TINEXTA CYBER

RANSOMWARE, IL RAPPORTO YOROI:
Attori, numeri e minacce
Aprile 2022

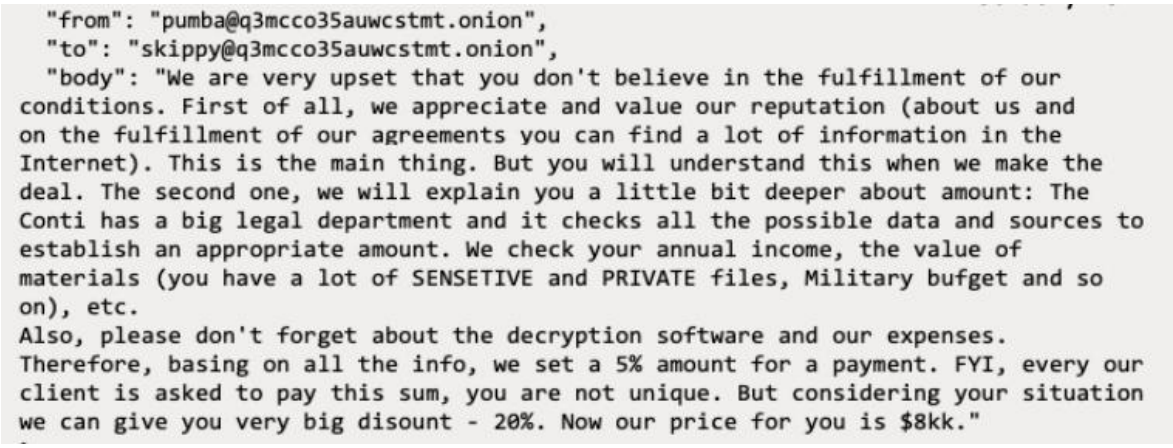
DEFENCE BELONGS TO HUMANS

Data	Attività	Autore
22/04/2022	Stesura del report	Yoroi
29/04/2022	Correzione Errata Corrige a pagina 8, sezione Maze	Yoroi

Indice dei contenuti

Introduzione

Gli attacchi di tipo Ransomware sono ormai una delle principali minacce cibernetiche che ogni organizzazione è costretta ad affrontare. Oltre ad essere minacce molto sofisticate sono realizzate da alcune delle operazioni cyber-criminali di maggiore successo che hanno come obiettivo la scalarità del business di estorsione.
Una conferma della imponente struttura organizzativa da parte delle organizzazioni criminali viene dal dataleak di Conti, noto gruppo ransomware, che ha rivelato l'interessamento di un importante gruppo "legale e finanziario" per la valutazione dell'ammontare dei riscatti.



```
  "from": "pumba@q3mcco35auwcstmt.onion",
  "to": "skippy@q3mcco35auwcstmt.onion",
  "body": "We are very upset that you don't believe in the fulfillment of our
conditions. First of all, we appreciate and value our reputation (about us and
on the fulfillment of our agreements you can find a lot of information in the
Internet). This is the main thing. But you will understand this when we make the
deal. The second one, we will explain you a little bit deeper about amount: The
Conti has a big legal department and it checks all the possible data and sources to
establish an appropriate amount. We check your annual income, the value of
materials (you have a lot of SENSETIVE and PRIVATE files, Military bufget and so
on), etc.
Also, please don't forget about the decryption software and our expenses.
Therefore, basing on all the info, we set a 5% amount for a payment. FYI, every our
client is asked to pay this sum, you are not unique. But considering your situation
we can give you very big disount - 20%. Now our price for you is $8kk."
```

Figura 1. Dataleak del gruppo ransomware Conti

L'importanza di comprendere il funzionamento di questo business per provare a prevenirlo è un passo importante verso la difesa da tali minacce.

Principali osservazioni

Sono molti gli elementi da segnalare nel panorama della criminalità informatica operante attraverso Ransomware, e questi sono i principali:

1. **Metodi di estorsione multipli**. Dal 2019 i metodi di estorsione si sono evoluti notevolmente, dalla richiesta di riscatto per dissequestrare i file presi in ostaggio fino al furto di informazioni critiche e al "public shaming"; le strategie degli attaccanti si sono evolute per mantenere un alto livello di successo nel perseverare con questi attacchi.
2. **Sviluppo di applicazioni *as a service* (*Ransomware as a Service*)**. Lo sviluppo di RaaS ha creato un intero ecosistema nell'underground criminale. Affiliati, fornitori di accessi, associazioni organizzate per la scelta degli "adepti", negoziatori professionisti per richieste di riscatto sempre più efficaci, uffici finanziari per stimarne l'ammontare e infine una sorta di ufficio stampa sempre più integrato con il business del gruppo.
3. **Sviluppo offensivo (Weaponization) della propria tecnologia nella ricerca e sfruttamento di nuove vulnerabilità**. La sofisticata organizzazione che si è creata attorno a questo business illecito ha permesso la formazione di veri e propri gruppi di sviluppo, veloci ed efficaci nell'inserire gli ultimi exploit all'interno dei propri sistemi di compromissione.
4. **Il Business prima di tutto**. Sempre più spesso le cybergang acquistano da "access brokers" gli ingressi delle organizzazioni da attaccare. Un tipo di attività che sottolinea ancora una volta la struttura organizzativa dell'intero mercato criminale affidato a procacciatori, consulenti e uomini d'affari invece che a tecnici informatici. Individui disinteressati alla sfida tecnologica ma solo orientati all'ottenimento del riscatto, indipendentemente dall'intero percorso di attacco, per entrare nei sistemi bersaglio tramite "scorciatoie" veloci.
5. **Nessuna regola è rispettata**: denigrare le vittime, contattarne i clienti, minacciare, sono tutti metodi utilizzati dagli attaccanti che, appartenendo a organizzazioni di grandi dimensioni, vogliono realizzare importanti risultati economici.

Osservando la distribuzione geografica delle richieste di estorsione note da parte delle gang del ransomware, si può notare come le Americhe (principalmente USA e Canada) siano state le principali vittime a livello globale, con l'Europa e l'Australia al secondo e terzo in termini di incidenti.

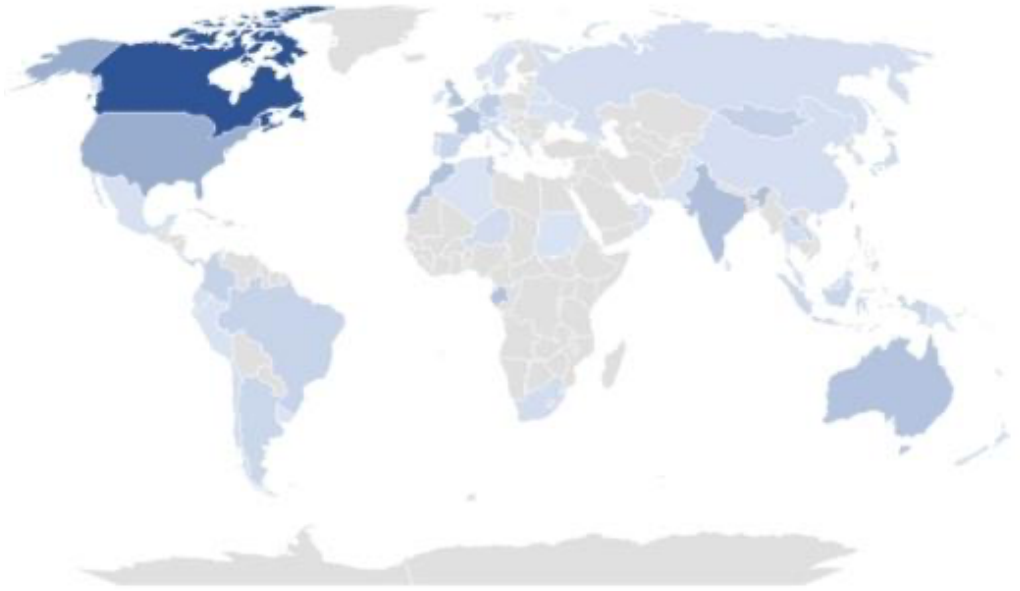


Figura 2. Distribuzione geografica delle richieste di estorsione

Principali attori

Nel periodo di osservazione che va dal 2014 alla fine del 2021 è possibile considerare i seguenti attori criminali come I maggiori responsabili di questi attacchi.

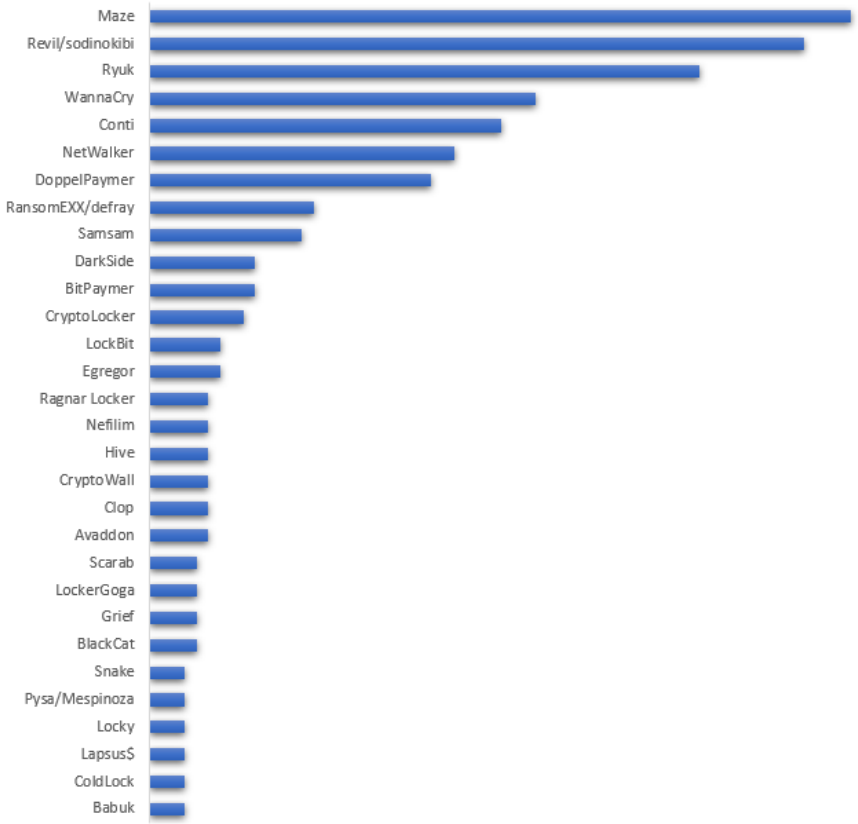


Figura 3. Top 30 Ransomware Groups

Di seguito vengono riportate brevi descrizioni dei gruppi criminali più osservati nel periodo di attività descritto.

Maze

Il gruppo che si cela dietro Maze è noto con i nomi di TwistedSpider e TA2101. Ha iniziato la propria attività criminale intorno a Maggio 2019 ed è diventato famigerato per attaccare grosse compagnie ed enti delle pubbliche amministrazioni, ERRATA CORRIGE PER DIFETTO DI TRADUZIONE[1] ~~tra cui anche l'Agenzia delle Entrate Italiana~~ anche tentando di spacciarsi per l'Agenzia delle Entrate Italiana. Oltre al più noto malware, Maze, nel corso del 2020 è stato osservato l'utilizzo di un altro malware denominato Egregor. Il modo di operare del gruppo spazia dallo sfruttamento di Exploit Kit alle email di Spear Phishing, passando anche per uso di malware IAaaS (Initial Access as a Service) come IcedID.

REvil

Il gruppo REvil è noto anche come Pinchy Spider, ed è conosciuto almeno da Gennaio 2018. REvil è l'evoluzione di un altro ransomware noto con il nome di GrandCrab, uno dei più famosi ransomware diffusi con l'approccio RaaS (Ransomware as a Service). Dopo la dichiarazione di terminazione del progetto di GrandCrab, dismesso alla

[1] Traduzione fatta dal sito https://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us

versione numero 4, il threat actor ha evoluto il proprio business model verso la Double Extorsion con il malware REvil/Sodinokibi. Il loro attacco più famoso è quello alla compagnia di Kaseya compiuto tra Giugno e Luglio 2021.

Ryuk

Il gruppo che si cela dietro Ryuk è noto con gli alias GRIM SPIDER, UNC1878, WIZARD SPIDER, e risulta essere attivo almeno da Agosto 2018. Ha colpito grosse organizzazioni in tutto il mondo chiedendo riscatti per oltre 3B$. È conosciuto per sfruttare le più note botnet come vettore di ingresso nelle aziende vittime e per l'uso di malware come Trickbot, Zloader, Emotet.

Wannacry

Wannacry è un ransomware che si discosta da quelli che abbiamo elencato precedentemente, in quanto sembra essere collegato con gruppi APT, piuttosto che con Threat Actor motivati finanziariamente. In particolare, esso risulta essere legato al gruppo Lazarus, famoso per essere al servizio del governo nord-coreano. È diventato famosissimo nel maggio del 2017 per aver sfruttato gli exploit della famiglia Eternalblue rilasciati dal gruppo hacker ShadowBrokers dopo un attacco all'NSA.

Conti

Il gruppo Conti è uno dei più attivi nell'ultimo periodo ed è noto alla comunità di Threat Intelligence a partire da Luglio 2020. Il gruppo ha abbracciato immediatamente il business model della Double Extorsion, ed è noto anche per la sua solida organizzazione e gerarchizzazione interna, grazie anche a una imponente campagna di affiliazione verso i suoi adepti. Nel corso del tempo sono stati divulgati addirittura documenti e materiali di formazione per le nuove leve in cui spiegava come compiere gli attacchi informatici. A Febbraio 2022 a seguito dell'escalation militare tra Russia e Ucraina, un ricercatore ucraino ha divulgato chat e informazioni sensibili relative al gruppo, tra cui anche il codice sorgente del ransomware. Tuttavia questo non ha fermato il gruppo, che continua ancora a operare e a compiere attacchi di tipo Double Extorsion.

Principali settori colpiti

Analizzando i principali settori colpiti negli anni, si possono individuare tendenze molto affini ai trend socio-politici soprattutto negli ultimi anni. Per esempio, si può osservare come il focus sul settore "healthcare" sia cambiato radicalmente dall'inizio della pandemia da Sars-Cov-19, con un netto incremento dall'anno 2020 proprio nel cuore della pandemia da Covid-19 mentre in passato appariva essere un settore di basso interesse.

Parallelamente, si è riscontrato un notevole incremento di attacchi rivolti alla pubblica amministrazione ed enti governativi a partire dagli ultimi anni, da quando, nello specifico, il cyberspace è diventato ufficialmente il quinto spazio di guerra dopo l'ambiente terrestre, aeronautico, marino ed economico.

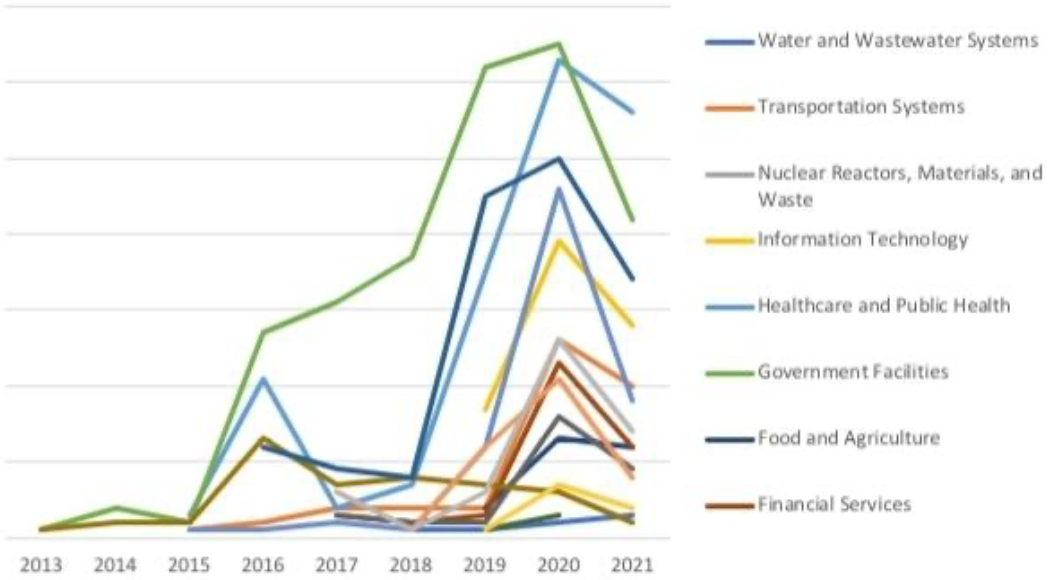


Figura 4. Principali settori colpiti da attacchi ransomware

Attacchi ransomware al settore finanziario sono noti e persistenti nel tempo proprio per la natura di questo tipo di business, particolarmente attrattivo per ogni attaccante in cerca di profitti economici, al contrario degli attacchi ransomware a settori agricoli o affini al "food" rispetto alle variabili di riuscita. Tali settori hanno una filiera di produzione molto significativa in termini di dimensione, e anche per questo motivo soggetti facili da attaccare.

Variazione del riscatto

Ancora una volta possiamo notare, dalla richiesta media di riscatto, l'evoluzione della complessità e del mercato ransomware.
Osservando il seguente grafico, in cui sono presenti 6 fasce di richieste iniziali di riscatto (non di effettivo pagamento di queste ultime), possiamo notare come inizialmente vi sia una netta prevalenza del colore blu (richieste di riscatti da un valore minore di $1.000) mentre mano a mano che ci avviciniamo alla contemporaneità, la fascia blue sparisce lasciando ampio spazio al colore verde (richieste di riscatti superiori o uguali a $5M), azzurro (richieste di riscatto minori di $5M) e giallo (richieste di riscatto minore di $50k).

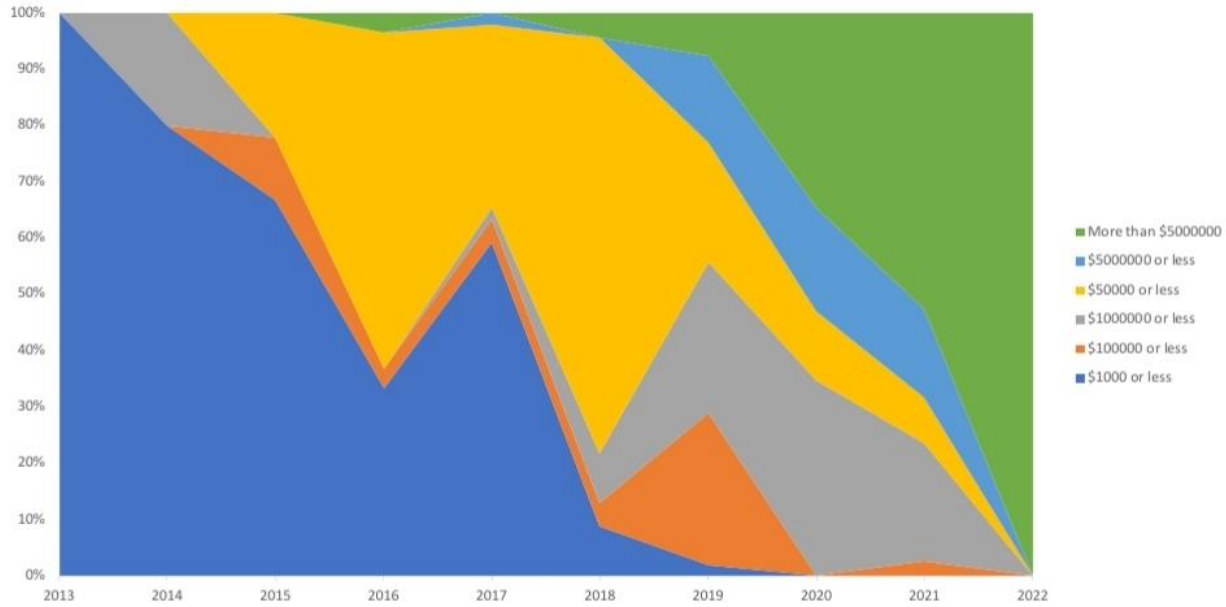


Figura 5. Entità economica delle richieste di riscatto nel tempo

L'incremento di valore economico potrebbe dipendere da due fattori prevalenti:

- La necessità da parte dell'organizzazione criminale di offrire alla propria catena di valore un compenso elevato per restare attrattiva, considerando l'elevato numero di organizzazioni criminali a contendersi affiliati, intrusori, brokers di accessi e negoziatori.
- La consapevolezza da parte degli attori attaccanti, ma anche da parte delle vittime, dell'importanza dei sistemi bersagliati dagli attaccanti e del possibile danno economico degli attacchi stessi.

L'organizzazione della galassia criminale oggi

Nel corso del 2021 sono stati affrontati numerosi attacchi ransomware e attacchi di altissimo profilo ormai noti agli addetti ai lavori con il nome di "Double Extortion". Gli attacchi ransomware sono la minaccia cyber che una qualsiasi organizzazione che conserva dati in formato digitale deve affrontare. Ormai esistono numerosi gruppi criminali che hanno creato dei veri e propri brand per rimarcare la loro supremazia nei confronti dei loro "competitor" nella stessa tipologia di "business".

Sembra anomalo, ma ad oggi conviene adottare lo stesso linguaggio che si usa per le normali aziende anche per questi attori criminali, proprio perché essi si sono strutturati allo stesso modo: una strutturazione complessa con una separazione dei compiti abbastanza rigida, del tutto simile a un'organizzazione aziendale. Ciascun gruppo di Ransomware as-a-service di alto profilo come quelli studiati, ha all'interno del suo organico i seguenti profili:

- I veterani del gruppo che rappresentano il consiglio di amministrazione del gruppo;
- Il gruppo di sviluppatori altamente specializzati nel produrre malware e strumenti di supporto per compiere gli attacchi;
- Esperti penetration tester e red-teamer che compiono le operazioni di intrusione avanzata all'interno delle organizzazioni bersaglio;
- I contabili che sono addetti al riciclaggio del denaro, e particolarmente nel mixing di bitcoin;
- I recruiter che cercano di attrarre persone all'interno del circuito;
- Gli esperti di negoziazione utilizzati per trattare con le vittime e gli eventuali consulenti e agenti di giustizia in modo da estorcere efficacemente i pagamenti;
- Gli esperti di marketing focalizzati a posizionare il brand all'interno della comunità.

Per mantenere un'organizzazione del genere, è necessaria una leadership di alto livello, ma allo stesso tempo, la flessibilità di azione dell'organizzazione deve essere calibrata per essere resiliente nel corso del tempo ad affrontare in maniera opportuna il turnover e le infiltrazione di soggetti sotto copertura.
Questi gruppi criminali ricorrono a diverse modalità per accedere al perimetro aziendale della vittima, sintetizzabili in due categorie:

- Si affidano a "servizi" esterni definibili come "Initial Access as-a-service", forniti, ad esempio, da altri gruppi che stabiliscono accessi silenti e persistenti all'interno dei perimetri aziendali tramite trojan sofisticati, oppure tramite attività di compravendita di exploit adatti a colpire determinate tecnologie;
- Realizzano soluzioni interne di sviluppo di tecniche e procedure per ottenere gli accessi nei confronti degli attaccati.

Tuttavia, già considerando queste complesse relazioni nel mercato underground, non manca spazio all'innovazione e all'evoluzione delle tattiche estorsive finora mostrate. Infatti, ad oggi, la nomenclatura di Double Extortion è diventata famosa proprio per il modo di agire sui due livelli già ampiamente descritti.

Ma non finisce qui.

Abbiamo già osservato e tracciato casi in cui si andava oltre questi livelli di estorsione di minaccia nei confronti delle vittime di questi sofisticati attacchi informatici.
In particolare, nel corso del 2021 abbiamo registrato altri due ulteriori livelli di estorsione, arrivando addirittura a quattro.
Essi sono:

1. Negazione dell'accesso ai file e/o ai sistemi, come da operazione base di attacco ransomware;
2. Minaccia di divulgazione pubblica di dati sensibili aziendali della vittima nella Wall of Shame del sito gruppo ransomware;
3. In caso di mancato pagamento del riscatto, gli operatori minacciano attacchi di tipo Denial of Service, DDoS, sui sistemi della vittima, impedendone o rallentandone il ripristino, grazie al fatto che presumibilmente hanno conservato gli accessi all'interno delle infrastrutture della vittima;

4. Il quarto livello è quello più subdolo dove gli attaccanti minacciano non di divulgare i dati pubblicamente, ma di venderli ad ulteriori attori, che possono essere altri attori criminali o APT che hanno interesse ad avere accessi privilegiati all'interno del particolare perimetro, oppure a competitor per quanto riguarda tutte le dinamiche sempre attuali di spionaggio industriale.

Conclusioni

Sembra abbastanza evidente che affrontare questa tipologia di attacchi va oltre quelle che sono le attività di cyber defence. Occorre quindi osservare il fenomeno da una prospettiva molto più ampia, dove la protezione dell'informazione digitale non è solamente la protezione delle infrastrutture informatiche formate dall'insieme di hardware e software, ma copre anche aspetti relativi all'ambito legale e alle politiche aziendali.
Per quanto riguarda l'Europa, un primo sforzo in ambito di gestione a livello legale per determinate tematiche è stato affrontato nel GDPR, il quale prevede una certa formalizzazione delle problematiche di cyber sicurezza una volta che un'organizzazione deve trattare dati provenienti da clienti di tipo diverso.
Per quanto riguarda le politiche aziendali è necessario compiere ancora significativi sforzi di miglioramento nella gestione della "Cyber-Crisis", che deve prevedere l'intervento congiunto di politiche aziendali e di tecnologie di protezione per la mitigazione degli incidenti.

In definitiva, le attività da Double Extortion sono diventate mainstream.

Quindi, il problema da porsi è come riuscire a gestire in maniera opportuna queste situazioni per affrontare nel migliore dei modi anche i vincoli operativi che necessariamente limitano ogni realtà aziendale, e che possono essere dovute sia alle logiche di business-continuity, sia a limitazioni dell'organizzazione di staff che preveda un team di IT security adeguato.

Le soluzioni sono molteplici e tutte dipendenti dalla strutturazione organizzativa: per esempio, in ambienti aziendali complessi, l'adozione delle best-practice potrebbe tradursi solo in costosi esercizi di rispetto di standard e compliance, seppure questo approccio abbia mostrato limiti significativi nella mitigazione della minaccia. Il dipartimento di sicurezza informatica dovrebbe riuscire a indicare chiaramente le priorità nella protezione, ossia se preferire di investire di più sulla protezione delle informazioni conservate all'interno dell'azienda piuttosto che delle infrastrutture di supporto, o viceversa. Questa non è una scelta dovuta al fatto di preferire un'opzione rispetto all'altra, ma è una constatazione oggettiva dell'ambiente reale dove la protezione informatica perfetta non esiste, per il fatto che il budget da allocare non è infinito.

Rispondere a domande come: "Quanto l'azienda ha investito in controlli di sicurezza preventivi?" - o - "L'azienda sta investendo nel rilevamento e nella risposta?" - o anche - "Quando è l'ultima volta che l'azienda ha rivisto a fondo la sua strategia di sicurezza?" può aiutare molto nel processo decisionale e può essere un utile esercizio di brain-storming che permette di definire le priorità per la difesa perimetrale.

Le strategie di sicurezza informatica possono quindi essere evolute potenziando la preparazione alle crisi informatiche a livello aziendale e i relativi piani di gestione dell'emergenza. Investire in operazioni di sicurezza, tecnologie di rilevamento e risposta come il Cyber Security Defense Center di Yoroi e Kanwa Agents, sfruttando operazioni e servizi maturi di Cyber Threat Intelligence, offre nuove opportunità di riduzione del rischio per l'azienda.

Profilo della società

YOROI è un'azienda che sviluppa e gestisce Sistemi Integrati Adattivi e Dinamici di Difesa Cibernetica e che ha l'obiettivo di giocare un ruolo di primo piano nel settore italiano della difesa cibernetica.
YOROI coniuga da un lato la più solida esperienza del mercato italiano grazie alla recente incorporazione di Cybaze S.p.A. (ex Emaze S.p.A.) e @Mediaservice.net s.r.l due società pioniere del mercato della cyber security in Italia con oltre 20 anni di vita, e dall'altro la vocazione all'innovazione tecnologica più all'avanguardia di Yoroi s.r.l., una realtà che dal 2015 si è rapidamente imposta all'attenzione nazionale ed ha sviluppato tecnologie proprietarie che hanno ottenuto significativi riconoscimenti anche sul mercato internazionale.

L'ultimo passaggio relativo alla crescita e all'affermazione di YOROI come punto di riferimento della Cyber Security in Italia è stato, nel Gennaio del 2021, l'acquisizione della maggioranza del capitale della società da parte di TINEXTA S.p.A.
In questa occasione Yoroi è stata scelta per integrare al suo interno tutte le componenti esistenti del gruppo Cybaze; tutto questo, unitamente alle acquisizioni della divisione progetti, soluzioni e R&D di Corvallis e della maggioranza azionaria di Swascan, ha permesso a TINEXTA di creare un polo nazionale specializzato nei servizi di sicurezza digitale.

YOROI è oggi una compagnia formata da oltre 120 persone e importanti infrastrutture tra le quali ricordiamo:

- 2 Defense Center (Cesena e Benevento), con oltre 40 cyber analisti qualificati
- Una delle principali organizzazioni CERT in Europa, certificata Trusted Introducer: YOROI è la prima società italiana ad avere avuto il riconoscimento del terzo livello "certified". Questa struttura è composta da oltre 10 analisti specializzati e operanti dalle sedi CERT di Cesena e Benevento (Yoroi CERT & Z-Lab)
- Uno dei più importanti team di ethical hacking formato da oltre 20 specialisti tra i più qualificati e riconosciuti sia a livello nazionale che Internazionale
- Un team di grande esperienza di oltre 30 sviluppatori in grado di assistere un'organizzazione nell'approccio di rilevanza strategica "security by design"
- Un team di eccellenza dedicato alla compliance&risk assessment

Il motto di YOROI è **"Defence Belongs to Humans"**

Questa frase sintetizza quello che esperienza e competenze in YOROI hanno portato a riconoscere come approccio fondamentale per ridurre significativamente il rischio dei danni provocati dagli attacchi informatici ed essere pronti a reagire immediatamente in caso si verifichino: la centralità dell'analista esperto, armato delle tecnologie più all'avanguardia. Il nostro credo è che fino a quando dalla parte di chi attacca ci sarà un essere umano con dei precisi obiettivi, a prescindere da quanta tecnologia possa essere messa in campo, soltanto un altro essere umano potrà essere in grado di intuirne o anticiparne proattivamente le mosse, per ridurre ad un rischio accettabile il rischio cyber.

In YOROI riteniamo che per implementare un sistema efficace di difesa cibernetica a protezione di un'organizzazione sia indispensabile:

- La comprensione del suo modello di business

- La conoscenza approfondita delle specificità e delle dinamiche del settore nel quale opera

- L'equilibrio fondamentale tra tre fasi: Predizione -- Prevenzione – Reazione/Proazione

Atteggiamento generale verso i Clienti e il Mercato e Postura del Servizio di Difesa

Yoroi desidera evidenziare tra gli argomenti differenzianti rispetto alla maggioranza del mercato, i seguenti fattori:

- L'atteggiamento di YOROI non è critico nei confronti delle scelte fatte dall'azienda Cliente in termini di spiegamento dell'arsenale difensivo contro le minacce informatiche; il principale scopo è quello di dare a quell'arsenale, integrandolo dove è necessario, dignità di sistema per contribuire al raggiungimento di un efficace livello di difesa, la più alta resilienza possibile agli attacchi e la mitigazione delle eventuali minacce riscontrate nel minor tempo possibile, anche in virtù del rispetto delle normative vigenti.
- È cura di YOROI segnalare, come contenuto delle relazioni conclusive dei servizi prestati, eventuali inadeguatezze e mancanza di efficacia delle difese messe a protezione dell'azienda.
- Yoroi ha sviluppato internamente tecnologie proprietarie, che utilizzano strumenti di Artificial Intelligence e Machine Learning all'avanguardia e non basa la propria attività sulla vendita di soluzioni di sicurezza "convenzionali" come, ad esempio, firewall, antivirus, antispam, proxy, SIEM ecc.
  In un'ottica di consulenza strategica, YOROI verificherà l'adeguatezza e l'efficacia degli strumenti presenti presso il Cliente e fornirà un completo resoconto di quanto riscontrato accompagnato da spunti e riflessioni sempre mirate alla mitigazione.
- Il servizio di difesa proposto da YOROI è in grado di interfacciare i propri sistemi (a vari livelli) con le principali soluzioni reperibili sul mercato sia open source sia proprietarie dei principali brand. Il diverso livello di integrazione dipende dalle capacità di dialogo offerte dagli strumenti terzi (via API, presenza e disponibilità di LOG di sicurezza (SysLOG), ecc.). I servizi sono erogati attraverso private cloud e sono basati sulle seguenti componenti e funzionalità:
  - ricerca e raccolta di segnalazioni di allarme della sonda proprietaria che sarà posizionata presso i diversi punti di accesso ad Internet dell'infrastruttura del Cliente. La sonda normalmente viene installata in ambiente virtualizzato ma è disponibile anche in versione appliance.
  - Pre-processing delle informazioni raccolte a cura della sonda da tutte le componenti presenti presso il Cliente in termini di Firewall, Soluzioni Anti-Spam e Proxy e altri strumenti di sicurezza.
  - Correlazione degli eventi di sicurezza riscontrati e raccolti mediante integrazione di soluzioni già in campo.
  - Ulteriori analisi, attraverso anche il passaggio delle componenti potenzialmente pericolose nella soluzione Multi-SandBox YOROI.
  - Presentazione delle informazioni raccolte e stato della rete attraverso un completo cruscotto informativo.

Capacità di Analisi e innovazione finalizzate alla Sicurezza dei Clienti e dei loro asset

Grazie all'integrazione con Mediaservice.net, azienda torinese dalla grandissima e rinomata esperienza nell'erogazione di servizi di analisi e audit di infrastrutture e perimetro applicativo aziendale, YOROI ha realizzato un servizio di Security Audit che combina in un'unica attività le discipline di Penetration Test e di Risk Assessment. La caratteristica discriminante di questo servizio è la forte interazione tra le due tipologie di verifica, che permettono principalmente di:

- ottimizzare le attività di penetration test, razionalizzando gli effort sulle attività di verifica e pesando al meglio le vulnerabilità;
- migliorare la precisione della rilevazione del rischio e della successiva mitigazione, includendo un livello di dettaglio tecnico.

Le attività di Risk Assessment prevedono l'applicazione di metodologie internazionali consolidate, in conformità agli standard ISO/IEC 27001:2005 e ISO/IEC 27005:2008, con la possibilità di valorizzazione qualitativa o quantitativa (in euro) dei rischi.
La metodologia OSSTMM, punto di riferimento decennale in materia e ampiamente richiesta a livello nazionale e internazionale, è la metodologia utilizzata per le attività di Penetration Test.

La sua applicazione è eseguita su ciascuno dei cinque canali previsti (TLC, reti di dati, wireless, accesso fisico e personale) a seconda delle necessità di sicurezza rilevate.

Grandi capacità di Ricerca e Sviluppo messe al servizio dei principali Service Provider

La fusione di Cybaze in YOROI ha portato in dote uno dei gruppi di Ricerca e Sviluppo più importanti in Italia, autore di soluzioni software progettate in base alle esigenze dei Clienti per risolvere specifici problemi strettamente legati a problematiche inerenti alla sicurezza.
In particolare, è possibile citare il progetto DCS (Device Check and Support) tramite il quale i nostri Clienti possono, tramite un'unica interfaccia, controllare e modificare i file di configurazione dei router della propria rete, di decine di migliaia di dispositivi di diversi modelli e produttori. Nel corso degli anni il team Ricerca e Sviluppo è stato autore di numerose altre soluzioni diventate un must per i grandi provider e, tra queste, possiamo ricordare il servizio "Rete Sicura" offerto da Vodafone. Inoltre, sono state rilasciate nel tempo altre soluzioni come DeCo, Rectify, Descover e ConCreTo.
Il portafoglio di soluzioni sviluppate dal centro di Ricerca e Sviluppo YOROI è completato da realizzazioni personalizzate su specifiche esigenze dei Clienti relativamente a provisioning, assurance, raccolta KPI, monitoring e predictive analysis.

Preziose competenze nella Formazione

Grazie alle solide competenze maturate nel tempo, all'esperienza sul campo e alla continua attività di difesa da un lato e di analisi dall'altro, YOROI è tra le poche realtà del mercato in grado di offrire un programma formativo di alto livello. L'offerta formativa è composta, principalmente, dai seguenti moduli: Sicurezza delle Informazioni, ricadute Aziendali del GDPR, Gestione del rischio (Security Compliance), Centralità del D. Lgs.231/01, Informazion Security Awareness e OSSTMM Professional Security Tester (OPST).

Registrazioni e Certificazioni

Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University

TF-CSIRT
Trusted Introducer

LINK

Yoroi S.r.l.
www.yoroi.company - info@yoroi.company

Piazza Sallustio, 9
00187 – Roma (RM)
+39 (051) 0301005