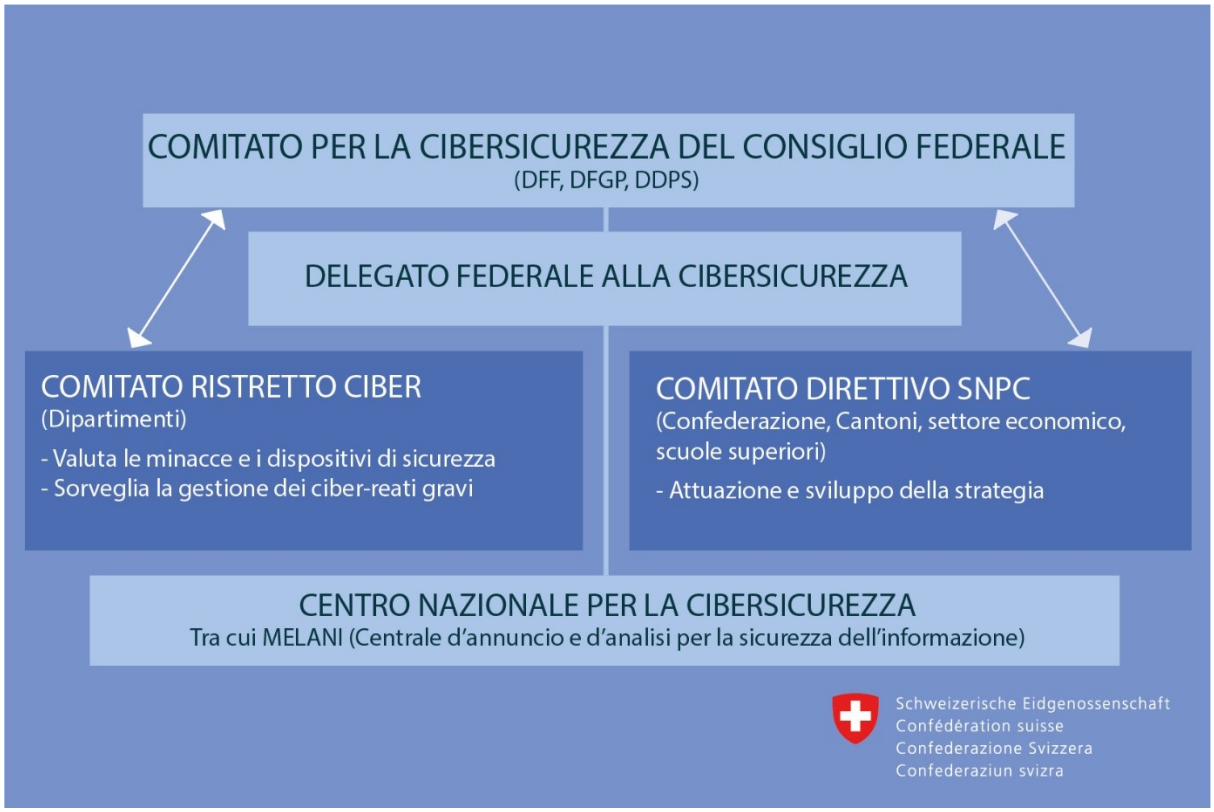

*Figura 1: Organizzazione della cibersicurezza in seno alla Confederazione*

[1] Vi invitiamo a compilare la valutazione del rapporto sulla nostra pagina web: https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti/evaluation-halbjahresbericht.html

# 3 Tema principale: i dati personali in rete

## 3.1 Introduzione

Oggigiorno la stragrande maggioranza delle operazioni di trattamento dei dati avviene in modalità elettronica e su dispositivi collegati più o meno direttamente a Internet. Di solito i dati sono archiviati sul cloud preferito, dal quale possono essere consultati.

I «nostri dati», o più precisamente i «dati che ci riguardano», sono archiviati dai soggetti più disparati in una molteplicità di luoghi e quasi nessuno sa di preciso chi abbia accesso a quali dati e dove questi vengano elaborati.

I dati vengono raccolti, scambiati, aggregati e spesso anche rubati – laddove «rubare» è fuorviante, visto che i dati vengono semplicemente copiati e non sottratti al proprietario. Lo stesso vale in caso di «vendita» dei dati. Di frequente i dati vengono «venduti», riprodotti e venduti di nuovo. Questo ne complica notevolmente la tracciabilità: quale strada intraprende un record di dati prima di ricomparire da qualche parte?

L'autodeterminazione circa i propri dati è quasi impossibile e perseguire le violazioni in materia di protezione dei dati è una grande sfida per le persone coinvolte e i servizi preposti.

Quasi ogni giorno le fughe di dati o il libero accesso ai dati dovuto a errori di configurazione conquistano le prime pagine.[2] Nel frattempo i casi più clamorosi parlano di oltre un miliardo di dati interessati.[3] MELANI aveva scelto la fuga di dati[4] come argomento principale nel suo rapporto semestrale 2017/2.

## 3.2 I dati della realtà online

Viviamo nell'era delle informazioni interconnesse. Immaginare la nostra quotidianità senza Internet non è più possibile. Attraverso la rete di comunicazione globale ordiniamo merci, acquistiamo servizi e ci procuriamo informazioni, scambiamo opinioni, immagini e molto altro ancora. Di conseguenza ci ritroviamo con numerosi account online presso innumerevoli operatori, che creiamo rapidamente e che a volte dimentichiamo altrettanto in fretta. In genere in ognuno di questi account sono registrati un indirizzo e-mail e una password. Per alcuni servizi è necessario fornire anche nome e cognome, indirizzo, data di nascita, numero di telefono, foto o dati della carta di credito. Probabilmente i gestori dei servizi dispongono di informazioni che abbiamo cercato o caricato in rete utilizzando l'account. In particolare attraverso gli account dei social media riveliamo molto: chi sono i nostri amici, con chi comunichiamo, chi seguiamo, cosa ci piace o condividiamo e quanto tempo dedichiamo a quali temi. Con queste informazioni si possono elaborare profili di personalità molto dettagliati.

---

2 https://www.helpnetsecurity.com/2019/11/14/breaches-2019/; https://www.immuniweb.com/blog/stolen-credentials-dark-web-fortune-500.html

3 https://securityaffairs.co/wordpress/94275/breaking-news/elasticsearch-social-information-1-2b-people.html; https://www.wired.com/story/billion-records-exposed-online/

4 Rapporto semestrale MELANI 2017/2, n. 3.

Anche semplicemente navigando in rete lasciamo tracce digitali sotto forma di dati che vengono archiviati nei server dei fornitori di servizi, delle reti pubblicitarie e di altri fornitori di contenuti – o nei nostri dispositivi, ad esempio sotto forma di *cookie*. Anche alcune estensioni del browser («add-on» o «plug-in») raccolgono dati per poi archiviarli o inoltrarli[5], senza necessariamente associarli al nome di una persona, ma a uno pseudonimo. Ciò consente di creare un profilo della persona e, tra le altre cose, di proporre messaggi pubblicitari personalizzati oppure di offrire ulteriori contenuti che suscitano il nostro interesse. Se questi dati vengono collegati a un identificatore personale (ad es. indirizzo e-mail o account di social media) possono, anche una volta estratti dal contesto di rilevazione, venir elaborati e utilizzati mantenendo il riferimento alla persona.

## 3.3 Dati dal mondo analogico

Sin dall'esordio dell'elaborazione elettronica dei dati (EED), quelli provenienti dal mondo analogico vengono archiviati in modalità digitale – inizialmente ancora nei singoli computer o nelle sole reti aziendali interne e oggi in dispositivi collegati, più o meno, direttamente a Internet. Corrispondenza, pianificazioni, schedari dei clienti, contabilità e amministrazione dei collaboratori sono in gran parte digitalizzati. È ormai abitudine, ad esempio, tenere la propria rubrica privata solo nel computer, sullo smartphone o sul cloud.

Sull'onda della digitalizzazione vengono elaborati in modalità elettronica i dati provenienti da un numero crescente di settori: nell'ambito del sistema sanitario con la cartella informatizzata del paziente o con le app di fitness, a livello di mobilità con i biglietti online per i trasporti pubblici o per il noleggio di biciclette tramite app, nei dispositivi smarthome studiati per esigenze abitative, nel servizio di consegna dei generi alimentari e di altre ordinazioni, tanto per citarne alcuni.

Anche le banche dati delle autorità sono passate da tempo alla tecnologia elettronica e oggi sono interconnesse per potenziare le prestazioni del Governo elettronico. Nel caso in cui dei soggetti non autorizzati accedessero ai sistemi delle autorità, gli effetti potrebbero riguardare una larga fetta della popolazione, se non tutta.[6]

## 3.4 Il caso speciale dei registri e delle banche dati pubblici

Anche per quanto riguarda i tradizionali registri pubblici che, grazie alla digitalizzazione, sono diventati accessibili online, è necessario tenere conto di alcuni aspetti legati ad Internet. Quello che prima veniva spedito unicamente in formato cartaceo o che si poteva esaminare in un ufficio, ora può essere consultato da qualsiasi parte del mondo e quindi archiviato localmente.

---

5 https://www.washingtonpost.com/technology/2019/07/18/i-found-your-data-its-sale/

6 Ecuador https://www.zdnet.com/article/database-leaks-data-on-most-of-ecuadors-citizens-including-6-7-million-children/;
Cile https://www.zdnet.com/article/voter-records-for-80-of-chiles-population-left-exposed-online/;
Bulgaria https://www.inside-it.ch/articles/55013

Eppure le relative ordinanze stabiliscono che i sistemi devono essere «protetti dalle interrogazioni in serie»[7] o che determinate registrazioni devono essere messe «a disposizione gratuitamente su Internet»[8]. Tuttavia, implementazione tecnica a parte, con un po' di pazienza e di lavoro di programmazione è possibile estrarre un intero registro. Da ciò nasce inevitabilmente un campo di tensione tra il carattere pubblico dei dati (anche elettronici) previsto dalla legge e la protezione di tali dati dal trattamento abusivo. Le basi legali non chiariscono se la consultazione debba poter avvenire in forma anonima. Al fine di impedire in modo efficace le consultazioni di massa abusive, o almeno scoprirle, le persone che effettuano la consultazione dovrebbero essere identificate e le loro ricerche dovrebbero essere registrate in un modulo per un certo periodo di tempo, il che a sua volta necessita di una base legale.

Gli elenchi telefonici sono stati digitalizzati già alla fine degli anni Ottanta e messi in vendita a suo tempo ancora su CD. Di lì a poco quei dati sono diventati accessibili anche in Internet, visto che erano già disponibili pubblicamente e che pertanto ciò era consentito. Anche se gli elenchi telefonici non contengono numeri di cellulare o indirizzi e-mail, le informazioni ivi contenute possono servire a costituire una base, soprattutto per quegli attori che non si curano della legalità del trattamento dei dati.

Un esempio particolare è quello delle informazioni, una volta accessibili pubblicamente, nell'elenco dei domini «Whois», dove tra l'altro sono pubblicati i titolari dei nomi di dominio. Oggi questi dati non si possono più consultare indiscriminatamente. In origine Whois era stato concepito per far sì che proprietari e gestori dei siti web fossero noti e potessero essere contattati facilmente. Ai tempi dell'Internet caratterizzato da valori idealistici la trasparenza era un'ovvietà. L'utilizzo abusivo dei dati pubblicati, sopravvenuto nel corso tempo, ha però prontamente innescato discussioni circa la forma, le finalità e la necessità di tale registro. Infine, sotto la spinta del Regolamento generale dell'Unione europea sulla protezione dei dati (RGPD), si è deciso di intervenire e ora i dati sui nomi di dominio sono solitamente anonimizzati.[9] Con la revisione imminente della legge sulle telecomunicazioni, anche l'accesso alle informazioni sui nomi di dominio svizzeri contenute in Whois dovrebbe essere limitato.

## 3.5 Legislazione in materia di protezione dei dati

Il trattamento dei dati e il commercio di dati personali sono consentiti dall'ordinamento giuridico applicabile a seconda delle circostanze. Le prescrizioni in materia di protezione dei dati sono però molto diverse da un Paese all'altro. Con il suo Regolamento generale sulla protezione dei dati (RGPD) l'Unione europea (UE) disciplina la protezione dei dati dei propri cittadini in maniera uniforme a livello globale. Anche se molte questioni circa l'attuazione sul piano internazionale di tali prescrizioni restano tuttora aperte, il RGPD ha già sortito alcuni effetti. Dall'entrata in vigore nel maggio 2018, numerosi attori prendono molto più seriamente la protezione e la sicurezza dei dati.

---

7 Ordinanza del 23 settembre 2011 sul registro fondiario (ORF, RS **211.432.1**), articolo 27: https://www.admin.ch/opc/it/classified-compilation/20111142/index.html#a27

8 Ordinanza del 17 ottobre 2007 sul registro di commercio (ORC, RS **221.411.1**), articolo 12: https://www.admin.ch/opc/it/classified-compilation/20072056/index.html#a12

9 https://www.icann.org/resources/pages/gtld-registration-data-specs-en

Secondo numerose previsioni, nel prossimo futuro le fughe di dati provocheranno danni enormi e gli investimenti nella sicurezza dei dati aumenteranno.[10] Questo anche perché, dall'entrata in vigore del RGPD, alle aziende che violano le prescrizioni in materia di protezione dei dati vengono comminate sanzioni severe. Nel calcolo dei danni si considera in particolare il rischio di multe alle imprese, che possono ammontare fino a 20 milioni di euro o al 4 per cento della cifra d'affari annua (se superiore).

Nella revisione della legge federale sulla protezione dei dati sono previste disposizioni penali, secondo le quali non si dovranno sanzionare le imprese bensì le «persone private», ossia i dipendenti delle imprese. Qualora accertare la persona punibile richieda mezzi sproporzionati, allora sarà possibile condannare al rispettivo pagamento l'impresa, solo se la multa prevista è inferiore a 50 000 CHF. Si vedrà fino a che punto ciò possa essere fonte di tensioni all'interno delle imprese, quando la direzione aziendale prenderà (o meno) decisioni ed emanerà (o meno) istruzioni, le cui conseguenze ricadranno sull'incaricato della protezione dei dati o su semplici collaboratori.

## 3.6 Rischi ed effetti collaterali

Raramente si parla dei danni indiretti delle violazioni in materia di protezione dei dati che potrebbero subire le persone. Tali danni sono per giunta difficili da quantificare. Dati come nome e cognome, indirizzo, data di nascita, numero di telefono, indirizzo e-mail ecc. non sono di per sé dati personali «degni di particolare protezione», ma se finiscono nelle mani sbagliate sono sufficienti per creare problemi (un incremento della quantità di spam sarebbe il minore dei mali). I dati trafugati vengono utilizzati dai criminali per attacchi mirati di *social engineering*, installare software nocivi, procurarsi altri dati (sensibili), ordinare pagamenti ingiustificati o perseguire altri scopi con effetti negativi sulle persone colpite.[11] L'abuso di dati personali può anche tradursi in usurpazione d'identità – qualcuno potrebbe spacciarsi per una determinata persona utilizzando i dati di quest'ultima. Con tale identità estranea si possono ad esempio creare account nei social media, registrare nomi di dominio o effettuare acquisti. Si verificano inoltre regolarmente casi di truffa ai danni dei contatti di persone il cui account di posta elettronica è stato compromesso o i cui dati sono stati altrimenti trafugati.

Le conseguenze delle pratiche non autorizzate di raccolta e trattamento dei dati sono difficili da stimare. Nell'era dei big data e dell'apprendimento automatico, l'unione automatizzata delle fonti più disparate di dati diventa sempre più semplice. Che questo avvenga per finalità legittime da parte di imprese in una zona grigia della sfera giuridica o che sia messo in atto da soggetti criminali è poco rilevante. Bisogna partire dal presupposto che ogni singola banca dati, prima o poi, verrà hackerata e che i dati sottratti prenderanno la strada del mercato nero.

---

10 https://securityintelligence.com/articles/11-stats-on-ciso-spending-to-inform-your-2020-cybersecurity-budget/; https://www.business2community.com/cybersecurity/10-cybersecurity-trends-in-2020-you-need-to-keep-an-eye-on-02275883; https://www.forbes.com/sites/gilpress/2019/12/03/141-cybersecurity-predictions-for-2020/; https://www.forbes.com/sites/gilpress/2019/12/12/42-more-cybersecurity-predictions-for-2020/

11 Cfr. https://www.microsoft.com/security/blog/2019/12/02/spear-phishing-campaigns-sharper-than-you-think/ e rapporti semestrali MELANI (capitoli dedicati all'ingegneria sociale).

## 3.7 Conclusione

I «nostri dati», o meglio i «dati che ci riguardano», sono archiviati da molti operatori in molti luoghi. Il rilevamento, la raccolta e l'unione di dati è un modello di business sia in ambiti legali che illegali e comporta il commercio di tali dati. È dunque necessario fare i conti con il fatto che industriali, artigiani e commercianti o inserzionisti e soggetti criminali dispongono di schedari di dati su di noi, più o meno completi, e che li possono utilizzare per colpirci individualmente. Se poi, partendo dai dati, vengono elaborati dei profili di personalità, si apre la via a eventuali influenze specifiche di tipo psicologico, non solo inerenti i consumi e l'esposizione ai raggiri, ma anche circa il formarsi dell'opinione e quindi, alla fin fine, pure a livello di comportamento elettorale.

Già oggi la pubblicità in Internet è spesso personalizzata. La tendenza proseguirà ed è destinata a essere sfruttata sempre più anche dal mondo politico per campagne elettorali mirate.

I criminali perfezioneranno ulteriormente i propri metodi di attacco, modulandoli su misura delle potenziali vittime. Da un po' ormai l'appellativo personalizzato in un'e-mail non è più un criterio adatto a stabilirne l'autenticità: già da tempo i criminali compilano le proprie e-mail con nome, indirizzo, numero di telefono e altri dati personali del destinatario. Anche indirizzi del mittente falsificati vengono utilizzati regolarmente in modo tale che sembrino provenire da un conoscente – posto che l'invio dell'e-mail o del messaggio di un social network non avvenga addirittura dall'account reale ma compromesso, del presunto mittente.

Valutazione / Raccomandazione

Benché Internet offra numerosi vantaggi e abbia enormemente semplificato l'accesso a informazioni preziose, non bisogna credere a tutto quello circola in rete o a ciò che arriva per e-mail. Navigare e comunicare in rete sono attività che richiedono prudenza e una sana dose di scetticismo. In caso di dubbi è meglio non rinunciare a confrontarsi con conoscenti su temi, fatti e notizie particolari. Prima di cliccare su un link o di aprire un documento che vi è stato inviato tramite e-mail chiedete conferma al presunto mittente.

Chi elabora e archivia i dati personali deve preoccuparsi di proteggerli adeguatamente da accessi non autorizzati. I registri pubblici devono accettare le consultazioni di carattere generale, ma impedire quelle di massa. Anche per quanto riguarda altre raccolte di dati alle quali è possibile accedere in maniera limitata (ad es. con procedure di test o demo) è necessario accertarsi che tali restrizioni non possano essere aggirate. Gli attori specializzati nella raccolta dei dati tentano di aggirare le restrizioni tecniche, ad esempio tramite la generazione automatica di numerosi account di prova o altre pratiche di simulazione di una molteplicità di utenti.

# 4 Situazione della minaccia

Il formulario d'annuncio online di MELANI[12] permette di comunicarci casi e porci domande. Le segnalazioni ci aiutano a individuare i trend inerenti i pericoli di Internet, a darne comunicazione e a raccomandare eventuali contromisure o ad adottarle direttamente. Il grafico di seguito sulla tipologia e sul numero di segnalazioni pervenute nel secondo semestre 2019 mostra con cosa è stata alle prese la popolazione svizzera in tale periodo.

In Internet si mente e si inganna molto, come emerge dalle segnalazioni relative a phishing, truffe e «*fake sextortion*». Tali fenomeni rappresentano casi che in linea di massima si possono riconoscere in modo abbastanza semplice e che quindi spesso si traducono in segnalazioni che, a loro volta, lasciano per lo più presupporre che gli utenti interessati abbiano subodorato la macchinazione e non ne siano rimasti vittima. Non siamo in grado di fare affermazioni fondate sul tasso di successo di tali attacchi. Per quanto riguarda le segnalazioni di malware, bisogna invece supporre che esse abbiano, almeno in alcuni casi, provocato dei danni di una certa entità. Altri eventi di malware avvengono indisturbati in background e per questo non risultano né individuati né segnalati dagli interessati (cfr. «Drive-by»: la situazione in Svizzera, n. 4.3.2).

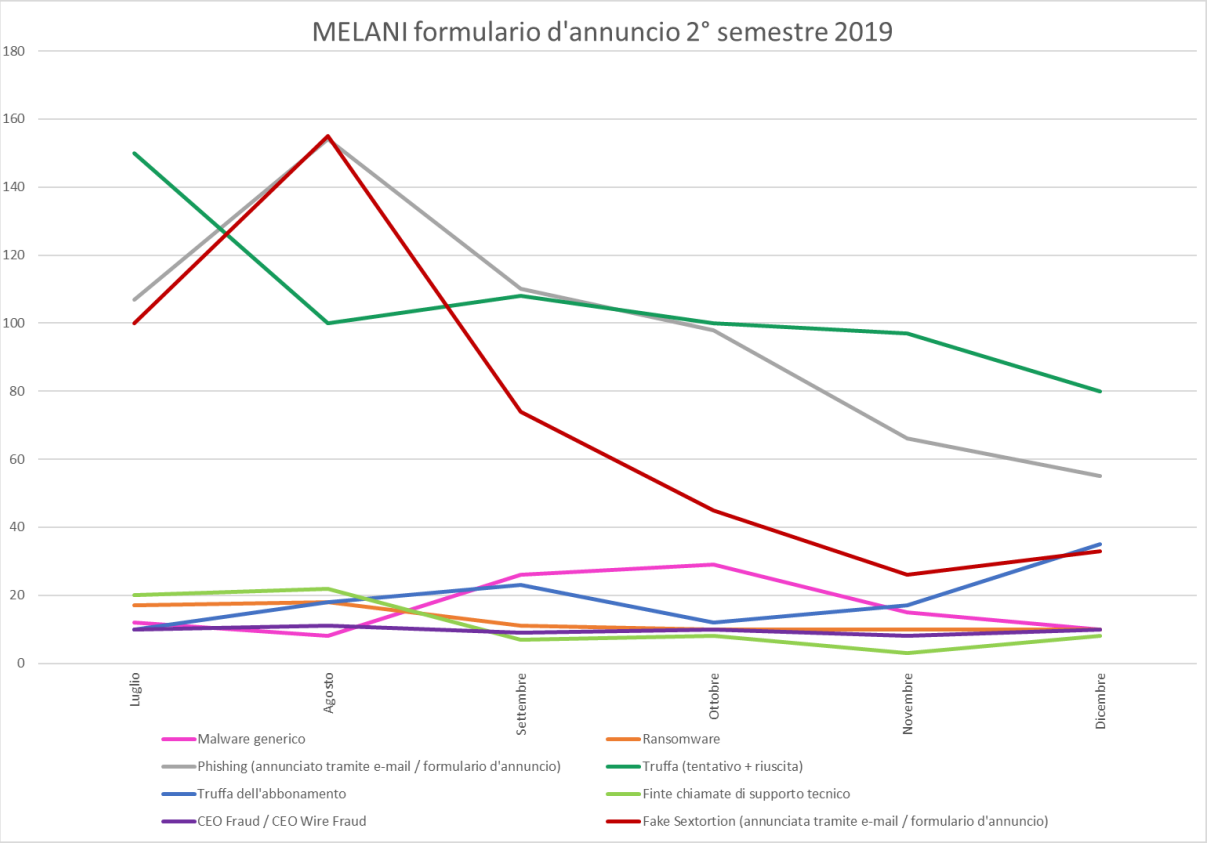


*Figura 2: Annunci effettuati tramite il formulario online. Sono escluse le segnalazioni giunte da altri canali.*

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

## 4.1 Spionaggio

Anche nel secondo semestre 2019 uno degli strumenti preferiti dagli Stati per raccogliere informazioni è stato lo spionaggio informatico, usato pure per il furto di proprietà intellettuale . Il «Threat Analysis Group» (TAG) di Google, che si adopera per individuare e contrastare attacchi informatici contro i propri utenti, dichiara ad esempio di aver notificato 12'000 tentativi di *spear-phishing* in 149 Stati nel solo terzo trimestre del 2019 (luglio-settembre).[13] Responsabili sarebbero oltre 270 gruppi legati a entità governative e operanti in almeno 50 Paesi. Nel computo rientrerebbero anche, oltre al classico spionaggio campagne di disinformazione volte a promuovere gli interessi di uno Stato o a screditare un movimento politico. Al pari di dissidenti ed attivisti, anche i politici fanno parte di un gruppo ad alto potenziale di rischio: È quanto attestano le diverse centinaia di tentativi d'attacco contro organizzazioni politiche registrati da «AccountGuard», piattaforma di Microsoft concepita allo scopo di mettere in guardia i candidati e gli uffici che lavorano a una campagna elettorale che sono diventati bersaglio di ciberattacchi. I tentativi di compromissione informatica mirati e sponsorizzati da uno Stato avrebbero però come obiettivo soprattutto le grandi aziende. In cifre dovremmo parlare di oltre tre quarti dei 10 000 utenti notificati da Microsoft nel 2019.[14] Il colosso dell'informatica ha poi stilato un elenco dei cinque gruppi di attacco più attivi del 2019, i cosiddetti «Advanced Persistent Threat» (APT). Stando a Microsoft e ad altre aziende attive nella sicurezza[15], «Holmium» alias «APT33» tra quelli elencati dovrebbe essere sponsorizzato dal governo iraniano. Il suo obiettivo consiste nel prendere di mira soprattutto le organizzazioni che operano nel campo dell'aviazione civile e militare nonché dell'energia ottenuta da fonti petrolchimiche. La campagna ha acquisito notorietà per aver infiltrato tra il 2016 e il 2017 un'organizzazione americana ed una saudita operanti nel settore dell'aviazione[16]. Secondo Microsoft, un altro gruppo particolarmente attivo è «Fancy Bear» alias «APT28» o «Sofacy». Secondo comunicazioni ufficiali di diversi Paesi (tra cui il Regno Unito e gli Stati Uniti) e rapporti di aziende attive nell'ambito della sicurezza (come CrowdStrike), il gruppo sarebbe collegato al servizio segreto militare russo (GRU) e inoltre sarebbe stato messo in relazione con gli attacchi al Bundestag tedesco (2015), al Comitato nazionale democratico statunitense («Democratic National Committee») (2016) e all'Agenzia mondiale antidoping (2016).

### 4.1.1 Ciberattacchi contro organizzazioni sportive e antidoping

Già da qualche anno le organizzazioni sportive e antidoping sono bersaglio di campagne di spionaggio informatico. Come illustrato nel rapporto semestrale MELANI 2018/1 (cap. 4.1.1), l'infrastruttura TIC dei Giochi olimpici invernali di Pyeongchang (Corea del Sud) era stata attaccata quello stesso anno dal worm «Olympic Destroyer», che secondo il fornitore di servizi di sicurezza Kaspersky Lab avrebbe avuto delle analogie con Sofacy. Sembra che anche il

---

13 https://blog.google/technology/safety-security/threat-analysis-group/protecting-users-government-backed-hacking-and-disinformation/

14 https://blogs.microsoft.com/on-the-issues/2019/07/17/new-cyberthreats-require-new-ways-to-protect-democracy/; https://arstechnica.com/tech-policy/2019/07/microsoft-warns-10000-customers-theyre-targeted-by-nation-sponsored-hackers/

15 https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

16 Cfr. Rapporto semestrale MELANI 2017/2, n. 5.1.2.

gruppo Fancy Bears  fosse legato a questa campagna: all'inizio dello stesso anno aveva pubblicato dei dati che risultavano essere stati sottratti al Comitato olimpico internazionale e al Comitato olimpico nazionale statunitense tra la fine del 2016 e l'inizio del 2017. Tra questi figuravano e-mail e cartelle cliniche di atleti.

Il 28 ottobre 2019 il «Threat Intelligence Center» di Microsoft annunciava di aver identificato numerosi attacchi, probabilmente messi a segno da Sofacy, contro almeno 16 autorità antidoping e organizzazioni sportive in tre continenti. È possibile che gli attacchi fossero iniziati a metà settembre, poco prima della pubblicazione della decisione dell'Agenzia mondiale antidoping (WADA) di escludere la Russia dai Giochi Olimpici di Tokio 2020.[17]

Questa campagna non è sicuramente l'unica collegata alle Olimpiadi estive che dovrebbero svolgersi in Giappone nel 2021, dopo esser state posticipate di un anno a cause della crisi del coronavirus. Gli organizzatori hanno messo in guardia contro campagne di e-mail che si servono del nome del comitato organizzativo dei Giochi olimpici e paraolimpici per indirizzare i destinatari su pagine di *phishing* o infettarne i dispositivi. Una campagna di phishing, in particolare, aveva come obiettivo 170 0000 singoli individui in Giappone e negli Stati Uniti. Alcuni dettagli di questo attacco, come lo scopo e la portata, sarebbero stati ritrovati in una chat del dark web.[18] In questo caso le informazioni sembrano indicare una paternità diversa rispetto ai tentativi d'infiltrazione dello scorso ottobre ai danni di organizzazioni sportive e antidoping.[19]

Cosa rende tanto interessanti questi obiettivi? Prima delle gare gli attacchi possono servire a raccogliere informazioni sugli atleti di altri Paesi, sulle loro capacità, sui loro punti deboli e sui programmi, nella speranza di poter sviluppare delle strategie vincenti grazie a tali informazioni. Un altro motivo potrebbe essere quello di falsificare i risultati dei test antidoping. In alcuni Paesi lo sport è più che una competizione tra atleti – diventa un elemento di coesione sociale è può essere utilizzato a scopi politici,permettendo per esempio a dei dirigenti di approfittare della popolarità di certi sportivi di successo. Inoltre, le grandi manifestazioni sportive sono la cornice ideale per mettere in mostra le proprie conoscenze informatiche. Potenzialmente questo genere di attacchi offre altresì l'occasione di ricollocare, attraverso tecniche di *«false flag»* (false bandiere), le pedine dello scacchiere politico internazionale, mettendo in cattiva luce un Paese concorrente. Infine, in un Paese sottoposto a sanzioni, gli attacchi possono rispondere a un sentimento di rivalsa.

### 4.1.2 La campagna di spionaggio industriale targata «Winnti»

Stando alle ultime rivelazioni, il numero delle multinazionali tedesche che negli ultimi dieci anni sono state vittime di ciberattacchi è in aumento. Il gigante delle comunicazioni Siemens, ad esempio, ha recentemente confermato di avere subito un attacco nel giugno 2016 che tuttavia, a quanto pare, non avrebbe causato alcuna fuga di dati. La stessa sorte è toccata a Covestro, produttore di materie plastiche e adesivi, che non avrebbe riportato danni. Il colosso farmaceutico Bayer ha reso noto ad aprile di essere stato colpito da spionaggio informatico già nel 2018. Diversi esperti di sicurezza ritengono che tutti questi attacchi siano opera di Winnti,

17 https://blogs.microsoft.com/on-the-issues/2019/10/28/cyberattacks-sporting-anti-doping/

18 https://www.bleepingcomputer.com/news/security/tokyo-2020-staff-warns-of-phishing-disguised-as-official-emails/

19 https://english.kyodonews.net/news/2018/09/e2d8f3727275-phishing-scam-on-2020-olympics-tickets-spotted.html

nome che identifica sia un gruppo sia il malware da questo utilizzato, noto tra l'altro per essersi infiltrato nelle acciaierie ThyssenKrupp nel 2016. Diversi tra questi esperti sono concordi nel sostenere che questi attacchi siano d'origine cinese. [20]

All'inizio il gruppo si concentrava sulle piattaforme di gioco online, che attaccava a scopo puramente finanziario. Almeno dal 2015 ha esteso la propria attività allo spionaggio industriale e oggi sembra interessarsi soprattutto al settore chimico e farmaceutico, nonché alle aziende specializzate in tecnologie di punta. Oltre alle vittime già menzionate, nell'ambito di un'analisi approfondita, due radio tedesche (Bayerische Rundfunk e Norddeutsche Rundfunk) hanno rilevato vecchie infezioni che finora non avevano fatto notizia. Esse citano ad esempio la società Henkel, che come Covestro produce prodotti adesivi per l'industria e che era stata infiltrata nel 2014. Un'altra vittima confermata sarebbe BASF («Badische Anilin- und Soda-Fabrik»), una delle maggiori aziende del settore chimico a livello mondiale, anch'essa con sede in Germania. L'attacco subito nel 2015 non ha avuto conseguenze gravi.[21]

Dopo essersi infiltrati in una rete aziendale, gli hacker creerebbero una mappatura per poi individuare i punti strategici nei quali poter nascondere il malware. In tal modo possono agire indisturbati a lungo, senza farsi notare, e raccogliere informazioni sulla società e sui suoi prodotti, nella speranza di trovare dei segreti commerciali. La persistenza è una delle principali caratteristiche di Winnti. Attraverso l'installazione di backdoor, l'autore dell'attacco si procura un accesso permanente alla rete aziendale. Nell'ottobre 2019 la società di sicurezza informatica ESET ha reso noto di aver individuato una backdoor sconosciuta fino ad allora, che prende di mira Microsoft SQL (MSSQL) e utilizzate da questo gruppo.[22]

Sebbene dopo l'attacco a ThyssenKrupp Winnti sia finita sotto i riflettori in Germania, la campagna è attiva anche in altri Paesi dell'Europa occidentale, dell'Asia e negli Stati Uniti. Da una ricerca di ESET è emerso che il gruppo dovrebbe aver infettato tramite «PortReuse», una backdoor diventata famosa nel marzo 2019, un grande produttore di hardware e software per dispositivi mobili con sede in Asia. Con questa compromissione il gruppo di hacker si preparava probabilmente a un attacco su vasta scala, passando attraverso la catena di fornitura.[23]

Questo malware è infine utilizzato anche per spionaggio politico. Gli esperti di Kaspersky Lab sostengono che attualmente siano almeno due i gruppi che utilizzano questo strumento. Il che rende più complicato stabilire in via definitiva se lo spionaggio informatico in campo industriale sia stato perpetrato dagli stessi soggetti dediti principalmente a quello politico – contro il governo di Hong Kong o contro il provider indiano di servizi di telecomunicazione nella regione in cui si trova la sede principale del governo tibetano in esilio („Central Tibetan Administration, CTA").[24]

---

20 https://www.waz.de/wirtschaft/spionage-mehrere-dax-konzerne-von-hackern-angegriffen-id226573145.html; cfr. anche rapporto semestrale MELANI 2016/2, n. 5.1.3.

21 http://web.br.de/interaktiv/winnti/

22 https://www.zdnet.com/article/researchers-find-stealthy-mssql-server-backdoor-developed-by-chinese-cyberspies/; https://www.welivesecurity.com/2019/10/21/winnti-group-skip2-0-microsoft-sql-server-backdoor/

23 https://www.bleepingcomputer.com/news/security/winnti-group-uses-new-portreuse-malware-against-asian-manufacturer/

24 http://web.br.de/interaktiv/winnti/

Conclusione / Raccomandazione

Già da molti anni le «Advanced Persistent Threat» (APT) non sono più un problema esclusivo degli organi di Stato e militari. Anche le organizzazioni internazionali e le imprese private di numerosi settori si trovano a fare i conti sempre più spesso con attacchi ad alta complessità. Questo fatto può essere in parte spiegato come una democratizzazione degli attacchi più sofisticati, nel senso che gli strumenti utilizzati per lanciarli sono ormai largamente disponibili (vedi anche il Rapporto semestrale 2019/1, cap. 5.1.1). Ciò ha permesso di entrare in attività a un gran numero di attaccanti con differenti obiettivi. Intanto numerose aziende non dispongono né delle risorse economiche né delle conoscenze necessarie per combattere questo genere di minaccia.

Una possibile soluzione è affidare la sicurezza dei propri computer a esperti informatici esterni, come provider di servizi e di sicurezza cloud. Ma ciò non solleva l'impresa dalla responsabilità di adottare ulteriori provvedimenti interni per sensibilizzare e formare i collaboratori. Non va sottovalutato il rischio che (ex) collaboratori concedano a terzi l'accesso al sistema aziendale: sarebbe un modo semplice per arricchirsi, agire sulla scia di un risentimento personale o danneggiare intenzionalmente il datore di lavoro.

È auspicabile iscriversi a una o più reti pubbliche o private, dove ci si scambiano informazioni sulle minacce attuali e si danno suggerimenti su come riconoscere i rischi e su cosa può fare ogni individuo per tutelarsi.

Misure tecniche

Se un'analisi del rischio interna evidenzia un pericolo concreto per la vostra organizzazione o struttura, dovreste proteggervi adottando autonomamente delle misure tecniche per limitare le possibilità di infezione.

**A livello di sistema**

- Utilizzare «AppLocker» (o una funzione analoga) per prevenire l'esecuzione di dati binari sconosciuti, segnatamente dalle cartelle dei profili di utente
- Ridurre i privilegi per gli utenti che non li necessitano
- Utilizzare un allarme che segnali l'avvio dei tool di esecuzione del sistema

**Per l'Active Directory (AD)**

- Accurato monitoraggio dell'AD per riconoscere richieste insolite e di grosse dimensioni
- Introduzione di un'autenticazione a più fattori per l'AD e in particolare per l'accesso remoto
- Per i clienti Microsoft si consiglia inoltre di utilizzare regolarmente il servizio RAP as a Service (cfr. https://services.premier.microsoft.com/assess/)

**A livello di rete**

- Archiviazione dei dati log per un periodo di almeno due anni in caso di sistemi gateway importanti, come proxy DNS
- Esecuzione della tecnica Passive DNS per verificare rapidamente i domini sospetti
- Introduzione di «Snort», un Intrusion Detection System (IDS) basato su firma
- Adozione di politiche di segmentazione interne (in generale è meglio evitare la comunicazione client-client)
- Raccolta di dati Netflow su diversi punti della rete interna
- Scelta di un punto di controllo centrale per l'accesso a Internet che sia oggetto di un monitoraggio accurato
- Gestione out-of-band dei server che utilizzano una LAN di management, nessuna navigazione né e-mail dalla stazione gestionale
- Whitelisting dei proxy per i server internazionali che devono comunicare all'esterno.

## 4.2 Sistemi di controllo industriali

In un articolo comparso nel primo rapporto semestrale, nel 2005 MELANI scriveva a proposito delle nuove linee guida per la sicurezza informatica degli impianti nucleari negli Stati Uniti: «Il principale problema di sicurezza dei cosiddetti sistemi SCADA delle centrali nucleari (Supervisory Control and Data Acquisition) si situa negli ambiti attualmente poco cifrati della trasmissione di dati e di comandi, del collegamento alle reti pubbliche nonché nell'assenza di standardizzazione delle tecnologie».[25]

Da allora la consapevolezza in materia di sicurezza dei sistemi di controllo industriali (ICS) è considerevolmente aumentata. A ciò hanno senz'altro contribuito anche gli attacchi all'integrità dei processi gestiti dai sistemi industriali di controllo, dei quali si è avuta notizia negli ultimi 15 anni. Oltre agli attacchi ai sistemi stessi, che chiaramente possono causarne la compromissione, meritano un'attenzione particolare gli attacchi che colpiscono il processo gestito dai suddetti sistemi. Stuxnet[26] nel 2010, Industroyer/CRASHOVERRIDE[27] alla fine del 2016 e Triton/Trisis,[28] scoperto nel 2017, sono tra i più famosi. Al capitolo 4.2.1 analizziamo a scopo illustrativo il danno a livello processuale che si prefiggeva CRASHOVERRIDE nell'attacco contro l'approvvigionamento elettrico ucraino.

La maggiore presenza in rete di sistemi di gestione nonché di attori e di sensori ha contribuito a complicare notevolmente la messa in sicurezza efficace di tali infrastrutture di sistema. L'«Industrial Internet of Things» (IIoT) rende possibili nuovi e promettenti processi di automatizzazione, ma allo stesso tempo allarga la superficie di attacco anche a tali processi. Garantire un livello adeguato delle misure di sicurezza continua a essere una sfida non ancora completamente superata.

### 4.2.1 L'approvvigionamento elettrico ancora nel mirino

Nel dicembre 2016 un attacco informatico ha colpito la rete elettrica ucraina provocandone il blackout.[29] In quella occasione i tecnici di Ukrenergo operativi nella sottostazione Nord nei pressi di Kiev erano però riusciti a ripristinare l'alimentazione elettrica mediante interventi manuali, dopo circa un'ora. Le nuove analisi[30] di questo attacco sferrato con il malware CRASHOVERRIDE mostrano tuttavia che nelle intenzioni degli autori era prevista, se l'operazione fosse andata a buon fine (cfr. fig. 3), la distruzione fisica degli elementi di rete. Uno degli obiettivi, tuttavia mancato, era colpire i relè di protezione della rete di trasmissione, mettendone fuori uso («denial of service») la funzione di protezione. Senza la protezione dei relè abbinata alla mancanza di visibilità nei sistemi di controllo attaccati, una sequenza di accensione sfavorevole avrebbe potuto danneggiare parte della rete, che a sua volta, oltre ai danni fisici, avrebbe protratto il blackout.

---

25 Rapporto semestrale MELANI 2005/1, n. 7.1.

26 Rapporto semestrale MELANI 2010/2, n. 4.1.

27 Rapporto semestrale MELANI 2017/1, n. 5.3.

28 Rapporto semestrale MELANI 2017/2, n. 5.3.2.

29 Rapporto semestrale MELANI 2016/2, n. 5.3.1.

30 https://dragos.com/resource/crashoverride-reassessing-the-2016-ukraine-electric-power-event-as-a-protection-focused-attack/


*Figura 3: Andamento previsto dell'attacco (fonte: dragos.com)*

Conoscere le intenzioni degli aggressori mostra quanto sia importante contenere il più possibile i rischi nelle aree critiche. Secondo un rapporto della Commissione federale dell'energia elettrica (ElCom)[31] del 2019, nel quadro dell'approvvigionamento di energia elettrica in Svizzera esiste ancora un potenziale di ottimizzazione nell'attuazione di misure di sicurezza adeguate.[32] L'ElCom afferma quindi, tra le altre cose, che «i sistemi OT devono essere regolarmente testati per valutarne la vulnerabilità». Nel periodo in rassegna si è venuti ad esempio a conoscenza di una serie di vulnerabilità[33] del sistema operativo in tempo reale VxWorks, che costituisce la base di molti sistemi di controllo specifici delle applicazioni. Questa profonda integrazione richiede il coinvolgimento di un'intera filiera di produttori di sistemi e gestori per colmare le lacune dei sistemi di controllo dei processi operativi. Un domani le lacune di sicurezza note a livello della gestione di processo potrebbero aumentare sensibilmente, in quanto in futuro, oltre ai sistemi IT classici, la competizione in atto tra hacker volta a individuare le falle dei software Pwn2Own[34] dovrebbe riguardare anche gli ICS. Oltre ai sistemi in uso, alla rete vengono collegati sempre più elementi[35] e questo complica ulteriormente l'implementazione coordinata delle direttive in materia di sicurezza con il coinvolgimento di tutti i fornitori interessati.

Per giunta sempre più aggressori prendono di mira il settore dell'approvvigionamento elettrico[36] e la relativa filiera di fornitura[37]. A fine estate 2019 si sono registrate negli Stati Uniti due ondate di *spear-phishing* che hanno colpito i distributori di energia elettrica e che avevano come obiettivo l'intrusione nelle aziende target attraverso il malware LookBack. Inoltre gli aggressori sfruttano il nome degli organi preposti alla concessione di licenza, noti nel settore, per indurre i destinatari ad aprire gli allegati. Una volta installato, il malware si comporta come un

31 https://www.elcom.admin.ch/dam/elcom/de/dokumente/2019/Cyber-Sicherheit%202019%20-%20Bericht%20der%20ElCom.pdf.download.pdf/Cyber-Sicherheit%202019%20-%20Bericht%20der%20ElCom.pdf

32 https://www.tagesanzeiger.ch/schweiz/standard/fuer-hacker-stehen-die-einfallstore-offen/story/20223699

33 https://www.armis.com/urgent11/

34 https://www.darkreading.com/vulnerabilities---threats/pwn2own-adds-industrial-control-systems-to-hacking-contest/d/d-id/1336191

35 https://www.zdnet.com/article/ameo-concerned-about-nation-state-attacks-on-power-grids/

36 https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks

37 https://www.wired.com/story/iran-apt33-industrial-control-systems/

«Remote Access Trojan» (RAT), mettendo a disposizione dell'aggressore infinite funzionalità dei sistemi infettati, tramite accesso remoto.

In un'ottica di transizione dai combustibili fossili alla mobilità elettrica, l'approvvigionamento elettrico acquisisce ancora maggior rilievo. Allo stesso tempo gli obiettivi fissati nel quadro delle politiche energetiche dislocano ulteriormente la produzione di energia dalle grandi centrali elettriche ai piccoli impianti decentralizzati di energie rinnovabili. A questo si aggiunge l'informatizzazione dell'approvvigionamento elettrico (SmartGrid). In collaborazione con i produttori di energia e i gestori di rete, MELANI si propone di salvaguardare nel miglior modo possibile l'approvvigionamento della Svizzera dalla presenza di rischi per la sicurezza delle informazioni. L'affidabilità dell'approvvigionamento elettrico è un fattore centrale per il funzionamento dell'economia e della società e per la conservazione del nostro benessere.

Raccomandazione

Invitiamo i lettori a segnalarci eventuali sistemi di controllo presenti in Internet, che siano accessibili al pubblico o protetti in modo inadeguato, in modo da poterne informare i gestori.


Formulario d'annuncio MELANI
https://www.melani.admin.ch/melani/it/home/meldeformular.html


Lista di controllo delle misure di protezione dei sistemi di controllo industriali:
https://www.melani.admin.ch/melani/it/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-industriellen-kontrollsystemen--ics-.html

## 4.3 Attacchi (DDoS, defacement, drive-by)

### 4.3.1 DDoS per ricattare o compromettere un servizio

Nella settimana a cavallo tra il 2019 e il 2020 si sono registrati attacchi DDoS contro i media svizzeri online[38] e alcune pagine web sono state temporaneamente irraggiungibili. Ad oggi il motivo non è chiaro.

L'acronimo DDoS («Distributed Denial of Service», negazione del servizio) indica un attacco ai sistemi informatici allo scopo di limitarne la disponibilità. Nell'ultimo semestre si è nuovamente registrato un aumento di attacchi DDoS a scopo di estorsione.[39] Spesso gli aggressori

[38] https://www.20min.ch/digital/news/story/Technische-Probleme-auf-20minuten-ch-12858361; https://www.nzz.ch/wirtschaft/cyberattacke-gegen-schweizer-medien-ld.1530906

[39] A proposito di questo modus operandi, si veda il rapporto semestrale MELANI 2016/1, n. 4.4.1 e altri contributi dei rapporti semestrali MELANI 2018/1, n. 4.3.1; 2017/2, n. 4.3.1; 2016/2, n. 4.4.1; 2015/2, n. 4.3.4, e 2015/1, n. 4.4.1.

lanciano un primo attacco di prova per dimostrare di possedere tali capacità e pretendono poi dalla vittima il pagamento di un riscatto, per scongiurarne uno più potente successivo. Questi attacchi possono avere anche motivazioni politiche, come dimostrato nel caso dell'attacco alle pagine web del Partito Laburista britannico.[40] Tuttavia, secondo alcuni ricercatori in materia di sicurezza, la tendenza prevalente è quella di attacchi di minore intensità, che evitano di innescare le misure difensive DDoS, ma pregiudicano comunque le prestazioni delle pagine web o dei server.[41]

Raccomandazione

MELANI raccomanda varie misure preventive e reattive per contrastare gli attacchi DDoS.


Lista di controllo delle misure contro gli attacchi DDoS:

https://www.melani.admin.ch/melani/it/home/dokumentation/checklisten-und-anleitungen/massnahmen-gegen-ddos-attacken.html

### 4.3.2 «Drive-by»: la situazione in Svizzera

Sono diverse le modalità con le quali un software maligno può infettare un dispositivo. Uno dei metodi diffusi consiste nell'hackerare le pagine web inserendo uno script, il quale, attraverso vari tentativi di *exploit*, cerca di individuare le lacune di sicurezza presenti nel browser o in altre applicazioni, come FlashPlayer. Dato che visitare il sito web manipolato potrebbe già essere sufficiente per infettarsi, si parla di infezione da «drive-by download».

Nel secondo semestre del 2019 MELANI ha individuato circa 500 siti web infettati in Svizzera e ne ha informato i gestori affinché li ripulissero.

Gli utenti che scoprono siti web infetti sono pregati di segnalarli a MELANI per contribuire alla sicurezza generale.

Raccomandazioni

1. Installate almeno due browser diversi. In questo modo, se dovesse emergere una grave lacuna di sicurezza in uno dei due, potrete passare all'altro senza problemi.
2. Installate sempre gli ultimi aggiornamenti per i vostri browser, preferibilmente attraverso la funzione di aggiornamento automatica.
3. Se possibile utilizzate un cosiddetto «*ad blocker*» e limitate al massimo l'uso di *JavaScript*.
4. Se un sito web vi chiede improvvisamente di scaricare un file, non accettate mai.

40 https://www.theregister.co.uk/2019/11/12/labour_party_reports_cyber_attack/

41 https://www.zdnet.com/article/ddos-attacks-getting-smaller-sneakier-and-more-dangerous/#ftag=RSSbaffb68

### 4.3.3 Ciberattacco contro la piattaforma per criptovalute Upbit

Le piattaforme per lo scambio di criptovalute sono sempre un bersaglio redditizio per gli aggressori, perché quando un attacco va a buon fine riescono a rubare molto denaro. Così è andata anche per la piattaforma sudcoreana Upbit, dove gli aggressori hanno sottratto 342 000 *Ether* dall'«*Exchange Hot Wallet*». Al momento del furto il valore di questi Ether era di 48,5 milioni di dollari. Parrebbe si sia trattato di una cosiddetta «exit scam»: gli insider trasferiscono sul proprio conto il denaro di utenti della piattaforma, sostenendo di essere stati vittime di un ciberattacco. Tuttavia trasformare gli Ether rubati in denaro contante è un'operazione complessa, perché è molto impegnativo «riciclarli»[42] se si vuole impedirne la tracciabilità fino all'origine.[43]

## 4.4 Ingegneria sociale e phishing

### 4.4.1 Phishing

Nel secondo semestre 2019 si sono registrati moltissimi attacchi di phishing, soprattutto sfruttando i nomi di vari marchi svizzeri. Il contenuto delle e-mail è sempre più o meno lo stesso: alcune chiedono i dati della carta di credito per poterli «verificare», altre contengono un link che rimanda a una pagina nella quale si chiede di effettuare il login e inserire la password per usufruire dei servizi Internet. In questi messaggi di phishing si fa regolarmente un uso illegittimo dei loghi di aziende famose o del servizio interessato per conferire una parvenza di ufficialità alle e-mail. I servizi e-mail continuano a essere costantemente bersagliati, in quanto potendo disporre dei dati di accesso agli account di posta elettronica aumentano le possibilità di effettuare ulteriori attacchi.

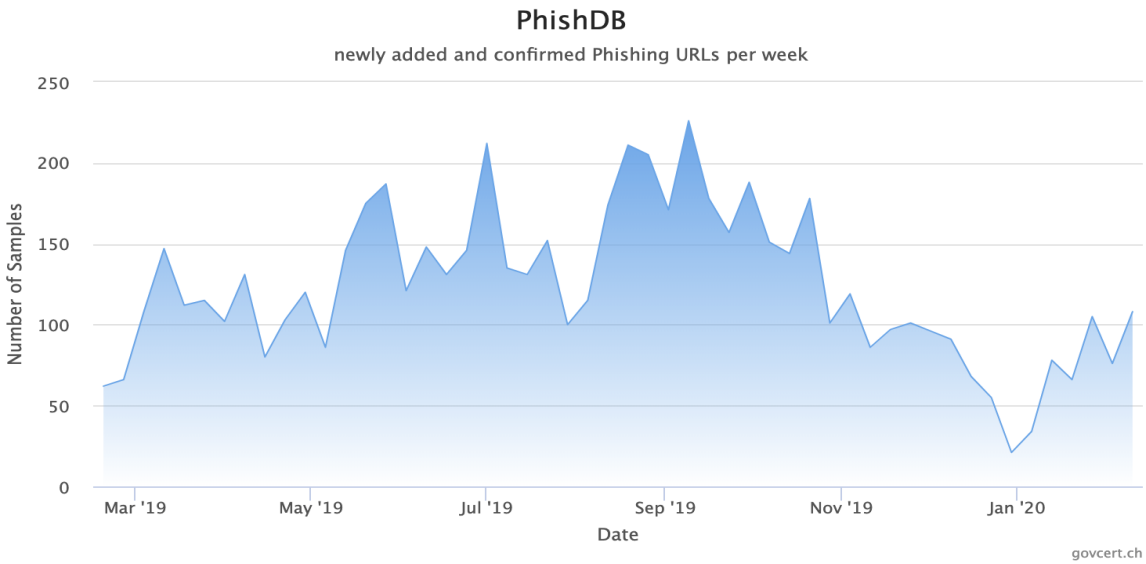


*Figura 4: Pagine di phishing segnalate e confermate settimanalmente su antiphishing.ch nell'ultimo anno; data di riferimento: 9 febbraio 2020.*

42 Cfr. anche n. 5.3

43 https://www.zdnet.com/article/upbit-cryptocurrency-exchange-loses-48-5-million-to-hackers/

### 4.4.2 Siti web di phishing con pagine di errore 404

Nei siti web si utilizzano le pagine di errore 404 per informare il visitatore che la sottopagina che intendeva visitare nel sito non è (più) disponibile all'indirizzo richiamato. Durante la progettazione di un sito web, la maggior parte dei gestori crea una pagina di errore 404 per questo genere di situazioni e la archivia come segnalazione di errore standard. Quando poi si verifica l'errore 404, è possibile inserire nella pagina i contenuti desiderati così da informare in modo mirato il visitatore ed eventualmente indirizzarlo altrove. Come in ogni pagina, anche in questa è possibile inserire contenuti maligni, come phishing o infezioni drive-by. Nell'agosto scorso Microsoft ha riferito di aver scoperto una campagna di phishing di questo tipo ai danni dei propri utenti. Una pagina di phishing, che imita perfettamente il portale per la registrazione in un account Microsoft, è stata archiviata come pagina di errore 404 nel sito web di un dominio registrato da soggetti criminali. Ciò vuol dire che ogni volta che un utente richiamava nel sito web un URL inesistente, veniva indirizzato alla pagina di errore 404 manipolata, ossia alla pagina di phishing.[44] Grazie a questo metodo gli aggressori possono creare un numero illimitato di URL di phishing secondo il principio della casualità e quindi renderne più complicati l'individuazione e il blocco in base ai link nelle e-mail, visto che gli URL hanno in comune solo il nome di dominio.


I criminali che si nascondono dietro le pagine di phishing sono costantemente alla ricerca di nuove possibilità per indurre gli utenti a cliccare su un link maligno. Quindi riflettete bene prima di cliccare su un link contenuto in un'e-mail o in un messaggio sullo smartphone. Sul nostro sito web potete trovare numerosi consigli:

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


Potete segnalare casi di phishing al seguente indirizzo:

https://www.antiphishing.ch/

Le vostre segnalazioni ci aiutano ad adottare misure e quindi a proteggere altri utenti.

### 4.4.3 Ricatto tramite illazioni: nuove varianti

Già da tempo i criminali inviano delle e-mail nelle quali sostengono di avere accesso al computer e alla webcam del destinatario, minacciandolo di divulgare immagini o materiale video compromettente, se non sarà disposto a pagare un riscatto in una criptovaluta entro una certa scadenza («*fake sextortion*»). Spesso queste e-mail contengono password e/o numeri di telefono realmente collegati ai destinatari. MELANI è a conoscenza di casi recenti, nei quali le potenziali vittime ricevevano, poco prima della scadenza del termine, un avvertimento, che ricordava loro la scarsità del tempo a disposizione e le conseguenze che sarebbero scaturite da un eventuale mancato pagamento.

---

44 https://www.bleepingcomputer.com/news/security/microsoft-warns-of-phishing-attacks-using-custom-404-pages/

Sono tuttavia stati registrati anche casi in cui il mittente sosteneva di essere in possesso di file video che ritraevano il destinatario durante il consumo di materiale pedopornografico. Per intimidire il destinatario, ai file allegati veniva assegnato un nome personalizzato o il suo indirizzo e-mail. Naturalmente anche le donne possono essere vittime di tali raggiri.

Esistono poi esempi di e-mail ricattatorie, in cui vengono utilizzate criptovalute diverse dai classici bitcoin. Ciò avviene in quanto i criminali suppongono che gli strumenti per tracciare il pagamento in criptovalute meno diffuse non siano ancora perfettamente funzionanti. Sono stati utilizzati anche *codici QR* al posto degli indirizzi di *wallet* per esteso, perché questi ultimi possono venir riconosciuti dai software di sicurezza, che spesso bloccano le e-mail che li contengono come fraudolente. Ciò dimostra ulteriormente l'importanza di abbinare misure di sicurezza tecniche a campagne di sensibilizzazione per una prevenzione efficiente dei ciberattacchi.

MELANI è inoltre informata di minacce che fanno riferimento addirittura a possibili attacchi con acido o all'impiego di assassini su commissione. Tuttavia questo genere di e-mail ricattatorie non sono così diffuse come la truffa della fake sextortion. Ciò è senz'altro riconducibile al fatto che, in presenza di una minaccia di violenza fisica, sia più difficile indurre qualcuno a non rivolgersi alle autorità, come invece avviene nei casi di fake sextortion, nei quali si fa riferimento a comportamenti intimi che si riferiscono al passato.

I ricercatori di sicurezza informatica[45] hanno scoperto per quale motivo le campagne di sextortion abbiano registrato ondate così abbondanti. Ad oggi oltre 450 000 computer sono stati infettati dal malware Phorpiex e riuniti in una *botnet*, della quale si servono i criminali per effettuare gli invii di massa delle loro e-mail ricattatorie. Gli indirizzi e-mail dei destinatari vengono prelevati secondo una modalità casuale da banche dati con indirizzi di posta elettronica. I contenuti delle e-mail vengono creati utilizzando moduli di testo, il che accresce ulteriormente il livello di automazione. La frequenza di invio è relativamente elevata, con circa 30 000 e-mail di sextortion all'ora. Le campagne hanno una portata di 27 milioni di vittime potenziali.



Non lasciatevi intimorire da illazioni e minacce. Non rispondete ad e-mail ricattatorie e in caso di dubbi rivolgetevi alle autorità. Maggiori informazioni sulle e-mail di fake sextortion sono disponibili all'indirizzo https://www.stop-sextortion.ch/, dove potrete anche segnalarle. Se utilizzate ancora la password citata nell'e-mail, cambiatela immediatamente. In generale le password dovrebbero essere modificate regolarmente, evitando altresì di utilizzare la stessa password per più servizi Internet. Per una prevenzione efficiente degli attacchi informatici è auspicabile abbinare alle misure di sicurezza anche campagne di sensibilizzazione.

45 https://m.pctipp.ch/news/artikel/user-pc-fuer-sextortion-spam-missbraucht-93135/

### 4.4.4 Compromissione delle e-mail aziendali: un modus operandi radicato e in costante evoluzione

Dal 2013 MELANI si è più volte occupata nei suoi rapporti semestrali della frode a danno di presidenti e dirigenti, la cosiddetta «*CEO fraud*» (truffa del CEO).[46] Con il passare del tempo questo fenomeno ha conosciuto molte varianti, i criminali migliorano costantemente il modus operandi per raggiungere nuovi obiettivi e colpire nuove vittime.

Sempre più spesso, negli ultimi anni, i truffatori hanno assunto l'identità di fornitori inviando ai rispettivi clienti delle fatture con un IBAN diverso da quello legittimo. Non di rado i criminali si procurano le informazioni necessarie per falsificare le fatture originali, infiltrando un account di posta elettronica o una piattaforma di collaborazione online.[47] Negli Stati Uniti le più recenti statistiche della «Financial Crimes Enforcement Network» (FINCEN) confermano l'aumento del trend di appropriazione indebita delle identità dei partner commerciali esterni dell'azienda presa di mira.[48] L'analisi della FINCEN fornisce inoltre dati interessanti sui settori di attività colpiti: in America sono particolarmente prese di mira l'industria manifatturiera e quella delle costruzioni. Forse questo si può spiegare con il fatto che tali settori dipendono in modo particolare da fornitori esterni e collaborano con molti subappaltatori. Malgrado ciò tutti i settori sono potenziali obiettivi di ciberattacchi di qualunque genere.

Sono però sempre più frequenti anche i tentativi di truffa nei quali gli aggressori fingono di essere una persona dell'azienda presa di mira. I criminali cercano di sfruttare i progressi compiuti dalla tecnologia per migliorare il proprio modus operandi. Nel settembre 2019 il Wall Street Journal ha riferito di un caso nel quale i truffatori non si sono limitati a fingere di essere il CEO tramite e-mail: grazie ai software di riconoscimento vocale e all'intelligenza artificiale i criminali erano in grado di imitare la voce dell'amministratore delegato e di indurre per telefono gli ignari collaboratori a trasferire del denaro.[49]

In una variante di questa tecnica, osservata di recente anche in Svizzera, i criminali si fingono collaboratori di un'impresa e scrivono ai colleghi addetti al pagamento degli stipendi (di norma le risorse umane) per comunicare che il «loro» stipendio deve essere versato da subito su un conto bancario diverso. Questo fenomeno era stato già documentato scrupolosamente all'inizio del 2019 da Trustwave, fornitore di soluzioni per la sicurezza[50]. Nel caso descritto da Trustwave i truffatori creavano degli indirizzi presso i servizi di posta elettronica gratuiti per poi procurarsi le informazioni necessarie all'attacco, come ad esempio l'identità delle persone addette agli stipendi, semplicemente dalle fonti accessibili (siti web aziendali, social network ecc.).

---

46 Rapporti semestrali MELANI 2013/1, n. 3.4; 2016/1, n. 4.5.1; 2016/2, n. 4.5.1; 2017/1, n. 4.3.3; 2018/2, n. 4.4.3, e 2019/1, n. 4.4.5.

47 Cfr. Rapporto semestrale MELANI 2018/2, n. 4.4.3

48 https://www.fincen.gov/sites/default/files/shared/FinCEN_Financial_Trend_Analysis_FINAL_508.pdf

49 https://www.zdnet.com/article/forget-email-scammers-use-ceo-voice-deepfakes-to-con-workers-into-wiring-cash/

50 https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/bec-payroll-scam-your-salary-is-mine/

Conclusione / Raccomandazione

Vista la grande creatività dei criminali e la loro abilità nell'adeguare costantemente il proprio modus operandi, la difesa dai tentativi di frode continua a essere una sfida per tutte le aziende. Sensibilizzate i collaboratori sottolineando la necessità per tutti di rispettare i processi e le misure di sicurezza stabiliti dall'impresa in qualsiasi circostanza. In particolare tutti i trasferimenti di denaro devono avvenire con firme collettive secondo il principio del doppio controllo. Particolare attenzione va riservata agli annunci che riguardano i cambiamenti di conto.


Informazioni e raccomandazioni sul tema della truffa del CEO:
https://www.melani.admin.ch/melani/it/home/themen/CEO-Fraud.html

### 4.4.5 Truffe di trading online

Nel semestre in analisi MELANI ha ricevuto diverse segnalazioni inerenti false piattaforme di trading online e siti web che le pubblicizzavano sponsorizzano promettendo celeri e lauti guadagni grazie alle criptovalut.. Questa pubblicità ingannevole viene spesso divulgata attraverso i social network e usa in modo illecito i nomi di personaggi famosi per risultare più credibile. In interviste fittizie, star del calibro di Roger Federer e DJ Bobo dichiarano che parte del loro patrimonio è merito dei bitcoin. La rete mette in guardia dal rischio di perdere il denaro investito.[51] Nella nostra epoca le «fake news» sono un fenomeno diffuso. Per difendersi è necessario assumere un atteggiamento critico nei confronti di notizie bizzarre o provenienti da fonti dubbie.

Inoltre il trading è, di principio, un'attività rischiosa. Se poi si viene contattati attivamente e in termini impersonali da una piattaforma di trading (ad esempio sui social network, via e-mail, SMS o WhatsApp), si può concludere che si tratta di invii di massa non affidabili. Un video esplicativo dell'Autorità federale di vigilanza sui mercati finanziari (FINMA) illustra dettagliatamente questo problema e spiega come difendersi da questo genere di truffa.[52] La FINMA ha altresì pubblicato un elenco di piattaforme elettroniche riconosciute.[53] Occorre tenere presente che anche la pubblicità (di massa) di offerte di dubbia validità può essere provvista in modo automatizzato del nome e di altri dati personali.

## 4.5 Fughe di dati

### 4.5.1 I dati dei pazienti sono accessibili

Nell'ambito di una ricerca[54] condotta nell'estate 2019 sono stati scoperti in rete diversi milioni di dati non protetti di pazienti di vari Paesi: si trattava di dati medici sensibili contenuti in server

51 https://www.20min.ch/schweiz/news/story/Wieso-stoppt-niemand-die-Bitcoin-Betrueger--13654244
52 https://finma.ch/it/documentazione/finma-videos/schutz-vor-anlagebetrug/
53 https://www.finma.ch/it/finma-public/bewilligte-institute-personen-und-produkte/
54 https://www.br.de/nachrichten/deutschland-welt/millionenfach-patientendaten-ungeschuetzt-imnetz,RcF09BW

Internet non protetti rimasti accessibili a chiunque per anni. Tra questi dati figuravano radiografie ad alta definizione complete di dati personali, tra i quali nome e cognome, data di nascita, data dell'esame e informazioni sul medico curante o sul trattamento stesso. Gli esami di diagnostica per immagini vengono inviati dai dispositivi a server speciali utilizzati per l'archiviazione delle immagini (cosiddetti «Picture Archiving and Communication Systems», PACS). Stiamo parlando di circa 50 Paesi e 16 milioni di dati. Tra i più colpiti figurano i pazienti degli Stati Uniti. In Germania i dati in questione sarebbero 13 000. L'Ufficio federale per la sicurezza informatica della Germania (BSI), che ha informato 46 Paesi, è in contatto con il gestore del server PACS tedesco e inoltre sta verificando le disposizioni legali inerenti eventuali misure di sorveglianza, che vanno dalle raccomandazioni tese a migliorare la sicurezza informatica fino alla comminazione di sanzioni. Dalle analisi svolte da MELANI non sono emersi dati di pazienti svizzeri, benché qualche server PACS si trovasse in Svizzera.

Sulla base del seguente esempio è possibile constatare la grande responsabilità degli organi di condotta aziendali.

Alcuni produttori di installazioni mediche non si limitano a commercializzarle, ma forniscono anche l'assistenza tecnica post vendita. In qualità di erogatrice di servizi, un'impresa è tenuta a rispettare gli standard di sicurezza generali e settoriali, nonché quelli concordati contrattualmente. Queste nozioni sono di cruciale importanza per la gestione del rischio nelle aziende mediche: il destinatario di una prestazione di servizi da parte di un terzo è responsabile di informarsi circa le misure di sicurezza effettive del prestatore del servizio e di richiedere la relativa documentazione. In tal modo è possibile accertare se i dati prodotti a livello aziendale interno sono adeguatamente trattati e archiviati dal prestatore di servizi esterno. Tali concetti di sicurezza dovrebbero essere verificati da un ufficio indipendente esterno.

Due altre fughe di dati nel settore sanitario evidenziano la portata di questo fenomeno e gli oneri di gestione che ne conseguono. Due società con sede negli Stati Uniti – un centro medico e un fornitore del settore medico – hanno riferito di fughe di dati a danno di circa 220 000 persone in totale.[55] Tali fughe di dati sono avvenute a seguito di un caso di phishing e di un attacco ransomware.

Nel corso di una campagna di phishing mirata, alcuni hacker sono riusciti ad accedere agli account Office 365 dei collaboratori e così hanno potuto muoversi indisturbati per circa due mesi nei vari account di posta elettronica. Probabilmente gli aggressori hanno avuto accesso alle informazioni presenti e passate di pazienti e collaboratori e se ne sono appropriati. Tra le informazioni potenzialmente trafugate figurano nome e cognome, indirizzo, data di nascita, numero di assicurazione sociale, numero di identificazione del collaboratore, informazioni di carattere medico, informazioni dell'assicurazione malattia, informazioni finanziarie, informazioni di pagamento, dati della licenza di condurre, dati del passaporto, password/PIN o credenziali dell'account e dati di fatturazione[56].

Nel caso dell'attacco ransomware al centro medico, che riuniva diversi prestatori di servizi del settore sanitario, sono stati crittografati gli schedari di dati di un membro del centro medico.

---

55 https://www.inforisktoday.com/2-health-data-breaches-affect-total-220000-a-13440

56 In un caso analogo gli hacker avevano accesso anche a informazioni come diagnosi e trattamento medico: https://www.bleepingcomputer.com/news/security/phishing-incident-exposes-medical-personal-info-of-60k-patients/

Grazie alle copie di sicurezza (backup) è stato possibile ripristinare l'accesso ai dati medici. Tuttavia i responsabili non sono stati in grado di garantire nuovamente l'accesso a tutte le informazioni interessate. L'azienda ritiene che l'episodio non abbia comportato la divulgazione a terzi delle informazioni sui pazienti.

In entrambe le circostanze le persone interessate sono state informate e con la notifica dell'accaduto è stato offerto loro un servizio gratuito di monitoraggio del credito per un certo periodo di tempo, allo scopo di impedire eventuali usurpazioni d'identità.

Raccomandazioni

Per le imprese la gestione del rischio secondo un approccio globale è di fondamentale importanza. Le fughe di dati di maggiore entità riguardano regolarmente anche i fornitori terzi. Le aziende di tutti i settori devono formulare precisi requisiti di sicurezza nei confronti dei fornitori terzi e farli inserire nei contratti. In tale ambito si dovrebbero affrontare anche le questioni legate alla prevenzione degli attacchi nonché alla gestione delle crisi e della continuità aziendale («Business Continuity Management», BCM). Dovreste inoltre accertarvi che la copertura dell'assicurazione contro i ciber-rischi del fornitore terzo sia sufficiente per coprire i danni derivanti dalla perdita dei dati di tutti i clienti.

### 4.5.2 Fughe di dati presso Sytech, partner industriale dei servizi segreti russi

Il 13 luglio 2019, presso l'azienda Sytech, sarebbe stato hackerato un uomo di contatto dei servizi segreti russi (FSB). BBC News Russian ha riferito che gli hacker hanno rubato dalla rete del mandatario 7,5 terabyte di dati, che comprendevano informazioni su numerosi progetti segreti elaborati da Sytech per conto del governo russo e dei suoi servizi segreti. I dati trafugati sono poi stati ceduti a un altro gruppo di hacker che li ha condivisi con i media russi. Stando a BBC News Russian si tratta della più grande divulgazione di dati non autorizzata nella storia dei servizi segreti russi.[57]

I dati riguardano numerosi progetti, tra cui:

1. «Mentor» (sviluppato presumibilmente per l'unità militare russa n. 71330) è l'intelligence radioelettronica dei servizi segreti russi, il cui fine è monitorare gli account di posta elettronica a intervalli regolari di tempo per raccogliere informazioni in determinate fasi;
2. «Nadezhda / Hope» è un progetto finalizzato a visualizzare il collegamento tra la Russia e il resto di Internet. Tale ricerca è parte del tentativo della Russia di creare un «Internet sovrano» nell'ambito del quale essa possa appunto isolarsi dal resto di Internet;
3. «Nautilus» è un progetto sviluppato tra il 2009 e il 2020 per raccogliere informazioni sugli utenti di social network come Facebook, LinkedIn e MySpace;
4. «Nautilus-S» è invece una ricerca che punta alla deanonimizzazione degli utenti della rete Tor attraverso la creazione di nodi di uscita controllati dal governo russo.

Nel frattempo il sito web di Sytech (www.sytech.ru) è stato disattivato e l'azienda non ha risposto alle domande della BBC.

---

57 https://www.bleepingcomputer.com/news/security/russian-fsb-intel-agency-contractor-hacked-secret-projects-exposed/

## 4.6 Crimeware

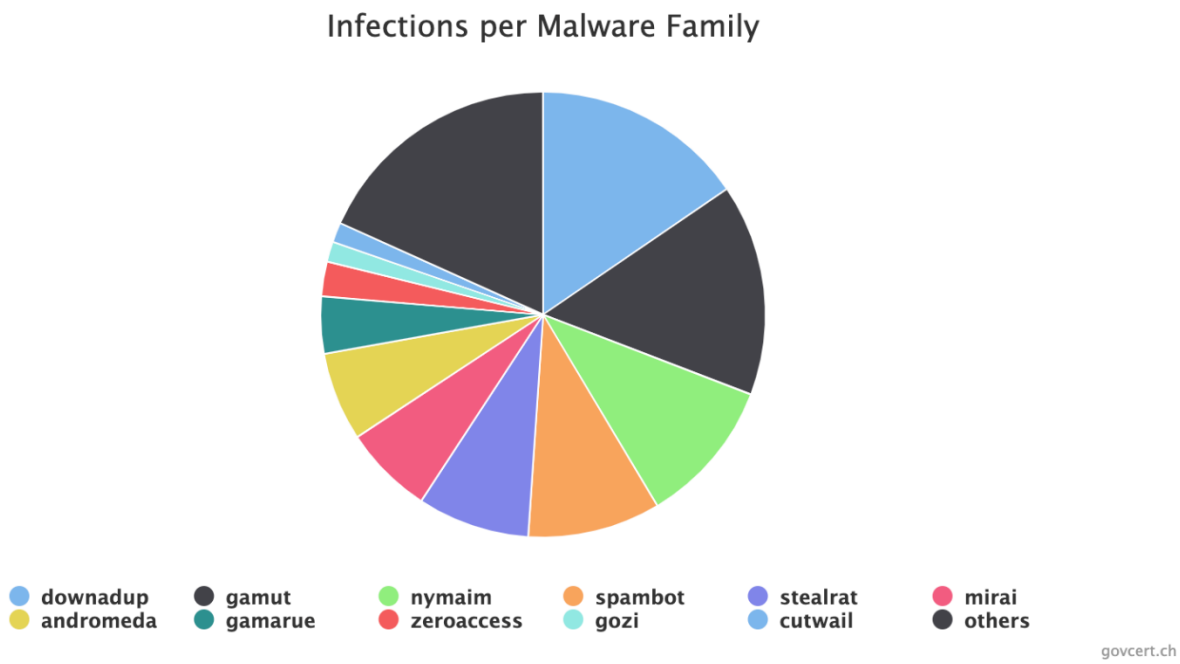


*Figura 5: Ripartizione dei malware in Svizzera nota al NCSC con l'ausilio di DNS sinkhole. Data di riferimento: 9 febbraio 2020. I dati aggiornati sono pubblicati all'indirizzo: http://www.govcert.admin.ch/statistics/dronemap/*

### 4.6.1 Ransomware: ultimi sviluppi

Immaginate di voler acquistare i biglietti per la partita della vostra squadra del cuore, ma al momento la prevendita online non è disponibile. Vi recate allora di buona lena al botteghino. Purtroppo non avete contante con voi e il lettore di carte non funziona. Il bancomat più vicino dista un paio di chilometri, che percorrete a piedi perché anche gli autobus hanno smesso di funzionare. Tutto ciò a causa di un malware che ha danneggiato diversi sistemi informatici a scopo di estorsione.

Questo genere di scenario è solo in parte immaginario: nell'anno in rassegna si è realmente verificato un attacco *ransomware* a scapito di una società di calcio, che ha avuto le conseguenze elencate sopra sul sistema dei biglietti e dei pagamenti.[58] Per quanto riguarda i trasporti pubblici è stato registrato un piccolo guasto, sempre a causa di un attacco sferrato dagli hacker.[59] L'ipotesi descritta può considerarsi immaginaria solo in quanto i due eventi sono accaduti in un lasso spazio-temporale distinto.

L'ondata massiccia e persistente di ransomware, che aveva spinto MELANI a dedicare il tema principale dello scorso rapporto semestrale a questa minaccia, non si è affievolita. Anche negli

58 https://www.inside-it.ch/de/post/der-gehackte-fc-basel-und-die-konsequenzen-20191205

59 https://www.20min.ch/ro/news/romandie/story/Les-TPF-victimmes-d-une-attaque-informatique-23708264

ultimi sei mesi gli attacchi sia su scala nazionale che internazionale sono stati numerosi, si sono inoltre definite delle nuove tendenze.

Il settore sanitario internazionale è stato fortemente interessato da tali eventi anche nel secondo semestre 2019. A novembre i sistemi informatici offline dell'ospedale universitario di Rouen in Francia sono stati compromessi da un ransomware e il personale ha dovuto provvisoriamente elaborare i dati in modalità analogica.[60] In Germania alcuni mesi prima erano stati crittografati i server di 18 ospedali.[61] Dagli Stati Uniti giungono dati ancora più allarmanti: il ransomware Ryuk si è introdotto nell'azienda IT Virtual Care Provider Inc. (VCPI), che fornisce hosting di dati nel cloud, sicurezza e gestione degli accessi a oltre 100 case di cura americane. L'attacco ha reso inaccessibili le cartelle cliniche dei pazienti.[62] Ryuk prende di mira soprattutto aziende e organizzazioni con cifre d'affari elevate per estorcere riscatti cospicui. Le aziende che gestiscono le infrastrutture IT di numerosi clienti sono un obiettivo strategico, perché consentono di diffondere il contagio e possono rivelarsi estremamente redditizie. Nel mese di ottobre Ryuk ha crittografato i dati di 400 cliniche veterinarie statunitensi della «National Veterinary Associates». A quanto pare l'infezione della *active directory* e di un *exchange server* era già avvenuta durante l'estate. Siccome non era stata eliminata completamente, l'infezione è tornata dopo aver avuto il tempo di diffondersi nuovamente.[63] Ryuk viene spesso veicolato da una precedente infezione dei trojan Emotet o Trickbot, come pare sia avvenuto almeno per uno degli attacchi citati (per un approfondimento dello schema di attacco a più livelli consultare il rapporto semestrale MELANI 2019/1, n. 3.4.1).

Ryuk non è però il solo a utilizzare un processo con differenti stadi d'infezione. Negli ultimi tempi questo modus operandi evidentemente redditizio è diventato sempre più frequente. Un *dropper* ultimamente osservato sia in Svizzera che all'estero è Ostap che di solito scarica il trojan TrickBot. Quest'ultimo si diffonde all'interno della rete aziendale come un verme informatico e installa un ransomware (come Ryuk, LockerGoga, MegaCortex ecc.) in sistemi selezionati.

Tuttavia il settore sanitario non è certamente l'unico bersaglio; il rischio riguarda le aziende di ogni ramo. Gli attacchi ransomware avvengono sia in modo mirato che casuale,[64] colpendo ad esempio i settori dell'industria, dei trasporti, della pubblica amministrazione, della comunicazione e dello sport. Recentemente il ransomware Ryuk ha preso di mira almeno cinque organizzazioni dell'industria petrolifera e del gas. In un caso gli aggressori si sono serviti del Remote Desktop Protocol (RDP) per infiltrarsi nel server *active directory* della vittima.[65] Nel secondo semestre 2019 è aumentato il numero di attacchi ransomware nei quali gli aggressori scansionano Internet alla ricerca di server *VPN* e *porte RDP* aperte nel tentativo di accedervi con attacchi *brute force*. Tale accesso viene poi utilizzato come vettore iniziale per infiltrarsi in

---

60 https://www.silicon.co.uk/security/cyberwar/french-hospital-ransomware-attack-318031

61 https://www.spiegel.de/netzwelt/web/rheinland-pfalz-und-saarland-hackerangriff-auf-krankenhaeuser-a-1277759.html

62 https://krebsonsecurity.com/2019/11/110-nursing-homes-cut-off-from-health-records-in-ransomware-attack/

63 https://krebsonsecurity.com/2019/11/ransomware-bites-400-veterinary-hospitals/

64 Cfr. Tema principale del rapporto semestrale MELANI 2019/1, n. 3.

65 https://www.darkreading.com/threat-intelligence/ryuk-ransomware-hit-multiple-oil-and-gas-facilities-ics-security-expert-says-/d/d-id/1336865

una rete aziendale. In Svizzera, ad esempio, è stato analizzato il modo in cui i malware Dharma, Phobos e Maze sfruttano gli accessi RDP aperti o non adeguatamente protetti che risultano visibili in Internet.

Una volta avvenuto il contagio, i punti deboli del protocollo RDP possono essere utilizzati per il movimento laterale all'interno del sistema. Già nell'aprile 2018 FireEye aveva individuato una campagna di distribuzione con falsi aggiornamenti per vari browser (Chrome, Internet Explorer, Opera e Firefox), che trasmettevano i malware Dridex, NetSupport Manager RAT, AZOrult o Chthonic.[66] Questo software maligno – dopo aver spiato la rete, rubato i dati di accesso e acquisito i diritti – funge da dropper per i ransomware BitPaymer e DoppelPaymer. Gli aggiornamenti sono comparsi su pagine infette, raggiunte dalle potenziali vittime ad esempio tramite redirezionamento «http://». Nel secondo semestre 2019 MELANI ha osservato a tal fine i siti web svizzeri compromessi.

Finora il modus operandi dei ransomware si basava essenzialmente sul concetto di «decifratura dei dati in cambio di denaro». Ultimamente alcuni gruppi di aggressori[67] scaricano i dati prima dell'attacco di crittografia per poi, in alcuni casi, comprovare il proprio operato attraverso la parziale pubblicazione, esercitare una maggiore pressione sulle vittime o semplicemente per estorcere loro del denaro minacciandone la pubblicazione – una sorta di alternativa qualora l'estorsione mediante crittografia dei dati vada a vuoto per l'avvenuto ripristino degli stessi.[68] Nel novembre 2019, ad esempio, il gruppo Maze ha fatto trapelare quasi 700 megabyte di dati che aveva sottratto a una società di sicurezza.[69] Lo stesso è accaduto anche ai dati di altre organizzazioni ricattate dal gruppo Maze: quelli del laboratorio di diagnosi medica MDLab, del produttore di fili e cavi Southwire e di una cittadina della Florida.[70] Il gruppo che si nasconde dietro questo ransomware è attivo anche in Svizzera.

L'attacco ransomware che diventa fuga di dati in caso di mancato pagamento del riscatto sembra essere un modello di business remunerativo e i gestori del ransomware REvil, noto anche come Sodinokibi, hanno annunciato di volerlo adottare.[71]

Alla luce di quanto precede, ogni attacco ransomware comporta il rischio di una potenziale fuga di dati, che resta tale anche dopo aver superato l'attacco: se il valore dei dati e delle informazioni lo giustifica, in futuro i criminali potrebbero comunque sfruttarli a loro vantaggio. Pertanto anche le aziende che elaborano dati personali rilevanti potrebbero finire sempre più nel mirino degli hacker.

---

66 https://www.fireeye.com/blog/threat-research/2019/10/head-fake-tackling-disruptive-ransomware-attacks.html

67 Ad esempio Maze, Sodinokibi e Doppel Paymer.

68 https://www.bleepingcomputer.com/news/security/new-megacortex-ransomware-changes-windows-passwords-threatens-to-publish-data/; https://www.bleepingcomputer.com/news/security/maze-ransomware-not-getting-paid-leaks-data-left-and-right/

69 https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/

70 https://www.bleepingcomputer.com/tag/maze/

71 https://www.bleepingcomputer.com/news/security/another-ransomware-will-now-publish-victims-data-if-not-paid/

Raccomandazioni

Le misure aziendali risultate efficaci sono le seguenti: accertatevi della completezza dei metodi di messa in sicurezza dei dati per accrescere le probabilità di poterli ripristinare totalmente dopo un attacco ransomware. Tra questi figura anche il test del processo di ripristino dei dati. Documentate la vostra infrastruttura IT, effettuate gli aggiornamenti software tempestivamente, appena sono disponibili, e mantenete sempre all'avanguardia le vostre direttive in materia di sicurezza. Realizzate dei sistemi di prevenzione e intervento, di comunicazione e di Business Continuity Management, verificandone l'efficacia con esercitazioni regolari. Per un'effettiva prevenzione dei ciberattacchi è necessario che alle misure di sicurezza tecniche si accompagni una costante sensibilizzazione dei collaboratori. Vigilare sull'attuazione di tali misure rappresenta un compito non delegabile degli organi di condotta di un'azienda.

Nessuna società è in grado di difendersi da qualsivoglia ciberattacco in modo sicuro. Migliorate quindi le capacità di reazione e resistenza per attenuare gli effetti di un attacco non scongiurabile.


Nel secondo semestre 2019 MELANI ha pubblicato le misure di sicurezza aggiornate su come proteggersi dai nuovi metodi usati per attacchi ransomware:

https://www.melani.admin.ch/melani/it/home/dokumentation/newsletter/update-ransomware-neue-vorgehensweise.html

Attenzione: in caso di infezioni a più fasi non è sufficiente ripristinare i dati tramite backup! È necessaria una pulizia della rete ed è consigliabile una nuova installazione del sistema per eliminare con certezza anche il dropper.

### 4.6.2 Emotet resta la più grande minaccia di infezione

Anche nel secondo semestre 2019 Emotet è stato molto attivo in Svizzera. Dopo un lieve calo a giugno, nel mese di agosto il gruppo è tornato a colpire con grande virulenza, tramite numerose attività di diffusione che hanno fatto vittime altrettanto numerose.

Analogo il modus operandi anche in questo semestre: il trojan preleva i contenuti da precedenti conversazioni e-mail e li utilizza per generare nuovi messaggi che poi invia ai destinatari presenti nelle liste di distribuzione. Le e-mail includono un allegato nocivo, spesso un documento Word che contiene una macro. Appena la vittima apre il documento e attiva la modalità di revisione, il malware si esegue. In assenza di misure di protezione aggiuntive, Emotet carica altri moduli creando una situazione di persistenza nel computer della vittima.[72]

Il gruppo ha perfezionato il proprio modus operandi e rivende accessi a reti e sistemi ad altri attori. Emotet è quindi diventato un protagonista della cibercriminalità organizzata. Nel mercato nero si aggirano persino gruppi parastatali interessati all'acquisto di accessi a sistemi compromessi da poter utilizzare a fini di spionaggio o a scopo di lucro.

[72] Cfr. Rapporto semestrale MELANI 2019/1, n. 3.4.1 e 4.6 nonché il relativo allegato tecnico.

Raccomandazioni

Occorre prudenza non solo con le e-mail di persone sconosciute, ma anche nei confronti di mittenti a noi noti. Diffidate anche da e-mail inattese che facciano riferimento a una vecchia conversazione. I criminali spesso usurpano l'identità di aziende particolarmente degne di fiducia per inviare delle e-mail falsificando l'indirizzo di provenienza. In caso di dubbio richiedete al presunto mittente tramite una modalità di contatto già nota, o ad esempio indicata sul suo sito web, di cosa si tratta esattamente e se ha realmente inviato quell'e-mail.

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


Le aziende dovrebbero attuare misure di difesa perimetrale bloccando i siti web che vengono utilizzati attivamente per la diffusione di Emotet, ad esempio nel web proxy o a livello di server DNS. Un elenco di tali siti web che trasmettono Emotet è disponibile ad esempio all'indirizzo abuse.ch.

## 4.7 Vulnerabilità

Eventuali errori nello sviluppo del software generano delle vulnerabilità. Ecco perché «life-cycle management» e «patch management» sono essenziali. Ogni singola azienda (sia essa una PMI o un gruppo industriale) deve tenere un inventario di tutti i suoi sistemi e le sue applicazioni e stabilire con un piano cosa e quando deve essere provvisto di patch, nonché quali software raggiungono in un dato momento la fine del proprio ciclo di vita. Questo vale anche per le componenti come firmware o management board. Nello sviluppo software bisognerebbe inoltre prestare attenzione alla vulnerabilità dei *framework* utilizzati e delle rispettive dipendenze.

Particolare criticità presentano le lacune che possono essere sfruttate da remoto attraverso la rete e senza autenticazione, come ad es. le lacune in *SMB* (EternalBlue[73]), *RDP* (BlueKeep[74], BlueGate[75, 76]), in Citrix Netscaler[77] e Oracle Weblogic[78]. Fintanto che una lacuna non è nota («0-day exploit»), ha un valore elevato e il più delle volte viene utilizzata solo per attacchi mirati. Appena diventa nota e sono disponibili dei patch, questi ultimi vengono analizzati e così si identifica la lacuna ancora aperta nei sistemi sprovvisti di patch. Con questa informazione vengono poi scritti i «codici exploit». Appena un «codice exploit» è di dominio pubblico, finisce nelle cassette degli attrezzi della maggior parte dei criminali e/o attori statali e la frequenza d'uso aumenta di conseguenza. Al più tardi a questo punto i sistemi raggiungibili dall'esterno e che contengono delle lacune sono da considerarsi compromessi. Le applicazioni web e *CMS*

73 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144
74 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708
75 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0610
76 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0609
77 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19781
78 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2546

con i rispettivi *plugin* vengono attaccate piuttosto spesso e necessitano di adeguate misure di sicurezza (cfr. anche «Misure per contribuire alla sicurezza dei sistemi di gestione dei contenuti», CMS[79]). Mentre il patching di tradizionali sistemi e applicazioni IT è relativamente semplice, nel quadro di sistemi di gestione, dispositivi IoT o dotazioni mediche esso si rivela molto più complesso. Nel settembre 2019 è stata individuata una lacuna in VxWorks, un sistema operativo in tempo reale, spesso utilizzato nei processi di gestione o anche nelle apparecchiature mediche, che espone a rischi una molteplicità di dispositivi[80] per certi versi molto complessi da aggiornare.

Sfruttare le lacune può avere diverse finalità:

1. furto di dati per spionaggio industriale o a scopo di estorsione;
2. distribuzione di ransomware;
3. acquisizione di un sistema per effettuare del mining di criptovalute;
4. invio di malware o spam;
5. punto d'attacco per ulteriori attività di penetrazione nella rete.

Raccomandazioni

Per disporre di un grado di sicurezza costante un'azienda ha bisogno di un buon «life-cycle management» e «patch management» per tutte le componenti utilizzate. Ciò riguarda non solo i tradizionali sistemi di automazione d'ufficio, ma anche le applicazioni web, i dispositivi mobili, i dispositivi IoT e i componenti di gestione. In quest'ottica è opportuno prestare attenzione anche ai framework e alle librerie software utilizzate.

In caso di vulnerabilità critiche che non vengono risolte subito, è auspicabile adottare delle soluzioni di sostituzione (ad es. un secondo browser) oppure la possibilità di isolare o rimuovere temporaneamente la lacuna (ad es. impiegando un web application firewall in caso di applicazioni web).

Le soluzioni *remote access* come *PN gateway*, *web application gateway*, accesso web all'e-mail o Servizi Terminal esposti sono fra gli obiettivi più interessanti per gli aggressori perché consentono l'accesso diretto alle risorse interne. Oltre al life-cycle management e al patch management, tali risorse richiedono in ogni caso misure di sicurezza aggiuntive, come ad es. autenticazione a due fattori, *hardening* e ricostruzione centralizzata degli eventi informatici.

Anche chi sviluppa autonomamente applicazioni, sistemi, strumenti di gestione o dispositivi IoT ha bisogno di un life-cycle management e patch management chiaro nonché dei corrispondenti canali di informazione verso i clienti. È inoltre importante mettere a disposizione un canale di contatto facile da trovare, attraverso il quale segnalare le lacune a livello di *security researcher*. Un programma *«bug bounty»* costituisce un'integrazione che vale la pena testare e che può servire alla segnalazione tempestiva delle lacune e alla loro eliminazione in modo coordinato.

79 https://www.melani.admin.ch/melani/it/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-content-management-systemen--cms-.html

80 https://go.armis.com/urgent11

## 4.8 Misure preventive

### 4.8.1 Nuovi standard minimi nell'approvvigionamento di generi alimentari

Alla luce della crescente dipendenza dei processi produttivi e delle procedure operative dalle tecnologie di informazione e comunicazione TIC, negli ultimi mesi l'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) ha pubblicato per diversi settori degli standard minimi per la sicurezza delle TIC. In caso di guasti sistemici sono a rischio l'operatività delle aziende e la fornitura di beni e servizi critici in Svizzera. Per proteggersi dai rischi associati alle TIC e garantire la filiera alimentare, l'UFAE ha recentemente pubblicato uno standard minimo per la sicurezza TIC nell'approvvigionamento di derrate alimentari teso ad aiutare le aziende del settore a evitare malfunzionamenti delle TIC o a porvi rimedio con rapidità.

Questa raccomandazione si aggiunge allo standard minimo per la sicurezza TIC nell'approvvigionamento idrico e al manuale per la protezione di base della «Operational Technology» nell'approvvigionamento elettrico («Handbuch für den Grundschutz von "Operational Technology" in der Stromversorgung») precedentemente pubblicati. Tali standard di settore vengono integrati con lo standard minimo TIC generale, frutto delle analisi di vulnerabilità ai ciber-rischi condotte nei vari settori fondamentali per il funzionamento del Paese. Le analisi di vulnerabilità sono state condotte dall'UFAE nell'ambito della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC).[81]

### 4.8.2 La polizia svizzera blocca gli shop online fittizi

Acquistare in Internet è comodo, ma non privo di pericoli. Gli acquirenti corrono infatti il rischio di non vedersi recapitare a casa gli articoli apparentemente acquistati o di ricevere prodotti diversi da questi ultimi. Oltre al furto, c'è il rischio che i dati comunicati vengano utilizzati per commettere altri reati.

Gli shop online fittizi hanno travolto anche la Svizzera, dove la cibercriminalità registra siti fraudolenti che sfruttano l'estensione «.ch». In certi periodi dell'anno, ad esempio prima di Natale, questo genere di attività cresce in modo esponenziale.

Il reparto della polizia cantonale di Zurigo che si occupa di cibercriminalità combatte attivamente questo fenomeno in collaborazione con SWITCH(l'organismo di registrazione svizzero che gestisce tutti i nomi a dominio con estensione «.ch»). Nel dicembre 2019 tale collaborazione è sfociata nel blocco di 450 shop online fittizi poco dopo la loro attivazione. Dall'inizio del 2018 la polizia cantonale di Zurigo ha identificato e chiuso complessivamente 6500 shop online di questo tipo.

Questa misura ha non solo ridotto il numero di shop online fittizi, ma ha anche causato una drastica flessione dei nuovi shop online fraudolenti con nomi di dominio svizzeri. È quanto conferma la polizia cantonale nel suo sito web.[82] Il reparto cibercriminalità spiega inoltre nel sito a quali aspetti bisogna prestare attenzione per evitare tali situazioni. Tra questi cita segnatamente i nomi di dominio che non hanno nulla a che vedere con i prodotti

---

81 https://www.admin.ch/gov/it/start/dokumentation/medienmitteilungen.msg-id-75891.html

82 https://www.kapo.zh.ch/internet/sicherheitsdirektion/kapo/de/aktuell/medienmitteilungen/2019_12/1912161f.html

offerti, l'assenza del simbolo del lucchetto, che indica una connessione crittografata al sito web, e la mancanza del colophon previsto dalla legge.[83]

### 4.8.3 Un'operazione internazionale distrugge l'infrastruttura di un «RAT as a service»

MELANI ha ripetutamente richiamato l'attenzione sulla pratica ormai largamente diffusa di offrire ciberattacchi o strumenti per realizzarli.[84] Perseguire tali reati è tutt'altro che semplice. Alla difficoltà di identificare un cibercriminale si aggiunge un ulteriore ostacolo: il confine tra legalità e illegalità è sottile e non sempre inequivocabile. Questo può spiegare come sia stato possibile che fin dal 2012 lo sviluppatore di software Shockwave™ potesse vendere online indisturbato Imminent Monitor, uno strumento di accesso remoto («remote administration tool», RAT), prima che nel novembre 2019 l'infrastruttura venisse smantellata nel quadro di un'operazione internazionale che ha visto impegnate diverse autorità di perseguimento penale.

Nel sito web tramite il quale vendeva il suo prodotto, l'autore ha preso le distanze dalle persone che volevano utilizzarlo a fini illegali, respingendo qualsiasi responsabilità. Al momento dell'acquisto era necessario rilasciare una dichiarazione, nella quale si affermava di non utilizzare il servizio per la distribuzione di malware. Malgrado ciò il prodotto disponeva di una serie di funzioni, di per sé atipiche e superflue per uno strumento di accesso remoto legale. Esso permetteva ad esempio di disabilitare software antivirus, aveva delle caratteristiche che ne complicavano il rilevamento, offriva una connessione al desktop remoto, all'insaputa della vittima ed consentiva perfino di eseguire un miner di criptovalute sul computer di quest'ultima.

Il prodotto di base, dal costo di appena 25 dollari, era accessibile a chiunque. Secondo le autorità questo articolo è stato effettivamente acquistato da oltre 14 500 soggetti criminali, che lo hanno utilizzato in 124 Paesi a danno di decine di migliaia di vittime.

L'operazione è stata condotta dalla polizia federale australiana (AFP), dall'Europol, dall'Eurojust, dall'FBI e da molte altre autorità penali e di polizia ed è sfociata nel sequestro di 430 dispositivi nonché nell'arresto di 13 utenti che utilizzavano il prodotto illegalmente.[85]

### 4.8.4 Bug Bounty: a caccia di bug in Internet

Nell'intento di incentivare gli hacker e offrire loro la possibilità di segnalare i punti deboli individuati, in passato si sono diffusi sempre più programmi cosiddetti «*bug bounty*». Si tratta in particolare di piattaforme che assegnano dei premi per le vulnerabilità verificabili. Esistono vari modelli di programmi bug bounty. Le piattaforme commerciali svolgono un'attività di mediazione tra hacker e impresa, definendo le regole per entrambe le parti. Alcune piattaforme adottano anche un approccio non commerciale: normalmente sono gratuite e basate su community, ma tra le parti non sussiste alcuna intermediazione istituzionalizzata. Tali progetti offrono

---

83 https://www.cybercrimepolice.ch/de/fall/betruegerische-internetshops-vorsicht-bei-der-online-schnaeppchenjagd/

84 Rapporti semestrali MELANI 2009/2, n. 4.7; 2016/2, n. 6.1, e 2019/1, n. 3.3.

85 https://securityaffairs.co/wordpress/94525/cyber-crime/imminent-monitor-rat-shutdown.html
https://unit42.paloaltonetworks.com/imminent-monitor-a-rat-down-under/

agli esperti di sicurezza una piattaforma per segnalare vulnerabilità in qualsiasi sito web. Per quanto concerne le imprese, esse hanno la possibilità di avviare un programma bug bounty per i nuovi software da introdurre, quindi solo a livello estemporaneo, oppure di introdurre un programma bug bounty permanente. In quest'ottica è possibile avvalersi dei servizi di un fornitore commerciale oppure realizzare un programma «bug bounty» interno all'azienda. Anche alcuni Stati[86] hanno elaborato delle regole per gestire le vulnerabilità.

Da anni si dibatte su come gli hacker dovrebbero comportarsi quando individuano delle lacune, per aiutare la collettività e non danneggiare le imprese. Al momento si sono affermati due approcci: «full disclosure» e «responsible disclosure». Con la «full disclosure» («pubblicazione integrale») l'hacker informa allo stesso tempo l'azienda e la collettività. L'azienda viene quindi messa sotto pressione, perché nel momento in cui la lacuna è di dominio pubblico, chiunque può approfittarne. Questo è anche il punto critico di tale approccio. Con la «responsible disclosure» («divulgazione responsabile») l'hacker informa inizialmente solo l'azienda, che così ha il tempo (di solito 60–120 giorni) di risolvere il problema. Solo dopo l'hacker renderà nota la lacuna.[87]

In linea di principio per la partecipazione ai programmi «bug bounty» si applica il criterio della «responsible disclosure», che consiste nei seguenti elementi:

1. l'azienda ha abbastanza tempo (di solito 60–120 giorni) per verificare le vulnerabilità e porvi rimedio;
2. le vulnerabilità non devono essere comunicate a terzi;
3. i test concernenti le vulnerabilità non devono compromettere servizi, prodotti e la normale attività dell'azienda;
4. i dati non possono essere spiati né ceduti;
5. le rivendicazione (soprattutto di carattere finanziario) legate alla segnalazione di una vulnerabilità non vengono prese in considerazione.

In futuro questa prassi sarà utilizzata sempre più frequentemente dalle imprese, cosicché per quanto riguarda Internet l'avvenire dei cacciatori di bug qualificati e dei ricercatori in materia di sicurezza appare roseo.[88] Le cifre relative ai programmi «bug bounty» esistenti, come quello di Swisscom, sono impressionanti: l'azienda di telecomunicazioni ha ricevuto ed elaborato 844 rapporti di vulnerabilità. Di questi, 427 si sono tradotti in una correzione e Swisscom ha corrisposto premi per un ammontare di 350 000 franchi svizzeri. La tipologia di vulnerabilità segnalate va da *low-level cross site scripting* (XSS) fino a *0-days* altamente critici in prodotti noti e molto diffusi.[89]

---

86 I Paesi Bassi sono fra questi: https://www.government.nl/topics/cybercrime/fighting-cybercrime-in-the-netherlands/responsible-disclosure

87 https://www.zeit.de/digital/datenschutz/2013-09/bug-bounty-hack/seite-2

88 https://www.swisscyberstorm.com/2019/11/26/some-background-on-switzerlands-biggest-bug-bounty-program/

89 Cifre a partire dal 2018, https://www.swisscyberstorm.com/2019/11/26/some-background-on-switzerlands-biggest-bug-bounty-program/

Recentemente gli hacktivisti hanno lanciato una nuova forma di programma «bug bounty» per ricompensare gli hacker inclini alla giustizia privata e quelli che svolgono attività di hackeraggio e divulgazione non autorizzata di dati in nome del pubblico interesse. Questa nuova forma ha soltanto il nome in comune con i programmi tradizionali, che rendono un importante contributo alla sicurezza, identificano le lacune presenti nei sistemi di sicurezza e le eliminano prima che possano essere sfruttate.

Il Centro nazionale per la cibersicurezza (NCSC) sta elaborando una «responsible disclosure policy» per la Svizzera.


Eventuali informazioni sulle vulnerabilità possono essere fornite sin d'ora all'indirizzo incidents@ncsc.ch.

# 5 Ricerca e sviluppo

## 5.1 Quando non funziona più niente: ransomware e adesso?

Nei suoi rapporti semestrali MELANI ha già più volte riferito il modus operandi dei gruppi criminali volto a estorcere denaro a fronte di dati crittografati.[90] Nel sito web MELANI sono disponibili i relativi documenti tecnici di riferimento su come tutelarsi da questi attacchi ransomware.[91]

Neanche i migliori provvedimenti tecnici proteggono però integralmente da un'infezione. Nel 2019 abbiamo assistito a una professionalizzazione che ha riguardato soprattutto i gruppi dediti al modello di business «ransomware». Ora non ci si limita più a crittografare i dati disponibili localmente e mediante accesso alla rete resi accessibili dalla vittima con l'apertura incauta di una presunta fattura telefonica o di un dossier di candidatura, giunti per e-mail. Infatti, sempre più spesso, dopo una prima infezione gli aggressori si prendono il tempo per spostarsi grazie ad un *trojan* all'interno della rete della vittima, nell'intento di procurarsi l'accesso a tutti i sistemi e i punti nevralgici, compresi i backup online. Ciò garantisce la massimizzazione del danno nel momento in cui il vero e proprio software di crittografia colpirà.

Per quanto concerne la sicurezza TIC, questa procedura a più livelli permette da un lato di scoprire gli aggressori, in determinate circostanze, e di difendersi prima che si verifichi un danno maggiore. MELANI viene costantemente informata dalle aziende di sicurezza e dalle organizzazioni partner sulle infezioni delle reti aziendali e inoltra tali informazioni ai gestori di rete coinvolti. Per altri versi la procedura a più livelli ha conseguenze disastrose qualora gli aggressori riuscissero ad inserire il ransomware e, oltre ai sistemi nevralgici, bloccassero le unità produttive estere della ditta, perché collegate tecnicamente alla rete attraverso la centrale aziendale.

---

90 Rapporti semestrali MELANI 2011/2, cap. 3.5; 2013/2, cap. 3.1; 2014/2, cap. 3.6 e 5.3; 2015/1, cap. 4.6.1.5; 2015/2, cap. 4.5.1; 2016/1, cap. 4.6.3 e 5.4.3; 2016/2, cap. 6.1; 2017/1, cap. 3; 2017/2, cap. 5.4.2; 2018/2, cap. 4.5.4 e 5.3.5 nonché 2019/1, cap. 3.

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

### 5.1.1 Il successo dei ransomware non è solo un problema TIC

Il modello di business dei gruppi di ransomware consiste nell'esercitare la maggiore pressione possibile sulle aziende e sulle organizzazioni colpite, così che esse prendano in considerazione le loro richieste di pagamento. Di conseguenza tali gruppi mirano all'arresto dei processi aziendali basati sulle TIC. Anche se in quest'ottica la fonte del problema è l'informatica, essa non è in grado di fornire una soluzione rapida al problema: ripristinare i processi e gli iter aziendali più critici e attivare un *business continuity plan* possibilmente elaborato in precedenza dal management.

Dopo un attacco ransomware riuscito occorre individuare più in fretta possibile i sistemi e processi che non sono stati colpiti dall'attacco e quelli che possono funzionare anche senza l'ausilio delle TIC.

In questi casi è necessario coinvolgere fin dall'inizio dei giuristi, visto che gli aggressori hanno avuto accesso ai dati, anche se solo per poco tempo. Trovano pertanto applicazione le prescrizioni della legge sulla protezione dei dati nonché quelle del regolamento generale sulla protezione dei dati (RGPD), qualora l'impresa operi anche all'interno dell'UE. Subito dopo occorre stabilire cosa sia sostanzialmente possibile ripristinare dei sistemi TIC sulla base dei backup e degli snapshot ancora disponibili. A tale scopo è auspicabile coinvolgere un fornitore esterno di servizi di sicurezza TIC che, grazie alla sua esperienza nei casi di ransomware, sarà in grado di stimare con una certa efficienza la reale estensione e le opzioni di intervento disponibili.

Una volta che queste due prime fasi avranno fornito le informazioni cercate, il terzo passo da compiere a livello di management sarà decidere, a dipendenza dell'entità del danno subito e dei relativi costi, se sia necessario scendere a patti con le richieste dei gruppi criminali. MELANI sconsiglia vivamente di pagare un riscatto, perché così facendo si avvalora il modello di business del gruppo di ransomware e lo si sostiene finanziariamente. Non si può credere cheL'importante è che le imprese colpite si mettano immediatamente in contatto con la polizia cantonale, che sporgano denuncia e che insieme discutano come procedere.

### 5.1.2 Azione penale: oltre l'arresto

La gestione di un incidente conduce dopo aver attuato i necessari provvedimenti immediati interni a una quarta fase, spesso sottovalutata ma imprescindibile, indipendentemente dall'intenzione della vittima di pagare o meno: il ricorso all'azione penale.

Di norma le aziende si guardano dall'avviare un'azione penale nei casi di ransomware. È opinione comune che la polizia non possa fare niente contro i gruppi di cibercriminali stranieri. Mentre in realtà le autorità di perseguimento penale hanno esperienza in quest'ambito e indagano a livello internazionale sui gruppi responsabili. Se pure un'azienda si decidesse a pagare il riscatto, la polizia dispone di collaboratori addestrati a mettersi in contatto con gli autori del reato.

Rivolgersi alle autorità di perseguimento penale è quindi vantaggioso sotto vari punti di vista; esse possono ad esempio raccogliere mezzi di prova non solo per elaborare il caso in questione, ma anche per corroborare procedimenti già avviati per altri casi e incrociando le indagini. Possono inoltre fungere da vero e proprio centro di competenza per la gestione dei casi di ransomware o limitarsi ad offrire un affiancamento a titolo di consulenza o ancora, in base

al gruppo di ransomware, mettere a disposizione delle conoscenze utili ai collaboratori o ai fornitori di prestazioni esterni responsabili del ripristino.

### 5.1.3 Un piano B come BCM

Nel 2019 le aziende svizzera sono state particolarmente colpite da attacchi ransomware. Questi attacchi sono frutto di una logica elementare: chi non può produrre è disposto a pagare un cospicuo riscatto per non rischiare interruzioni dell'attività aziendale per giorni e giorni. Il che è comprensibile. Anche il solo effetto iniziale della notizia, secondo la quale tutto è fermo a causa di un attacco ransomware, è stato descritto da un imprenditore come una «*near death experience*».

Il ransomware attacca la disponibilità di processi e in questo senso si differenzia solo marginalmente dagli attacchi contro la disponibilità dei webshop (attacchi DDoS). I criminali sperano di interrompere le attività di dell'azienda colpita e che questa acconsenta a pagare il riscatto per poterle riprendere. Ecco perché questi attacchi mirano proprio a mettere fuori uso innanzitutto le TIC e di conseguenza si accaniscono contro imprese fortemente dipendenti dall'informatica.

Uno dei compiti della direzione generale di qualsiasi azienda e organizzazione consiste nel far sì che in caso di necessità i processi aziendali critici possano funzionare indipendentemente dalla divisione TIC. Il cosiddetto Business Continuity Management (BCM) deve assolutamente essere definito prima di un ciberattacco.

## 5.2 L'escalation dei conflitti in Medio Oriente minaccia anche i partner commerciali in Svizzera

Le organizzazioni che intrattengono relazioni d'affari con il Medio Oriente rischiano di diventare il trampolino di lancio per attacchi contro obiettivi collegati ai conflitti in corso da anni.

Oltre ai conflitti noti in Siria e nello Yemen, il Medio Oriente è da tempo una regione a rischio anche dal punto di vista della sicurezza delle informazioni. Pertanto il regime di vigilanza dei governi regionali è per certi versi più severo di quanto accada nella maggior parte degli Stati europei. Lo scorso anno Reuters[92] ha riferito circa il Project Raven, nell'ambito del quale i veterani dei servizi di intelligence americani avrebbero aiutato gli Emirati Arabi Uniti nello sviluppo di capacità informatiche difensive. Secondo l'agenzia di stampa, Project Raven è stato successivamente migrato all'interno dell'azienda DarkMatter. Nel Regno dell'Arabia Saudita ha fatto notizia l'uso di software governativi o GovWare alla vigilia dell'assassinio del giornalista Khashoggi[93] e presumibilmente contro Jeff Bezos, fondatore di Amazon e proprietario del Washington Post.[94] Diversa è stata la risposta delle forze armate israeliane, che hanno sferrato

92 https://www.reuters.com/investigates/special-report/usa-spying-raven/

93 https://citizenlab.ca/2019/04/dubious-denials-scripted-spin-spyware-company-nso-group-goes-on-60-minutes/

94 https://techcrunch.com/2020/01/22/bezos-nso-group-hack/

un attacco aereo contro l'edificio dal quale il gruppo palestinese Hamas lanciava attacchi informatici contro di loro, stando al comunicato israeliano.[95]

Sulla scia di questo scenario complesso, i governi coinvolti e le aziende private, in particolare i gestori di infrastrutture critiche, hanno costantemente investito nel proprio assetto per la sicurezza delle informazioni. Queste organizzazioni robuste rappresentano un obiettivo sempre più difficile da espugnare, ragion per cui gli aggressori hanno iniziato a cercare occasioni lungo la filiera di fornitura in Europa[96, 97] e nell'America del Nord[98]. Oltre ai fornitori del settore industriale,[99] anche i prestatori di servizi nel campo delle TIC in particolare rappresentano un valido obiettivo intermedio,[100] per poi sferrare l'attacco vero e proprio contro le istituzioni nemiche.

Visto che nel prossimo futuro non si intravede alcuna tregua in Medio Oriente, le organizzazioni elvetiche che hanno relazioni nella regione dovrebbero confrontarsi con il rischio di un attacco informatico proveniente da quelle aree. A tal fine non ha alcuna importanza se si finisce nel mirino degli aggressori in qualità di fornitore, prestatore di servizi o solo come partner commerciale di un'organizzazione, che ha un qualsivoglia legame con le regioni del conflitto. Raggruppamenti come APT33[101], Oilrig[102], Muddywater[103], Leafminer[104], APT39/Chafer[105] ecc. non si risparmiano pur di procurarsi un varco di entrata per le proprie operazioni.

Le descrizioni dei raggruppamenti, disponibili nel catalogo MITRE ATT&CK[106] sui metodi e sulle tecniche degli aggressori, contengono sia i metodi di attacco utilizzati sia le misure di mitigazione opportune. Una corretta implementazione e un'applicazione coerente dell'autenticazione a più fattori previene molti attacchi di questo genere o quanto meno li complica considerevolmente.

## 5.3 Nuovi modelli di business per riciclare in modo sempre più efficace

La cibercriminalità è un tipico esempio di «work sharing» avanzato: ogni singola tipologia di attacco informatico può essere vista come una successione di mansioni ben definite, nelle quali spesso si sono specializzati determinati soggetti che ambiscono a essere sempre più efficaci, contribuendo così alla produttività del fenomeno. Tra queste diverse mansioni specifiche, occupa un posto speciale il riciclaggio di denaro frutto di attività illegali. Di fatto l'intera rete criminale non servirebbe a nulla se alla fine il denaro non potesse essere ripulito per

95 https://www.zdnet.com/article/in-a-first-israel-responds-to-hamas-hackers-with-an-air-strike/
96 Rapporto semestrale MELANI 2018/2, cap. 5.2.2
97 https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/shamoon-attackers-employ-new-tool-kit-to-wipe-infected-systems/
98 https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage
99 https://www.wired.com/story/iran-apt33-industrial-control-systems/
100 https://www.symantec.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain
101 https://attack.mitre.org/groups/G0064/
102 https://attack.mitre.org/groups/G0049/
103 https://attack.mitre.org/groups/G0021/
104 https://attack.mitre.org/groups/G0077/
105 https://attack.mitre.org/groups/G0087/
106 https://attack.mitre.org/

essere utilizzato sul mercato legale. Si tratta di un'attività fiorente: secondo uno studio pubblicato da Bromium nel 2018, ogni anno vengono riciclati dalle organizzazioni criminali dagli 80 ai 200 miliardi di dollari.[107]

Lo sviluppo di valute virtuali ha rivoluzionato le transazioni derivanti da attività criminali. Oggi numerose attività criminali online sono finanziate con valute virtuali come i bitcoin. Ciò permette ai pirati informatici, nonostante le transizioni siano documentate, di cancellarne le tracce attraverso la tecnologia *blockchain*, ad esempio utilizzando dei «mixer / tumbler».[108] Eppure i proventi di alcune attività cibercriminali si materializzano tuttora sotto forma di valute tradizionali. È il caso, ad esempio, delle infezioni con trojan e-banking o dei pagamenti con carte di credito rubate. Per tale tipo di operazioni occorrono attività di riciclaggio tradizionali. Già da tempo è stato documentato che i privati vengono ingaggiati per mettere a disposizione i propri conti bancari per ricevere denaro e incassare una provvigione per il trasferimento a un altro conto. I privati così reclutati sono detti «money mule» o «agenti finanziari». Fedeli al loro approccio opportunistico, i criminali tentano anche di approfittare delle piattaforme esistenti. Tra i sistemi noti di riciclaggio figurano ad esempio i micropagamenti tramite PayPal o gli acquisti eBay a prezzi esorbitanti.

Attualmente il successo di piattaforme come AirBnB o Uber ha suscitato l'interesse dei criminali. Grazie all'impiego delle nuove tecnologie, tali piattaforme permettono a un fornitore di servizi di entrare in contatto direttamente con i propri clienti. Un classico esempio di questi nuovi metodi di riciclaggio di denaro sono le «corse fantasma» di Uber. I criminali reclutano autisti di Uber, disposti a non sottilizzare e desiderosi di arrotondare il salario mensile. A tale scopo vengono pubblicati degli annunci nei forum underground. Il criminale ordina una corsa e paga quindi all'autista nella forma prescritta. Questa corsa però è fittizia e l'autista può restare tranquillamente nella propria abitazione, per poi restituire il denaro al criminale trattenendo una percentuale a titolo di ricompensa. Un modello molto simile è stato osservato su AirBnB, la piattaforma per sublocazioni del settore immobiliare. Anche in questo caso il criminale effettua il pagamento per un appartamento che non occuperà e il locatore gli restituisce il denaro al netto di una provvigione.

L'obiettivo della lotta alla cibercriminalità è interrompere una catena di attività altamente redditizie, attaccando una delle maglie che la compongono. Questi metodi di riciclaggio sono pertanto costantemente nel mirino delle azioni di polizia. Nel dicembre 2019, ad esempio, l'Europol ha reso noto che un'operazione alla quale partecipavano 31 Paesi, aveva portato all'arresto di 228 reclutatori di money mule.[109] Già nel mese di maggio queste stesse autorità, in collaborazione con quelle di Lussemburgo e Paesi Bassi, avevano comunicato di aver sequestrato Bestmixer.io, un servizio che ha permesso di riciclare circa 200 milioni di dollari in un anno[110]. Come mostrano gli abusi a danno di piattaforme come Uber e Airbnb, ai criminali non

---

107 https://www.bromium.com/press-release/up-to-200-billion-in-illegal-cybercrime-profits-is-laundered-each-year-comprehensive-research-study-reveals/

108 Servizio che consente di occultare le transazioni di somme considerevoli in criptovalute, introducendoli segretamente attraverso singoli wallet molto attivi e frammentandoli in tante transazioni di piccola entità.

109 https://www.europol.europa.eu/newsroom/news/228-arrests-and-over-3800-money-mules-identified-in-global-action-against-money-laundering

110 https://www.europol.europa.eu/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down

mancano idee e competenze su come diversificare i modelli per il riciclaggio di denaro. Oltre al lavoro della polizia e alle misure di sensibilizzazione dei potenziali money mule, una parte della soluzione è indubbiamente nelle misure che sono state introdotte dai servizi online oggetto di abusi e nella loro capacità di individuare l'uso illegittimo dei servizi a scopo di riciclaggio.

# 6 Prodotti MELANI pubblicati

## 6.1 Blog GovCERT.ch

### 6.1.1 Trickbot: un'analisi dei dati raccolti dalla botnet

Nel corso delle attività di monitoraggio di varie minacce, negli ultimi anni abbiamo raccolto molti dati sulla botnet Trickbot. Questo documento si basa su un'analisi di aspetti selezionati della nostra raccolta di dati Trickbot. L'analisi si articola in due tronconi principali. Nel primo ci concentriamo sulla marca temporale PE dei dropper Trickbot (ossia i file binari distribuiti dagli operatori Trickbot) e dei rispettivi blocchi informativi (ossia i file binari PE spacchettati e quindi eseguiti dopo l'esecuzione di un dropper). L'analisi si basa su una raccolta di circa 2100 dropper e relativi blocchi informativi raccolti tra luglio 2016 e febbraio 2019.

https://www.govcert.admin.ch/blog/37/trickbot-an-analysis-of-data-collected-from-the-botnet (in inglese)

## 6.2 Bollettino d'informazione MELANI

### 6.2.1 Aggiornamento ransomware: nuova procedura

30.07.2019 – Nelle settimane passate le imprese svizzere sono state bersaglio di un nuovo tipo d'attacco, con cui aggressori sconosciuti hanno infiltrato con successo reti aziendali e cifrato ampiamente i loro dati per mezzo di ransomware. Sono state colpite dagli attacchi anche diverse aziende svizzere famose.

https://www.melani.admin.ch/melani/it/home/dokumentation/newsletter/update-ransomware-neue-vorgehensweise.html

### 6.2.2 Microsoft sospende il supporto per i prodotti meno recenti: pericoli in agguato

16.12.2019 – Microsoft ha annunciato che il 14 gennaio 2020 sospenderà il supporto e gli aggiornamenti per diversi prodotti non più recenti, ovvero il sistema operativo «Windows 7», «Windows Server 2008» e «Windows Server 2008 R2».

https://www.melani.admin.ch/melani/it/home/dokumentation/newsletter/microsoft-end-of-life.html

# 7 Glossario

| Termine | Descrizione |
|---|---|
| Agente finanziario | È un agente finanziario chiunque svolga legalmente l'attività di intermediario finanziario e quindi anche operazioni di trasferimento di denaro. In tempi recenti questo concetto è utilizzato nel contesto delle transazioni finanziarie illegali. |
| Advanced Persistent Threat (APT) | Questa modalità di attacco prevede l'uso di diverse tecniche e tattiche. Si tratta inoltre di attacchi estremamente mirati contro una singola organizzazione o un Paese. Il più delle volte essi possono provocare danni ingenti. Ecco perché l'aggressore è disposto a investirvi molto tempo, denaro e conoscenze e a tal fine dispone generalmente di notevoli risorse. |
| App | Il concetto di app (dall'abbreviazione inglese di «application») indica in generale ogni forma di programmi di applicazione. Nell'uso linguistico si fa nel frattempo perlopiù riferimento alle applicazioni per i moderni smartphone e computer tablet. |
| Attacchi Supply Chain | Attacco con cui si cerca di infettare l'obiettivo finale infettando precedentemente un'azienda nella catena di fornitura. |
| Attacchi Watering Hole | Infezione mirata per mezzo di software maligno tramite siti che di preferenza vengono visitati solamente da un gruppo specifico di utenti. |
| Attacco DDoS | Attacco di Distributed-Denial-of-Service. Un attacco DoS in cui la vittima è attaccata simultaneamente da numerosi sistemi diversi. |
| Autenticazione a due fattori | L'autenticazione a due fattori è impiegata per accrescere la sicurezza. A tal fine sono necessari almeno due dei tre fattori di autenticazione: 1. una cosa che si conosce (ad es. password, PIN ecc.); 2. una cosa che si ha (ad es. certificato, token, elenco da cancellare ecc.); 3. una cosa che si è (ad es. impronte digitali, scanner della retina, riconoscimento vocale ecc.). |
| Backdoor | Backdoor (in italiano: porta posteriore) designa una parte del software che consente agli utenti di accedere al computer eludendo le normali protezioni di accesso oppure un'altra funzione altrimenti protetta di un programma per computer. |
| BGP<br><br>Border Gateway Protocol | Protocollo di istradamento o «routing» utilizzato in Internet che determina il percorso dei pacchetti dati tra le reti. |

| Termine | Descrizione |
|---|---|
| Bitcoin | Sistema di pagamento decentrato che può essere utilizzato in tutto il mondo e nome di un'unità di moneta digitale. |
| Bot | Trae origine dalla parola slava per lavoro (robota). Designa un programma che esegue autonomamente una determinata azione alla ricezione di un comando. I cosiddetti malicious bot possono pilotare a distanza i computer compromessi e indurli a eseguire qualsiasi azione. |
| Botnet | Una rete costituita da più bot, pilotata tramite un'infrastruttura del tipo «command and control». |
| Brute Force | Metodo di risoluzione di problemi nei settori dell'informatica, della crittografia e della teoria dei giochi, fondato sulla sperimentazione di tutti i casi possibili. |
| C2<br>Command & Control | Infrastruttura di comando e controllo delle botnet. La maggior parte dei bot può essere sorvegliata attraverso un canale di comunicazione e ricevere comandi. |
| CaaS<br>Cybercrime-as-a-Service | La cibercriminalità come servizio acquistabile consente a criminali tecnicamente poco esperti di svolgere attività illegali in Internet per mezzo di strumenti di facile utilizzo. |
| CEO-Fraud | Si parla di «CEO Fraud» (truffa del CEO) nel caso di usurpazione dell'identità di un dirigente d'azienda e quando a suo nome si richiede al servizio competente (servizio finanziario, contabilità) di effettuare un versamento su un conto generalmente all'estero. |
| CPU / Processore | «Central Processing Unit» / processore: unità centrale di un computer, contiene i circuiti logici necessari al funzionamento di un programma per computer. |
| Cryptomining | Con il mining vengono creati nuovi blocchi che si aggiungono alla blockchain. Il procedimento richiede calcoli molto complessi, pertanto viene retribuito. |
| Defacement | Deturpamento di pagine web. |
| DNS<br>Domain Name System | Con l'ausilio del DNS, Internet e i suoi servizi sono di agevole utilizzazione, in quanto gli utenti al posto dell'indirizzo IP, possono utilizzare un vocabolo (ad es. www.melani.admin.ch). |
| Dropper / Downloader | Programma che scarica e installa una o più istanze di malware. |

| Termine | Descrizione |
|---|---|
| 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. |
| File ZIP | Zip è un algoritmo e un formato di file per la compressione dei file, destinato a ridurre lo spazio di memorizzazione dei file per l'archiviazione e la trasmissione. |
| GPS<br><br>Global Positioning System | Il Global Positioning System (GPS), ufficialmente NAVSTAR GPS, è un sistema globale di navigazione satellitare per la determinazione della posizione e la misura del tempo. |
| Infezione da «drive-by» | Infezione del computer mediante malware unicamente attraverso la consultazione di una pagina web. L'infezione avviene perlopiù per il tramite dell'utilizzo di exploit che sfruttano le lacune nel sistema di sicurezza lasciate scoperte dal visitatore. |
| Infezione da pagina web | Infezione di un computer con malware unicamente attraverso la consultazione di un sito web. Spesso le pagine web colpite contengono offerte serie e sono state precedentemente compromesse allo scopo di propagare il malware. L'infezione avviene perlopiù per il tramite dell'utilizzo di exploit che sfruttano le lacune nel sistema di sicurezza lasciate scoperte dal visitatore. |
| Internet delle cose | L'espressione «Internet delle cose» indica che nel mondo digitale il computer è integrato in misura crescente da «oggetti intelligenti», ossia dall'applicazione dell'intelligenza digitale agli oggetti reali. |
| ISP<br><br>Internet Service Provider | Gli offerenti di prestazioni Internet forniscono servizi, contenuti o prestazioni tecniche indispensabili per l'utilizzazione o la gestione dei contenuti e dei servizi Internet. |
| Javascript | Un linguaggio di script orientato sugli oggetti per lo sviluppo di applicazioni. Gli Javascript sono elementi di programma integrati nel codice HTML, che consentono determinate funzioni nel browser di Internet. Ne può essere un esempio il controllo dei dati immessi dall'utente in un modulo web. È così possibile verificare se tutti i caratteri immessi alla richiesta di un numero telefonico corrispondono effettivamente a delle cifre. Come gli ActiveX Control, gli JavaScript sono eseguiti sul computer del visitatore di pagine Internet. Oltre a funzioni utili, è però anche possibile programmare funzioni nocive. Diversamente dagli ActiveX Control, gli JavaScript sono supportati da tutti i browser. |

| Termine | Descrizione |
|---|---|
| Lacuna di sicurezza | Vulnerabilità dell'hardware o del software, tramite la quale gli aggressori possono accedere a un sistema. |
| Malspam | Invio di e-mail di massa con cui viene diffuso il malware. |
| Malware / Software maligno | Termine generico per software che esegue funzioni nocive su un computer. Rientrano tra l'altro in questo gruppo i virus, i vermi informatici e i cavalli di Troia. |
| Metadati | I metadati o metainformazioni sono dati che contengono informazioni su altri dati. |
| MITM | Attacco Man-in-the-Middle. Attacco nel corso del quale l'aggressore si insinua inosservato su un canale di comunicazione tra due partner, in modo da essere in grado di seguire o di modificare lo scambio di dati. |
| MSP<br>Managed Services Provider | Un fornitore di modelli operativi o di soluzioni operative è un fornitore di servizi IT che fornisce e gestisce un insieme definito di servizi per i propri clienti. |
| NAS<br>Network Attached Storage | Archiviazione collegata alla rete: disco rigido o server di dati collegato direttamente a una rete. |
| P2P | Peer to Peer. Un'architettura di rete nel cui ambito i sistemi partecipanti possono assumere le medesime funzioni (diversamente dalle architetture cliente-server). Il P2P è sovente utilizzato per lo scambio di dati. |
| Patch | Un software che sostituisce le componenti di un programma affette da errori, sopprimendo così per esempio una lacuna di sicurezza. |
| Phishing | Nel caso del phishing i truffatori tentano di accedere ai dati confidenziali di ignari utenti di Internet. Si può trattare per esempio di informazioni sui conti di offerenti di aste online (ad es. eBay) o di dati di accesso a servizi bancari via Internet. I truffatori sfruttano la buona fede e la disponibilità delle loro vittime inviando loro e-mail nei quali l'indirizzo del mittente è falsificato. |
| Protocollo SMB | Server Message Block (SMB): protocollo per la condivisione in rete di file, stampanti e server in reti di computer. |
| Proxy | Interfaccia di comunicazione in una rete che funge da intermediario che riceve le richieste da un lato per poi effettuare il collegamento dall'altro lato con il proprio indirizzo. |

| Termine | Descrizione |
|---|---|
| RaaS<br><br>Ransomware-as-a-Service | Il ransomware come servizio acquistabile consente a criminali tecnicamente poco esperti di effettuare attacchi per mezzo di strumenti di facile utilizzo. |
| Ransomware | Malware che nel caso tipico codifica i dati delle vittime per convincerle a pagare un riscatto. |
| RDP<br><br>Remote Desktop Protocol | Un protocollo di rete di Microsoft per l'accesso a distanza ai computer Windows. |
| Remote Administration Tool | Il software di manutenzione a distanza (in inglese: Remote Administration Tool) costituisce un'applicazione nell'ambito del concetto di manutenzione a distanza di qualsiasi computer o sistema di computer. |
| Router | Apparecchiature del settore delle reti di computer, della telecomunicazione o anche di Internet che collegano o separano più reti di computer. I router sono ad esempio utilizzati nelle reti domestiche per effettuare il collegamento tra la rete interna e Internet. |
| Script PowerShell | PowerShell è un framework multipiattaforma di Microsoft che consente di automatizzare, configurare e gestire sistemi ed è composto da un interprete a riga di comando (shell) e da un linguaggio di scripting. |
| Sistemi industriali di controllo (ICS) | I sistemi di controllo e di comando constano di una o più apparecchiature che guidano, regolano e/o sorvegliano il comportamento di altre apparecchiature o sistemi. Nella produzione industriale il concetto di «sistemi industriali di controllo» (inglese: Industrial Control Systems, ICS) è corrente. |
| Smartphone | Lo smartphone è un telefono mobile che mette a disposizione una maggiore funzionalità di computer di quella di un telefono mobile progredito usuale. |
| SMS | Short Message Service. Servizio per l'invio di messaggi brevi (160 caratteri al massimo) agli utenti di telefonia mobile. |
| Social Engineering | Gli attacchi di social engineering sfruttano la disponibilità, la buona fede e l'insicurezza delle persone per accedere per esempio a dati confidenziali o per indurre le vittime a effettuare determinate operazioni. Una nota forma di social engineering è il phishing. |
| Software maligno / Malware | Termine generico per software che esegue funzioni nocive su un computer. Rientrano tra l'altro in questo gruppo i virus, i vermi informatici e i cavalli di Troia. |

| Termine | Descrizione |
|---|---|
| Spam | Il termine spam designa l'invio non sollecitato e automatizzato di pubblicità di massa, definizione nella quale rientrano anche le e-mail di spam. Si designa come spammer l'autore di queste comunicazioni mentre l'invio come tale è denominato spamming. |
| Spearphishing mail | Attacco mirato di phishing. Si fa ad esempio credere alla vittima di comunicare tramite e-mail con una persona di fiducia. |
| Spoofing | Falsificazione degli elementi di indirizzo o dei segnali allo scopo di ingannare il destinatario o il dispositivo ricevente. |
| Take down | Take down (rimozione) è un'espressione utilizzata quando un provider ritira un sito dalla rete a causa della presenza di contenuti fraudolenti. |
| TCP/IP | Transmission Control Protocol / Internet Protocol (TCP/IP). Famiglia di protocolli di rete anche designata come famiglia di protocolli Internet a causa della sua grande importanza per Internet. |
| TLD<br>Top-Level-Domain | Ogni nome di dominio in Internet consta di una successione di serie di caratteri separati da un punto. La designazione Top-Level-Domain si riferisce all'ultimo nome di questa successione e costituisce il livello più elevato della risoluzione del nome. Se ad esempio il nome completo di dominio di un computer, rispettivamente di un sito web, è de.example.com, l'elemento a destra (com) rappresenta il Top-Level-Domain di questo nome. |
| UDP | «User Datagram Protocol»: protocollo di rete molto semplice, senza connessione, che trasporta datagrammi della famiglia di protocolli Internet. |
| USB | Universal Serial Bus. Bus seriale che (per il tramite di corrispondenti interfacce) consente il raccordo di periferiche come tastiera, mouse, supporti esterni di dati, stampante ecc. Al momento del raccordo o della disgiunzione di un dispositivo USB il computer non deve essere riavviato. I nuovi dispositivi sono per lo più riconosciuti e configurati automaticamente (a dipendenza però del sistema operativo). |
| Verme informatico | Diversamente dai virus, i vermi informatici non necessitano di un programma ospite per diffondersi. Essi sfrut- |

| Termine | Descrizione |
| --- | --- |
| | tano piuttosto le lacune di sicurezza o gli errori di configurazione del sistema operativo o delle applicazioni per diffondersi autonomamente da un computer all'altro. |
| WLAN | L'abbreviazione WLAN (o Wireless Local Area Network) significa rete locale senza fili. |
| Zero-Day | Exploit che appare il giorno stesso in cui la lacuna di sicurezza è resa nota al pubblico. |