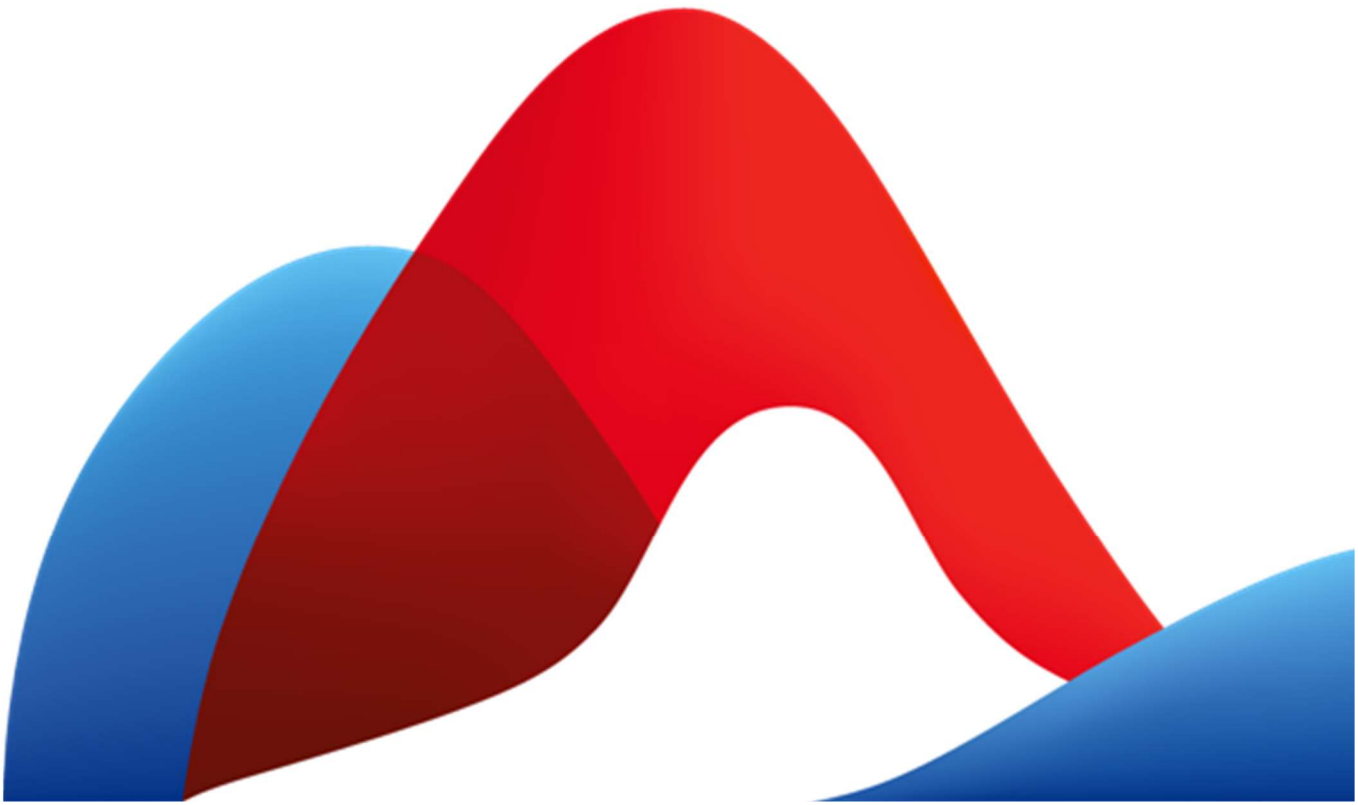
Cyber Security 2018:

Artificial Intelligence, Malware & Cryptocurrencies

Autore: Swisscom Security
Il presente report è risultato della stretta collaborazione tra Swisscom Security e altre unità operative.

Maggio 2018



Indice

1. Introduzione 3
2. Quadro della situazione – Radar delle minacce 4
2.1 Metodologia 4
2.2 Minacce 5
2.3 Conclusione 8
3. Artificial Intelligence & Cyber Security 9
3.1 Intervista con Laure Willemin, Head of AI, Swisscom 10
3.2 Applicazioni di AI & ML nella Cyber Security 11
3.3 Conclusione 13
4. Minacce nella rete di Swisscom 14
4.1 Malware Call Home 15
4.2 Crypto Mining 18
4.3 Conclusione 20
5. Glossario 22

1. Introduzione

Il Cyber Security Report di Swisscom giunge nel 2018 alla seconda edizione. Oltre allo stato attuale delle minacce, prendiamo in considerazione due argomenti che stanno attualmente preoccupando la Security Community in seno a Swisscom e presso i nostri partner e clienti, ma anche a livello internazionale.

Primo: l'applicazione dell'intelligenza artificiale nell'ambito della Security. Si constata da un lato l'impiego abusivo al fine di sferrare attacchi più intelligenti; dall'altro, soprattutto, l'impiego più mirato al fine di individuare e risolvere prima, oltre che in maniera più puntuale, attacchi e punti deboli.

Secondo: il malware che abbiamo individuato nella nostra rete. La diffusione del malware è e rimane lo strumento principale degli aggressori per compromettere servizi, rubare dati o abusare di sistemi di terzi a proprio vantaggio. La maggior parte degli attacchi viene peraltro sferrata per scopi finanziari e non c'è quindi da stupirsi che anche le criptovalute trovino posto nel nostro report.

Il presente report è il risultato della collaborazione tra diversi dipartimenti in seno a Swisscom.

Per i lettori «sbrigativi» abbiamo riassunto dopo ogni capitolo principale una conclusione che consenta loro di informarsi rapidamente. Di conseguenza, quest'anno rinunciamo a un summary finale al termine del rapporto.

Lo scorso febbraio Swisscom ha comunicato che nell'autunno 2017 terzi non autorizzati hanno avuto accesso ai dati di clienti di Swisscom attraverso un partner di distribuzione. Questo incidente non fa parte del presente rapporto. Con tale documento vogliamo presentare le tendenze generali nel cyberspazio in Svizzera e non discutere di singoli episodi concreti. A livello interno abbiamo rafforzato le misure di sicurezza al fine di escludere il ripetersi di un simile evento.

2. Quadro della situazione – Radar delle minacce

Le minacce hanno origine proprio nel continuo sviluppo di nuove tecnologie, oltre che nel loro uso e nella loro diffusione all'interno della società. Pertanto occorre individuare quanto prima e rilevare sistematicamente le minacce potenziali. Per descrivere lo stato attuale delle minacce e la relativa evoluzione ci serviremo di un radar (Figura 1).

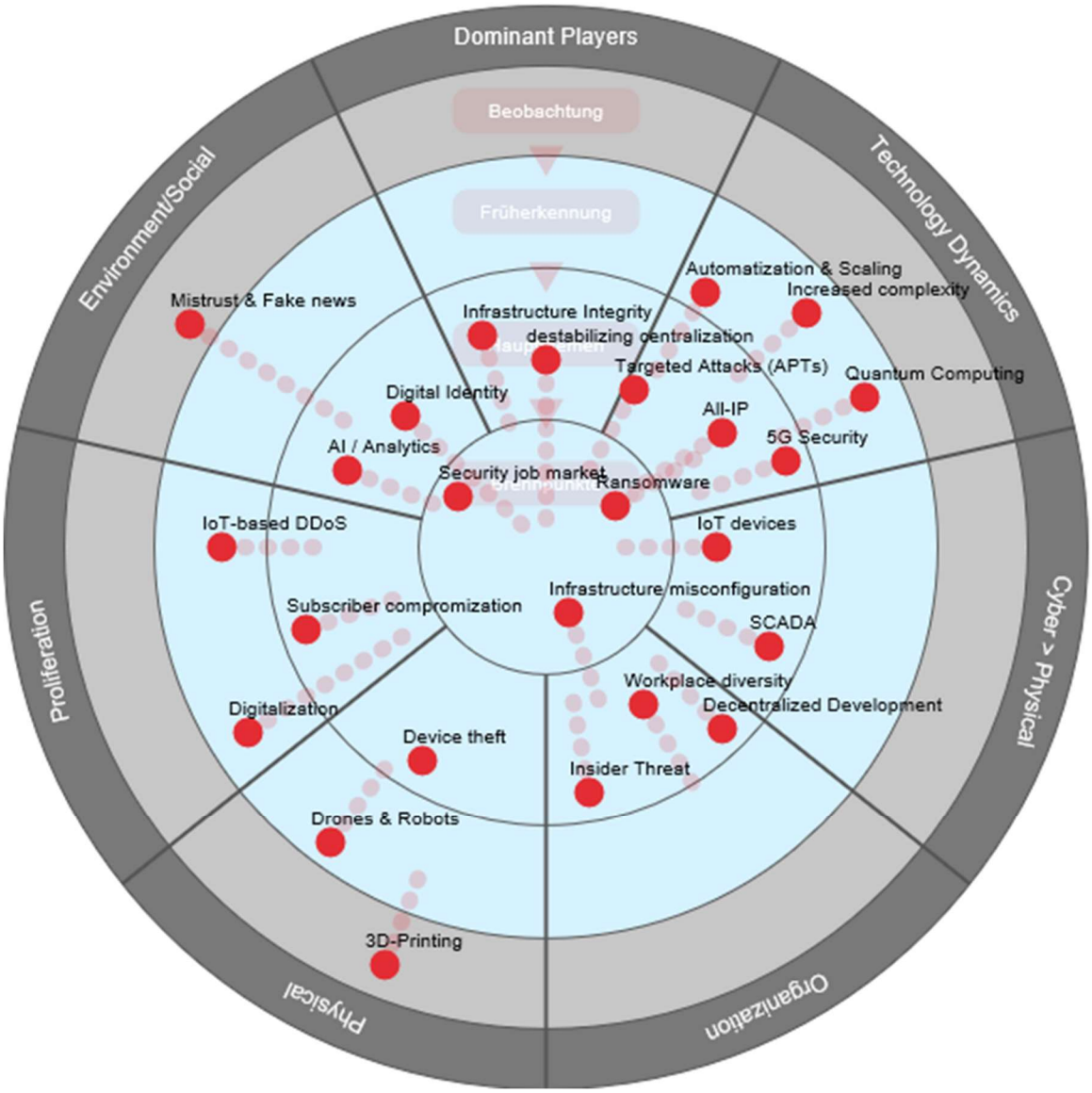


Figura 1: radar delle minacce

2.1 Metodologia

Il radar delle minacce è diviso in sette segmenti che delimitano i diversi domini delle minacce. In ogni segmento le relative minacce possono essere assegnate a uno dei quattro anelli concentrici. I cerchi indicano l'attualità della minaccia e quindi anche l'approssimazione della valutazione della minaccia. Più la minaccia è vicina al centro

del cerchio, più è concreta e tanto più importanti sono le contromisure necessarie. Definiamo gli anelli come

- **emergenze** per minacce già reali e controllate con un impiego relativamente importante di risorse;
- **temi principali** per minacce che sono già comparse occasionalmente e controllate con un impiego normale di risorse. Spesso sussistono processi regolati per contrastare in modo efficiente queste minacce;
- **allerta precoce** per minacce non ancora comparse o che attualmente mostrano solo un'azione ridotta. Sono stati avviati dei progetti per contrastare tempestivamente una futura crescente importanza di tali minacce;
- **osservazione** per minacce che compariranno solo tra qualche anno. Non vi sono misure concrete per gestire queste minacce.

Inoltre, le minacce contrassegnate dai punti citati mostrano una tendenza. Questa può essere in aumento, in diminuzione o stabile nella propria criticità. La lunghezza del raggio della tendenza indica la velocità di trasformazione attesa della criticità della minaccia.

2.2 Minacce

2.2.1 Dominant Players

Minacce derivanti da interdipendenze di produttori, servizi o protocolli dominanti.

Temi principali	**Infrastructure Integrity:** i componenti fondamentali di infrastrutture critiche possono aver installato per negligenza o volutamente delle falle che minacciano la sicurezza del sistema. **Destabilizing Centralization:** la forte centralizzazione nella struttura di internet comporta un rischio di accumulazione. L'interruzione di un servizio può avere effetti a livello mondiale, come ad esempio l'interruzione di Amazon Web Services (AWS).

2.2.2 Technology Dynamics

Le minacce derivanti dalla rapidissima innovazione tecnologica da un lato forniscono nuove opportunità agli hacker e dall'altro creano nuove minacce dovute allo sviluppo stesso.

Emergenze	**Ransomware:** i dati critici vengono cifrati su vasta scala e decifrati (eventualmente) in cambio di un riscatto.
Temi principali	**Targeted Attacks (APTs):** le persone chiave sono identificate e aggredite in modo mirato per ottenere informazioni rilevanti o per creare il massimo danno possibile. **All-IP:** durante il lancio con copertura capillare di All-IP aumentano i rischi in relazione alla tecnologia VoIP.

	5G Security: 5G è una tecnologia comunicazione mobile ancora giovane, l'introduzione porterà con sé oltre alle numerose opportunità anche delle minacce ancora sconosciute.
Allerta precoce	**Automatization & Scaling:** una maggiore automazione dei processi operativi tecnici sarà di maggiore impatto in caso di attacchi compiuti con successo o configurazioni errate. **Increased Complexity:** è in continua crescita la complessità dei sistemi, in particolare oltre i confini tecnologici e aziendali. Aumenta di conseguenza il rischio di esposizione e la ricerca dell'errore diventa sempre più difficile. **Quantum Computing:** i computer quantistici possono rendere inutilizzabili le procedure crittografiche esistenti, poiché riescono a decifrarle in pochissimo tempo.

2.2.3 Cyber goes physical

Gli attacchi tramite le infrastrutture nel cyberspace provocheranno sempre più danni nel mondo fisico.

Temi principali	**IoT Devices:**i dispositivi con una protezione debole possono essere compromessi e sabotati. Potranno così essere limitati nella propria funzione, ad esempio in fatto di disponibilità o integrità dei dati. **SCADA:**esistono ancora dei sistemi di controllo protetti male o non protetti per gli impianti delle infrastrutture critiche.

2.2.4 Organization

Minacce che si basano sulle modifiche nelle organizzazioni o sfruttano i punti deboli nelle organizzazioni.

Emergenza	**Infrastructure Misconfiguration:** sfruttamento di componenti mal configurati delle infrastrutture e/o falle identificate ed eliminate tardivamente.
Temi principali	**Workplace Diversity:** oltre alle numerose opportunità che i nuovi modelli di lavoro portano con sé, l'impiego incontrollato di tali modelli, come ad es. «Bring your own Device» (BYOD) oppure il maggiore impiego di postazioni di lavoro remote comporta una maggiore esposizione al rischio. **Insider Threat:** partner o collaboratori manipolano, usano in modo illecito o vendono per negligenza o intenzionalmente le informazioni. **Decentralized Development:** i classici settori di sviluppo sono in via d'estinzione, lo sviluppo di applicazioni si avvicina alle Business Unit e al contempo si riducono i cicli delle release.

2.2.5 Physical

Minacce derivanti da un ambiente fisico e di regola orientate verso obiettivi fisici.

Temi principali	**Device Theft:** il furto, in particolare di componenti dell'infrastruttura critica o in futuro sempre più di apparecchi IoT, può comportare la perdita di dati o compromettere la disponibilità dei servizi.
Allerta precoce	**Drones and Robots:** lo spionaggio o gli attacchi da grande distanza diventano più semplici ed economici.
Osservazione	**3D-Printing:** la produzione ad esempio di chiavi o di altri dispositivi fisici diventa più economica e semplice con la migliore qualità delle stampanti 3D.

2.2.6 Proliferation

Minacce che approfittano della sempre più semplice ed economica disponibilità di media IT e know-how. Da un lato perché la diffusione comporta un maggior numero di potenziali bersagli di attacchi e dall'altro perché incrementa la disponibilità di strumenti di attacco.

Temi principali	**Subscriber Compromization:** il software dannoso attacca i dati privati degli utenti mobile o viene utilizzato per attacchi all'infrastruttura IT o delle telecomunicazioni.
Allerta precoce	**IoT-based DDoS:** la grande diffusione di dispositivi IoT con una scarsa protezione porta a un maggior numero di «candidati di trasmissione» per botnet. **Digitalization:** una messa in rete sempre maggiore del mondo reale e virtuale e della vita privata e commerciale comporta un maggior numero di vie di attacco.

2.2.7 Environmental / Social

Minacce che originano da cambiamenti socio-politici o che diventano più semplici o vantaggiosi per gli hacker a causa di tali cambiamenti.

Emergenza	**Security Job Market:** la richiesta di Security-Professionals viene soddisfatta con molta difficoltà, comportando un minore know-how nell'attività contro attacchi sempre più complessi e intelligenti.
Temi principali	**AI / Analytics:** un numero maggiore di dati e migliori modelli di analisi mediante AI possono essere oggetto di abuso allo scopo di influenzare il comportamento degli uomini. Le decisioni sono lasciate sempre più a sistemi autonomi. **Digital Identity:** identità digitali personali autenticate possono essere oggetto di furto o abuso, ad esempio per stipulare contratti a nome di terzi.
Osservazione	**Mistrust & Fake News:** la sempre più scarsa fiducia verso gli uffici statali o sociali può portare a una riduzione dello scambio

di informazioni per l'identificazione e la difesa contro potenziali attacchi.

2.3 Conclusione

Il nostro quadro della situazione mostra la sempre maggiore complessità della situazione delle minacce. Gli hacker profittano del crescente valore degli asset virtuali, accrescendo la motivazione per un attacco mirato e intelligente. Inoltre, le innovazioni tecnologiche e la convergenza del mondo fisico con quello virtuale creano nuove opportunità di attacco. I cambiamenti sociali hanno un effetto sulla fiducia reciproca e sul modo in cui si collabora. Tutti fattori che gli hacker possono utilizzare per i loro scopi.

Rispetto al quadro della situazione dell'anno scorso possiamo constatare che la maggior parte delle minacce note è rimasta parimenti rilevante. Alcune di queste minacce, ad esempio **Destabilizing Centralization**, **5G Security**, **Insider Threat** e l'impiego di **Ransomware**, sono invece diventate più critiche rispetto al 2017. Le relative cause (ad es. nel caso di 5G Security) possono essere la maggiore diffusione di nuove tecnologie oppure (ad es. ransomware) l'ulteriore diffusione di strumenti che consentono di sferrare questi attacchi.
L'ipotesi che le minacce tramite i sistemi SCADA siano invariate è stata corretta con un trend in crescita. Per il futuro prevediamo un inasprimento del problema in seguito al collegamento sempre più capillare dei sistemi fisici a internet.
Altre minacce ci paiono meno critiche. Gli attacchi DDoS basati su 3D-Printing e IoT in realtà non sono tanto frequenti come si pensa, sebbene rimangano rilevanti.

Nel quadro della situazione abbiamo incluso anche nuove minacce già note lo scorso anno, ma considerate meno critiche rispetto alle altre. Abbiamo ora rivalutato questa stima. Le nuove minacce nel radar sono: **Automatization & Scaling, Increased Complexity, Quantum Computing, Decentralized Development, AI / Analytics** e **Digital Identity**. Si noterà in particolare la dinamicità tecnologica nell'ambito dell'intelligenza artificiale, che da un lato ha effetti sulla Cyber Security, ma dall'altro influenza anche lo stato attuale delle minacce e assiste ad esempio potenziali hacker con strumenti intelligenti.

3. Artificial Intelligence & Cyber Security

Artificial Intelligence (AI)[1], Machine Learning (ML) e Deep Learning descrivono tre modelli collegati tra loro che delimitiamo come segue gli uni dagli altri:

Artificial Intelligence	Artificial Intelligence è l'intelligenza rappresentata dalle macchine con l'aiuto di logica, regole chiare e alberi di decisione.
Machine Learning	Machine Learning è un sottogruppo dell'AI che utilizza complesse tecniche statistiche affinché le macchine possano svolgere sempre meglio i loro compiti con l'aiuto dell'esperienza.
Deep Learning	Deep Learning è un sottogruppo di ML che consente al software di allenarsi autonomamente per eseguire compiti quali il riconoscimento vocale e delle immagini mettendo a disposizione enormi quantitativi di dati a una rete multipla neuronale.

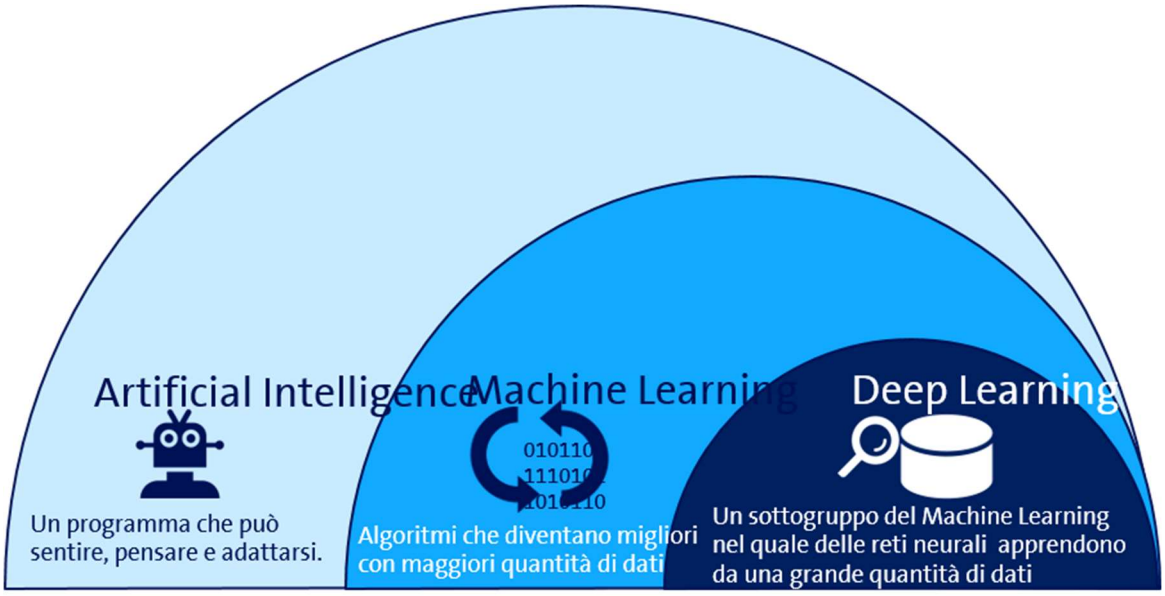


Figura 2: Artificial Intelligence, Machine Learning e Deep Learning

1 Nell'area linguistica tedesca si parla anche di intelligenza artificiale, mentre nella tecnologia di informazione si è imposto il termine inglese, che è quello che utilizziamo qui.

3.1 Intervista con Laure Willemin, Head of AI, Swisscom

Laure Willemin e il suo team sviluppano e gestiscono sistemi software robusti e scalabili utilizzando le più recenti tecnologie di AI, ML e Deep Learning, tra cui Enabler Sentiment Analysis, Key Phrase Extraction, Named Entity Recognition. La nostra collega Swisscom ama raccogliere ambiziose sfide tecnologiche e da oltre 15 anni lo fa come sviluppatrice di software, ingegnere e architetto di sistema.

Laure, l'Artificial Intelligence è semplicemente un'opportunità per Swisscom e la nostra società, o deve essere classificata anche come minaccia alla sicurezza?

Non consideriamo l'AI come una minaccia. Con la nuova tecnologia possiamo aiutare a comprendere meglio grandi quantità di dati e ad assistere gli sforzi della nostra azienda in direzione della sicurezza. Le nuove tecnologie spesso comportano incertezza e malintesi. Possono anche essere utilizzate in modo improprio. Tuttavia, gli effetti positivi sono di gran lunga superiori.

Quali sono i malintesi più frequenti che hai sentito sinora su Artificial Intelligence e Machine Learning?

Innanzitutto troppe aspettative rispetto a ciò che è possibile fare con l'AI. La parte critica di un sistema efficace sono i dati. Questi dati spesso non sono strutturati e occorre allenare i sistemi che li elaborano prima che possano essere utilizzati in modo utile. Con la più recente tecnologia possiamo fare un buon lavoro nella compilazione di modelli di dati e vediamo inoltre progressi nel lavoro con quantitativi inferiori di dati. Ciò nonostante, un'elevata qualità dei dati è la parte principale delle applicazioni AI di successo.

Secondo te AI & ML sono fattori di disturbo nel panorama industriale svizzero? A tuo parere quali sono i principali cambiamenti imminenti?

AI non è un fattore di disturbo, ma un elemento essenziale per mantenere la concorrenzialità anche in futuro. Con AI l'industria svizzera sarà in grado di automatizzare i processi e i compiti ricorrenti e impiegare personale qualificato per lavori più complessi e creativi. Al contempo AI aiuterà le persone a prendere decisioni in maniera migliore, oltre che più rapida, ad esempio con l'analisi in tempo reale dei dati.

Secondo te, AI, ML e Deep Learning come possono contribuire allo sviluppo di Cyber Security?

È possibile utilizzare la più recente tecnologia AI per analizzare grandi quantità di dati e trovare facilmente delle anomalie. In questo modo si possono individuare gli eventi riguardanti la sicurezza prima, o perlomeno prima che diventino un problema serio. La tecnologia AI non sostituisce i sistemi o gli esperti esistenti, ma riduce il lavoro spesso manuale, riduce il tempo di reazione e quindi aumenta la sicurezza complessiva di un'azienda.

A quale progetto stai lavorando attualmente?

Sviluppiamo una nuova piattaforma per il dialogo con i clienti. Swisscom segue ogni anno circa 20 milioni di interazioni con i clienti. Questo numero è in crescita continua, poiché molti clienti di norma passano direttamente da un canale all'altro. Un servizio di qualità elevata su tutti i canali è pertanto indispensabile per un'esperienza eccellente del cliente. Idealmente il cliente non dovrebbe ridare i propri dati quando passa da un canale all'altro. A tale fine Swisscom sta realizzando una nuova piattaforma digitale basata su AI per armonizzare i diversi canali di interazione tra loro e assistere al meglio il cliente.

3.2 Applicazioni di AI & ML nella Cyber Security

Come abbiamo dimostrato con il quadro della situazione 2018, diverse tendenze oggi portano a sviluppare e attuare soluzioni AI & ML per misure di Cyber Security.

- Quantità di dati sempre maggiori e applicazioni AI & ML; valutazioni circa un eventuale impiego abusivo, ad esempio per portare a termine in modo più efficace attacchi mirati.
- Lo spostamento di valori sempre più consistenti nello spazio virtuale aumenta pertanto anche la motivazione dei criminali organizzati a impiegare nuove tecnologie per rubare o compromettere tali valori.
- Il fabbisogno in continua, rapida crescita di esperti di Cyber Security genera già oggi difficoltà a formare in misura sufficiente talenti di spicco, a portarli in azienda, a farli crescere e tenerli. Nei prossimi anni la situazione è destinata a peggiorare ulteriormente.

3.2.1 Security Operations Center

Un pilastro di una strategia matura di Cyber Security è la capacità di capire che c'è stato un attacco. Questo compito viene svolto da Security Operation Center (SOC).

Un compito importante di un analista SOC consiste nel distinguere gli eventi rilevanti da quelli non rilevanti (cosiddetti falsi positivi) e di continuare a elaborare solo quelli rilevanti (true positives) come evento o evento relativo alla sicurezza. Gli analisti svolgono già oggi questo compito, ad es. con strumenti basati su regole. Tali strumenti risultano tuttavia adeguati solo nella misura in cui le regole precedentemente definite lo sono. Il loro punto debole consiste pertanto nel fatto che non sono in grado di reagire rapidamente ai cambiamenti e a eventi straordinari non previsti. Con l'aumento delle quantità di dati e attacchi sempre più intelligenti, gli strumenti basati sulle regole non saranno più sufficienti per proteggere le aziende e i relativi clienti dagli attacchi.

Sistemi intelligenti che imparano da soli sono la chiave per sviluppare ulteriormente la capacità di impedire o perlomeno individuare e respingere tempestivamente gli attacchi. Inoltre, sistemi di questo tipo sono in grado non solo di individuare anticipatamente le minacce, ma anche di cercare attivamente i punti deboli nella configurazione di un sistema e proporre o attuare direttamente misure correttive.

3.2.2 Phisherman

In Swisscom puntiamo già sull'apprendimento automatico per affrontare le minacce per la sicurezza. Il phishing è una minaccia che riguarda quotidianamente la nostra attività e i nostri clienti. Con il phishing i criminali cercano ad esempio di ottenere tramite e-mail false i dati degli utenti come password o dati delle carte di credito.
La colonna portante della prevenzione antiphishing consiste nell'individuare correttamente e rapidamente le e-mail fraudolente e distinguerle da quelle vere. Gli attacchi di phishing diventano sempre più mirati e professionali, e persino gli utenti attenti e tecnicamente bravi non sono sempre in grado di individuare chiaramente degli attacchi di phishing come tali.
In casi come questi, l'apprendimento automatico apporta un valore aggiunto. Phisherman, la nostra applicazione per impedire gli attacchi di phishing, utilizza tecniche progredite di apprendimento automatico per individuare e qualificare tentativi di phishing.

La figura seguente è un estratto effettivo di Phisherman con una comparazione delle tendenze del 2016 e 2017.
«Top phished companies» significa che gli hacker hanno cercato di farsi passare per l'azienda indicata agli occhi di altre persone. La modalità più frequente per questi tentativi sono le e-mail false. Si può chiaramente vedere che nel 2006 sono state interessate soprattutto le aziende americane e i rispettivi clienti, mentre nel 2017 sono state interessate soprattutto aziende svizzere. Mentre al «primo posto» si conferma sempre Apple e Swisscom occupa tutti e due gli anni il quinto posto, nel 2017 sono fortemente interessate anche UBS e Postfinance.

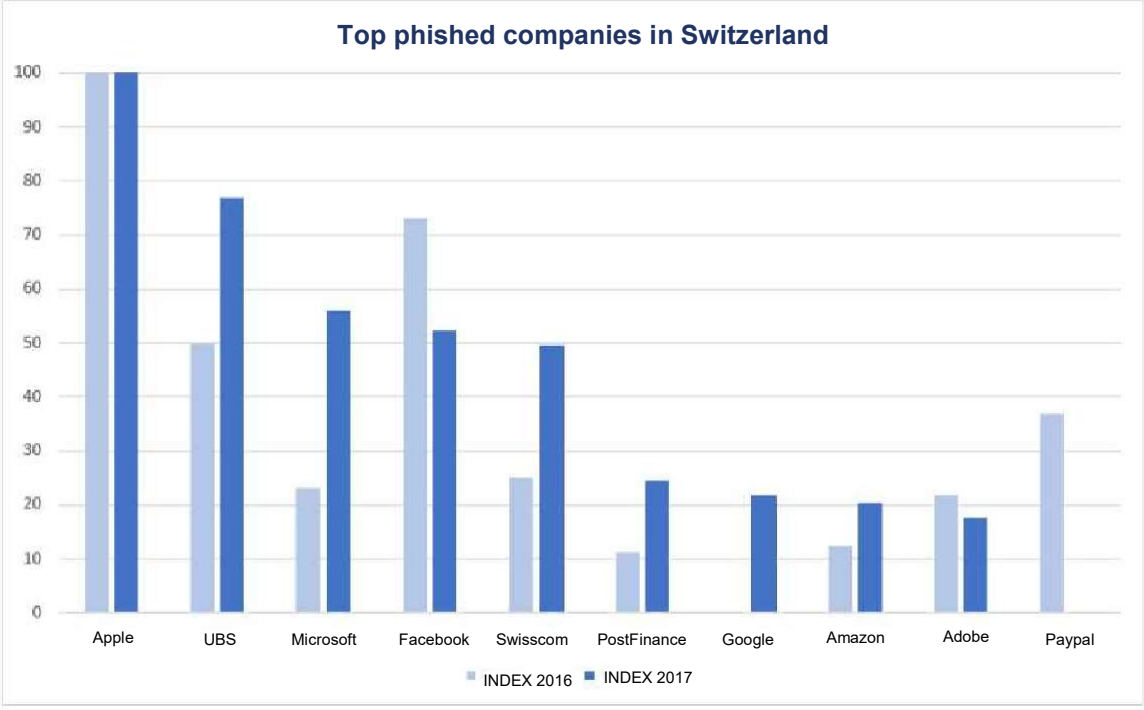


Figura 3: Top phished companies in Svizzera, valutazione 2016/17 da parte di Swisscom Phisherman

In base a questa evoluzione si può dedurre che gli attacchi di phishing sono diventati più mirati, più intelligenti e, tra le altre cose, anche più regionali. Più gli hacker sono vicini al vero contesto di vita delle persone interessate, più è facile per loro ingannarli e trarne vantaggio.

3.3 Conclusione

L'impiego di applicazioni AI sarà a breve e medio termine un fattore decisivo nell'ambito della Cyber Security. Come abbiamo dimostrato, gli analisti di Security non sono più in grado di elaborare in maniera conclusiva le quantità crescenti di dati tramite gli attuali sistemi di supporto. Gli attacchi diventano inoltre sempre più intelligenti e mirati. Anche se occorrono applicazioni AI per distinguere eventi critici da eventi non critici, in un primo momento bisognerebbe utilizzare questi sistemi solo a titolo di supporto. La responsabilità relativa alle decisioni rimarrà a lungo ancora degli specialisti prima che AI possa affermarsi come strumento valido a lungo termine nella quotidianità.

4. Minacce nella rete di Swisscom

Con diversi milioni di accessi a Internet e in quanto fornitore di infrastrutture IT e di telecomunicazione per le grandi aziende, Swisscom è interessata quotidianamente e in grande misura dalle più svariate minacce. Esse sono rivolte ai clienti finali, ma anche a infrastrutture proprie di Swisscom.

Per riuscire a delineare un quadro della situazione relativo a queste minacce, abbiamo valutato dati da DNS Sinkholes (v. glossario) e dati DNS passivi per un periodo di sei mesi. L'analisi per il riconoscimento ha preso in considerazione principalmente gli accessi DNS per l'attribuzione delle minacce all'interno della rete Swisscom per il segmento clienti finali. La validità di questo metodo di analisi è limitata, poiché l'individuazione dipende dal fatto che il dominio sia noto e che sia registrato nei dati Sinkhole.

Scopo dei risultati qui presentati è di fornire una panoramica relativa alle principali conoscenze acquisite:

La valutazione delle minacce individuate mostra un chiaro predominio di Malware Call Home Traffic (Command and Control), mentre amplificazione DNS e Adware sono presenti in misura minore. Un ulteriore predominio che si sta delineando è la comunicazione con infrastrutture di Crypto-Mining.

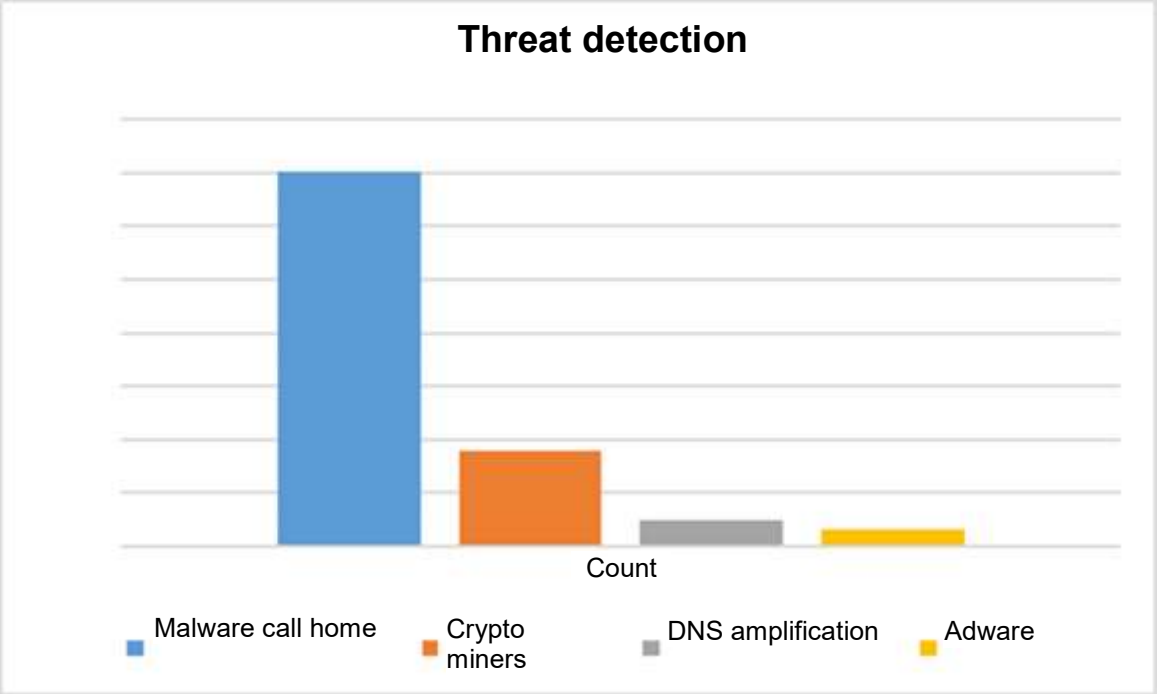


Figura 4: individuazione delle minacce

4.1 Malware Call Home

Definiamo Malware Call Home il tipico traffico di rete Command and Control (CnC). Command and Control designa la comunicazione tra un sistema infettato (ad es. bot) e il sistema sotto il controllo di un aggressore. Per poter continuare ad avere il controllo sul sistema infestato e poter eseguire altre azioni quali attacchi DDoS, l'invio di e-mail di spam o il contagio di altri sistemi, l'hacker ha bisogno di questo canale. All'interno della rete del cliente finale di Swisscom sono rappresentati in particolare Conficker, Ramnit e Gamut. Poiché nel ransomware spesso non si utilizzano componenti Command and Control, è molto difficile individuare il ransomware consultando il DNS. Rappresenta un'eccezione il ransomware di WannaCry, che può essere riconosciuto tramite il dominio Kill-Switch.

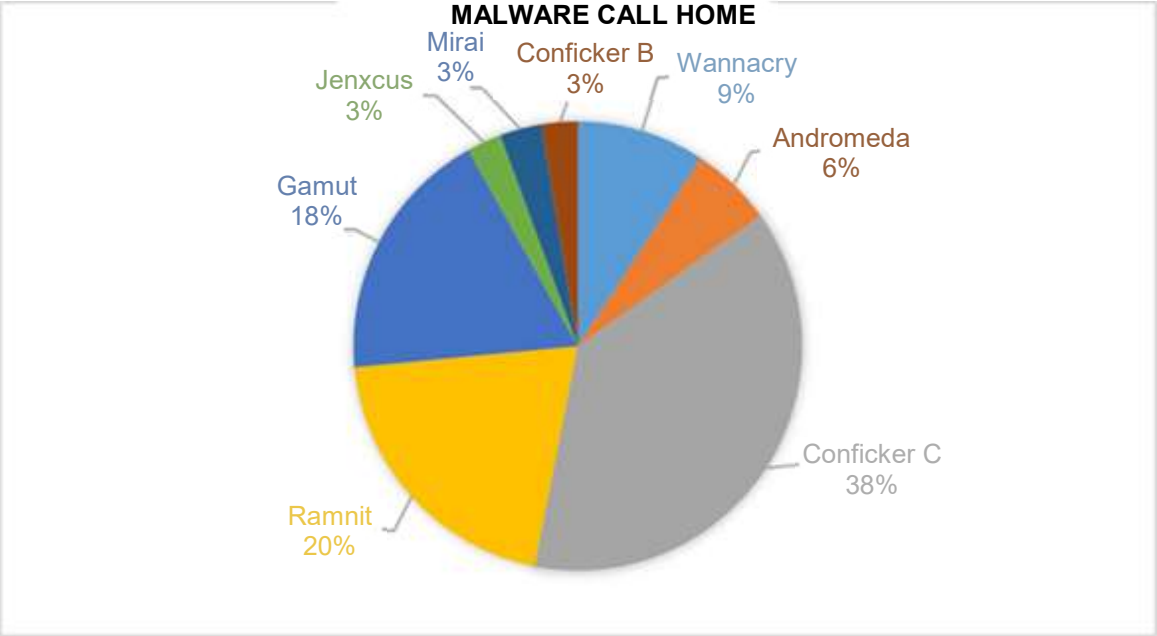


Figura 5: Malware Call Home

I risultati rappresentano attacchi riconosciuti a infrastrutture già bloccate tramite DNS Sinkholes.

Conficker, noto anche come Downadup, è emerso dal 2008 in diverse varianti e ha infettato milioni di sistemi Windows. Il malware ha sfruttato un punto debole nel Server Service di Microsoft Windows e ha utilizzato nelle versioni B e C un Dictionary Attack e Windows Autorun per autopropagarsi. La versione C è la famiglia di malware più diffusa in Svizzera. Un working group (Conficker Working Group) è stato istituito appositamente per fermare Conficker. Il working group è riuscito ad arrestare l'ulteriore diffusione di Conficker. A tutt'oggi non si conoscono gli attori dietro Conficker.

Ramnit è un malware toolkit modulare che gode di grande popolarità tra i criminali informatici già dal 2010. Il malware è in grado di seguire il comportamento di web-browsing dei sistemi delle vittime e a leggere ed estrarre ad es. i dati d'accesso

immessi. Il toolkit utilizza diversi metodi per rimanere con persistenza su un sistema infettato. Tra gli altri vengono infettati file .exe, .dll, .htm e .html. Il malware si copia autonomamente su tutti i dischi rigidi collegati (anche gli apparecchi collegati tramite USB vengono infettati). Le infezioni Ramnit sono ancora molto presenti in Svizzera.

Gamut è una botnet di spamming che prende il controllo dei sistemi Windows per inviare dello spam. Secondo un'analisi aggiornata, insieme allo Spam Botnet Necurs, Gamut è stato responsabile del 97% delle e-mail di spam inviate nell'ultimo trimestre 2017.

4.1.1 WannaCry

Sebbene sulla nostra rete si rilevi una presenza più ridotta di WannaCry, desideriamo comunque trattare questo ransomware tenuto conto delle sue caratteristiche particolari. Il ransomware precedentemente noto si caratterizzava per il fatto che arrivava ai sistemi target mediante e-mail di spam, pagine web infettate o tramite botnet e vi rimaneva per estorcere denaro alle proprie vittime. Il ransomware è molto popolare soprattutto tra i criminali informatici. I motivi principali, a nostro parere, sono quelli raffigurati nella tabella seguente.

Low Entry Barrier	Una crescente professionalità delle offerte di Ransomware as a Service, grazie alle quali anche i criminali senza conoscenze di programmazione o know-how tecnico hanno la possibilità di effettuare attacchi di ransomware.
Trasferimento anonimo di denaro	Con la diffusione di criptovalute anonime quali Monero, i criminali informatici possono agire in tutto il mondo ed estorcere globalmente denaro digitale alle loro vittime senza che la loro identità venga resa nota e possa essere rintracciata.
Impotenza delle vittime	Soprattutto gli utenti privati e le PMI che non hanno una strategia di backup per i loro dati considerano il pagamento del denaro chiesto come unica possibilità per recuperare i loro dati.

Con WannaCry è stata raggiunta per la prima volta una nuova dimensione dell'infezione automatica di ransomware. La campagna WannaCry individuata nel maggio 2017 ha sfruttato il già noto ETERNALBLUE Exploit per la pubblicazione non desiderata dell'arsenale dell'NSA. Nel giro di pochi giorni, più di 230 000 sistemi in oltre 150 paesi sono stati automaticamente infettati. Tra le vittime interessate c'erano anche infrastrutture critiche come il National Health Service o Deutsche Bahn[2].

2 https://www.heise.de/newsticker/meldung/Ransomware-WannaCry-befaellt-Rechner-der-Deutschen-Bahn-3713426.html

Figura 6: infezione WannaCry

Anche la Svizzera è stata ed è interessata dalla campagna WannaCry, a differenza di molti altri paesi, tuttavia, non sono state colpite infrastrutture critiche. Globalmente, l'attacco dimostra comunque in modo esemplare che sfruttando un unico punto debole si può dare il via a una pandemia tramite meccanismi di propagazione laterali, e che i confini della rete quali il perimetro e la rete interna si fondono mettendo a nudo la vulnerabilità dei nostri sistemi interconnessi e della nostra epoca digitale.

4.2 Crypto Mining

Mentre le criptovalute continuano a godere di grande popolarità negli attacchi di ransomware, è emersa un'altra nuova tendenza tra le minacce individuate nella rete di Swisscom: il mining delle[3] criptovalute. Per il mining di criptovalute in quanto minaccia riconosciuta s'intende il mining non autorizzato di criptovalute, ad es. mediante l'installazione di miner da parte di...

Insider	La possibilità gratuita di procedere al mining sfruttando le risorse (potenza di calcolo) e a spese dell'azienda (elettricità) rende il mining attraente per i collaboratori delle aziende. Potrebbero farne uso i collaboratori con privilegi particolari (ad es. amministratori, power user)[4].
Malware	A differenza del ransomware con pagamenti unici, il mining garantisce entrate regolari ed è pertanto molto più redditizio per i criminali informatici.
Drive By Mining	Drive By Mining viene eseguito direttamente tramite linguaggi di scripting nel browser e utilizza la potenza della CPU dei visitatori delle pagine web

Una valutazione generale dei nostri dati DNS passivi rileva quali pool vengono utilizzati attivamente per il mining delle criptovalute.

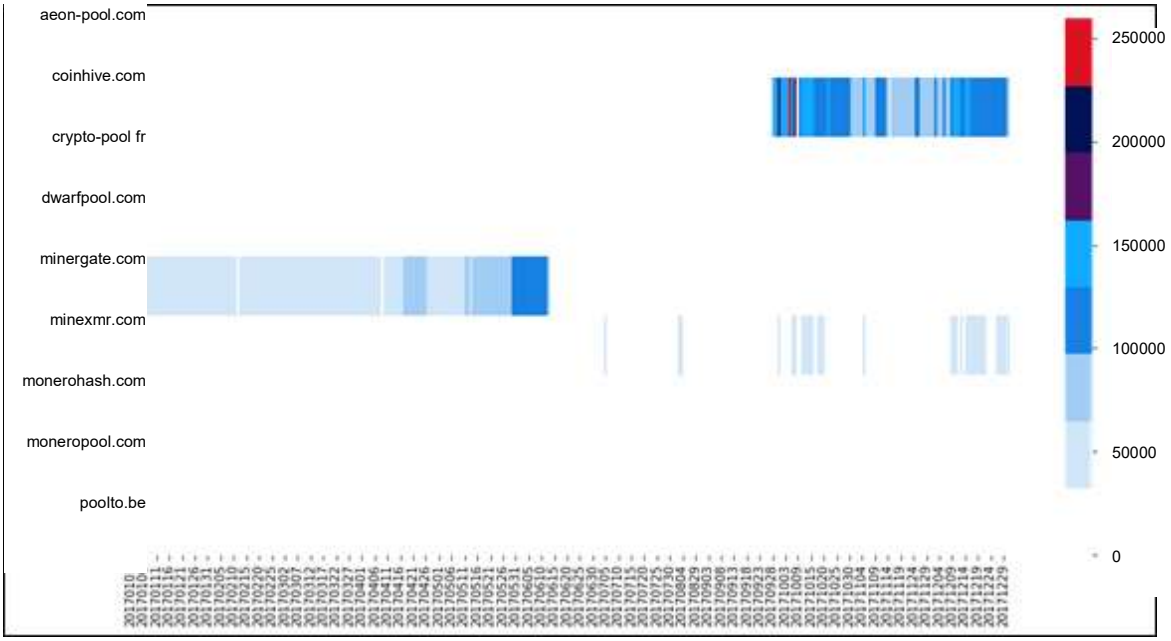


Figura 7: utilizzo del mining pool

Le voci in bianco si situano al di sotto di 50 000 esecuzioni al giorno. Si sottolineeranno i pool minergate.com e coinhive.com. L'utilizzo di questi pool non è

3 Il mining utilizza la potenza di calcolo per confermare transazioni di criptovalute. Il mining è incentivato finanziariamente.
4 https://www.rferl.org/a/russia-sarov-nuclear-facility-workers-arrested-using-supercomputer-mine-bitcoin/29030004.html

riconducibile in generale a cattive intenzioni, ma i criminali informatici hanno iniziato da tempo a dotare il loro software dannoso di un cryptominer, e per questo modello redditizio di monetizzazione dei calcolatori infettati si rifanno ai mining pool collaudati.

La proliferazione di installazioni di miner riguarda client, server e anche browser.

4.2.1 Coinhive

È soprattutto Coinhive a godere di grande popolarità tra gli hacker per il mining delle criptevalute tramite Drive By Mining. Poiché Coinhive viene eseguito direttamente nel browser di una vittima e, per effettuare il mining della criptovaluta Monero, sfrutta la potenza della CPU dei visitatori della pagina web tramite Javascript, è facile da usare e non comporta costi di esercizio per i criminali informatici. Per ottenere quanti più soldi possibile, i criminali informatici mirano le pagine web molto visitate. Da tempo sono diventate un target anche le pagine web governative, su cui è stato integrato il Javascript Coinhive Mining, che è oggetto di abuso per attacchi Drive-By Mining[5].

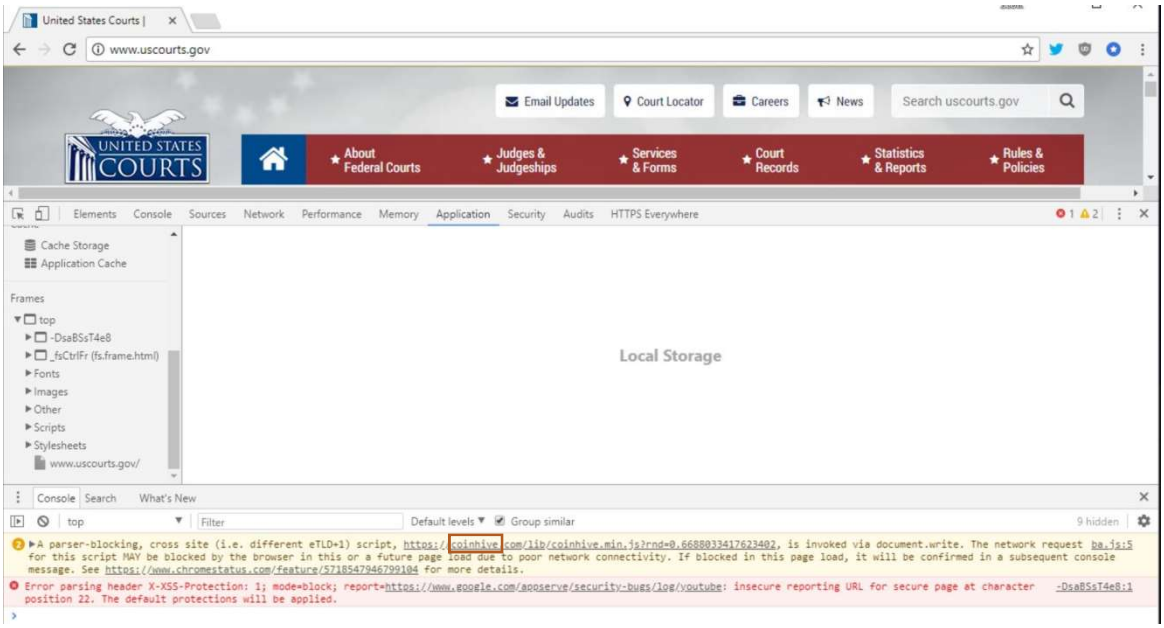


Figura 8: pagina della United States Court infettata con il Javascript Coinhive.

In un'analisi attuale abbiamo utilizzato la pagina publicwww.com per individuare pagine web che caricano il Javascript Coinhive.

5 https://twitter.com/Scott_Helme/status/962684239975272450

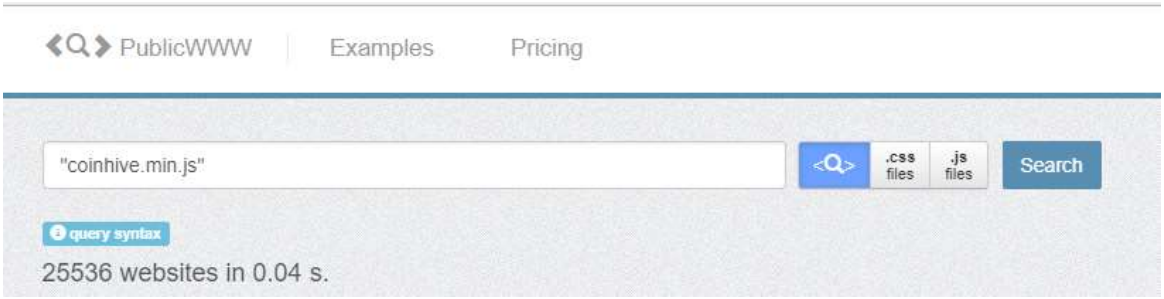


Figura 9: Coinhive su publicwww

Nel complesso sono state identificate più di 25 500 pagine web che eseguono tramite Coinhive operazioni di Drive-By-Mining sui terminali dei visitatori delle pagine web. Molte di queste pagine web sono state dichiarate compromesse[6].

4.3 Conclusione

Con infezioni Conficker, Gamut, Ramnit e WannaCry, le famiglie di malware sono presenti per diversi scopi presso i clienti finali all'interno della rete Swisscom. Le infezioni di Conficker fanno pensare che molti dei sistemi infettati utilizzino ancora sistemi operativi Legacy con punti deboli sfruttati da Conficker. Le infezioni Gamut e Ramnit mostrano che i criminali informatici hanno il controllo di un numero elevato di sistemi di clienti finali svizzeri che utilizzano in modo abusivo per i loro scopi. Nonostante la Svizzera sia stata interessata poco da WannaCry, in futuro dobbiamo attenderci che, con la crescente digitalizzazione (v. Threat Radar), aumenti il pericolo di un'ulteriore arma informatica «fuori controllo» con conseguenze a livello globale.

La valutazione dei mining pool per le criptovalute ha rilevato un numero elevato di possibili accessi drive-by-cryptomining. Il modello di lucro e l'anonimato delle criptovalute rendono questa nuova tecnologia particolarmente interessante per i criminali informatici. Oltre all'installazione di miner da parte di insider o drive-by-Mining come Coinhive, anche le imprese potrebbero mettersi a utilizzare le risorse aziendali presenti per effettuare mining.

In quanto Internet Service Provider, Swisscom garantisce un accesso a internet impeccabile, sicuro e senza barriere per i nostri clienti e la nostra società. Da un lato ci impegniamo a proteggere i nostri clienti; dall'altro, non possiamo compromettere l'aspetto pubblico della rete e sosteniamo un Internet aperto in Svizzera[7].

Per garantire la protezione da malware abbiamo già in uso diversi meccanismi stabiliti quali:

6 https://badpackets.net/cryptojacking-malware-coinhive-found-on-30000-websites/
7 https://asut.ch/asut/media/id/153/type/document/bv_verhaltenskodex_mit_asut_201603.pdf

Spam Traps	Le Spam Traps sono indirizzi e-mail senza utente, creati per identificare e-mail illegittime quali messaggi di spam e phishing o attacchi malware. Swisscom gestisce migliaia di account e-mail analoghi il cui contenuto viene analizzato automaticamente per poi confluire nei filtri di protezione.
Internet Guard	La Swisscom Internet Guard funziona sulla base di blacklist di fornitori terzi e blacklist proprie che vengono alimentate e bloccate sui nostri server DNS. Tramite l'impiego dell'infrastruttura DNS Internet Guard, i clienti sono protetti da siti web considerati nocivi.
Segnalazioni dei clienti	I siti web fraudolenti (ad es. phishing o tentativi di frode), i siti web con un software dannoso (virus, trojans ecc.) e i siti che sfruttano una falla nella sicurezza sugli apparecchi possono essere segnalati direttamente tramite e-mail a spamreport@bluewin.ch.

I clienti che sono già infettati con malware vengono delimitati in una sandbox, una rete di quarantena isolata. Quando tenta di collegarsi, il cliente visualizza una pagina informativa che gli comunica la misura e il motivo e gli fornisce ulteriori informazioni per risolvere autonomamente il problema. Non sono interessati dal blocco Swisscom TV e la telefonia. Inoltre, sono possibili connessioni che aiutano il cliente a risolvere il problema, ad esempio tramite programmi antivirus, aggiornamenti di software ecc.

5. Glossario

0-day/Zero-day exploit	Exploit di un software che è noto già da prima o dal momento in cui una faglia nella sicurezza viene resa nota. Ciò significa che l'exploit è disponibile da prima che i produttori del software abbiano predisposto una patch di sicurezza.
API	Application Programming Interface. Interfaccia di programmazione che permette ai programmi di scambiarsi dati con un unico linguaggio (macchina-macchina).
Backdoor	Porta sul retro nell'informatica che permette di accedere a un computer aggirando le protezioni.
Botnet	Rete di cui fa parte un elevato numero di computer compromessi, controllati centralmente da un botmaster.
Defacement	Inserimento di contenuti indesiderati in una pagina web attaccata da hacker.
DoS, DDoS	Denial of Service (DoS). Malfunzionamento di un sistema causato da un elevato numero di richieste. Distributed Denial of Service (DDoS). Attacco DOS che parte simultaneamente da un elevato numero di sistemi distribuiti (ad es.: una botnet). Fermare l'attacco non è facile.
DNS Sinkhole	I DNS Sinkholes vengono impiegati principalmente per dirigere un dominio notoriamente nocivo verso un altro indirizzo IP tramite DNS.
Exploit	Programma, codice o sequenze di comandi che permettono di sfruttare le vulnerabilità di un software.
Exploit Mitigation	Concetto generico che indica le tecniche utilizzate per ostacolare o impedire lo sfruttamento delle vulnerabilità dei sistemi.
ICS	Industry Control System. Termine generico che indica i sistemi di controllo industriale, vedere SCADA.
ICT	Information and Communication Technology, abbreviazione che indica il settore informatico e delle telecomunicazioni.
Jamming	Disturbo intenzionale delle telecomunicazioni.
Kill-switch	Software nascosto e in grado di reagire a ordini esterni. Disturba il funzionamento di un sistema o lo rende inutilizzabile.
Malware	Software che avvia attività dannose e indesiderate.
Money mule	Persone indotte ad accettare pagamenti dai «clienti» e a trasferire le somme di denaro, in cambio di una

	commissione. Il soggetto (money mule) è convinto di lavorare per un'organizzazione legittima.
Monero	La criptovaluta Monero presenta vantaggi particolari per i criminali informatici, ad es. transazioni non rintracciabili e l'algoritmo CryptoNight che preferisce le CPU e GPU di computer e server. Con quest'ultimo Monero si distingue nettamente da Bitcoin con riferimento al mining, per il quale occorre ormai un hardware speciale molto caro.
OSINT	Open Source Intelligence Raccolta di informazioni con l'utilizzo esclusivo di fonti pubblicamente accessibili.
Patch Aggiornamento per la sicurezza	Codice che sostituisce il software difettoso per eliminarne le faglie nella sicurezza.
Phishing	Con il phishing gli utenti vengono indotti (perlopiù tramite e-mail con false richieste) a rivelare informazioni sensibili.
SCADA	Supervisory Control And Data Acquisition System Sistemi per il monitoraggio e il controllo degli impianti (ad es.: processi industriali).
Vulnerabilità	Faglie nella sicurezza o punti deboli di hardware o software che forniscono agli aggressori un punto di accesso al sistema.
SDR	Software Defined Radio. Trasmettitore universale ad alta frequenza che genera il segnale da software, adattabile pertanto da parte dell'utente a diversi protocolli e applicazioni.
Smart grid	Rete elettrica intelligente. Il concetto di smart grid comprende l'interconnessione e il controllo di generazione, stoccaggio e utilizzo di energia elettrica, nonché delle reti di trasmissione e distribuzione.
Smart home	Domotica. Concetto che abbraccia il controllo in rete e parzialmente automatizzato di energia, manutenzione e sicurezza in edifici e appartamenti.
Social Media	Siti web che permettono lo scambio tra gli utenti attraverso un profilo proprio (es.: Facebook, Twitter, LinkedIn, Zing).
Spearphishing	Attacchi di phising mirati e personalizzati, ad es. per ottenere i dati di accesso di persone chiave.
Spoofing	Tentativi di frode all'interno di reti al fine di nascondere la propria identità.