TINEXTA CYBER

CYBERSECURITY ANNUAL REPORT 2022

DEFENCE BELONGS TO HUMANS

Indice dei contenuti

Introduzione

Il 2021 è stato un anno all'insegna della continuità sotto il profilo delle minacce cyber rispetto all'anno precedente. Come abbiamo osservato durante il 2020, le strategie adottate dagli avversari si sono consolidate sugli schemi già analizzati nel precedente report annuale. L'evoluzione della struttura organizzativa appartenente a gruppi criminali, operanti nel digitale, si avvicina sempre più alla struttura organizzativa di complesse organizzazioni criminali operanti nel dominio fisico. Questo ha permesso ai criminali di raggiungere un grado di efficienza e di maturità mai osservato precedentemente. Tali condizioni hanno reso la "fabbrica del malware" un'entità prolifica e funzionale agli obiettivi malevoli delle organizzazioni stesse.

Dalle osservazioni in essere possiamo affermare - senza ombra di dubbio - che la tendenza da parte di attori criminali, intuita e descritta nel corso dei report annuali precedenti ove abbiamo descritto la presenza di gruppi dedicati denominati "Dark Teams", ha avuto una spiacevole conferma.
Il proliferare di gruppi criminali denominati "Double Extortion" e il rispettivo spasmodico miglioramento organizzativo ne sono la principale testimonianza.
Uno dei casi più eclatanti risulta essere quello di LockBit, il quale ha effettuato una operazione di rebranding, paragonabile a quelle attuate da organizzazioni tradizionali per rilanciarsi nel proprio mercato, dando vita a LockBit 2.0. Il fatto sorprendente della strategia di "marketing" adottata dal gruppo criminale è concentrato nella proposizione di confronto con altri gruppi criminali paragonati a "competitor", evidenziando una sorta di supremazia tecnologica nei confronti degli altri attori. Tale operazione è servita come polo attrattivo verso la loro cerchia di affiliati, ottenendo una crescita significativa di nuovi collaboratori. Altri attori criminali, invece, hanno deciso di portare ad un livello successivo la pratica delle estorsioni, creando ulteriori di livelli di pressione sociale sulle vittime, che approfondiremo in seguito.

Il 2021 è stato un anno di conferma della proliferazione e soprattutto dell'impatto che attacchi alla Supply Chain possono avere nei confronti di organizzazioni strutturate. L'attacco alla "catena di fornitori" prevede un cambio di paradigma significativo dove al posto di colpire direttamente il bersaglio prefissato, i criminali digitali prendono di mira un fornitore di servizio della vittima, attaccandolo o sfruttando altre tipologie di vulnerabilità presenti nella sua rete. Una volta ottenuto l'accesso alla struttura del fornitore, essi sfruttano accessi diretti e/o indiretti (spesso di natura reputazionale) all'infrastruttura della vittima reale passando, spesso, inosservati. Il caso più eclatante è stato quello delle backdoor chiamate Sunburst e Supernova, riportate entrambe nell'annual report precedente, dove, per compromettere determinati bersagli altamente protetti, hanno deciso di colpire l'azienda Solarwinds e uno dei loro principali prodotti Orion, per poi compromettere alcuni bersagli di alto spessore. Direzionare gli sforzi per effettuare un attacco digitale verso un fornitore di servizi può essere estremamente più efficace in quanto le misure di sicurezza potrebbero essere inferiori se confrontate con quelle dell'organizzazione target. Questo metodo di attacco aumenta notevolmente la superficie di attacco e conversamente l'area da difendere per ogni organizzazione che ora non può limitarsi alla difesa del proprio perimetro.
Sfortunatamente ulteriori conferme di questa tendenza arrivano nel 2021 con attacchi a compagnie e prodotti software ampiamente adottati, come ad esempio "Kaseya", "ua-parser-js" e non per ultimo "Log4J".

Oltre alla supply chain non sono tramontati attacchi di tipologia opportunistica, come botnet ed email di spam. La prevalenza di questi vettori di infezione non accenna a diminuire ed il continuo perfezionamento delle infrastrutture criminali permette loro di continuare ad agire. Questa tendenza è confermata, ad esempio, dal ritorno della minaccia Emotet, la cui rimozione era stata annunciata agli inizi di gennaio 2021, ma che in realtà si è rivelata essere non più di un semplice "stop and go" riprendendo le attività malevole a metà novembre 2021.
In questi casi, gli sforzi di Yoroi e del team di Threat Intelligence si sono concentrati sul tracciamento delle campagne intercettate, fornendo così un maggiore grado di protezione ai clienti anche attraverso meccanismi proattivi già ben strutturati.

I dati del rapporto

Una delle caratteristiche più importanti del Cyber Security Annual Report di Yoroi riguarda i dati. I dati grezzi utilizzati non appartengono all'open source intelligence (OSINT) o alle rilevazioni di reti esterne, ma piuttosto a incidenti reali che sono stati gestiti da analisti umani. Infatti, l'OSINT potrebbe contenere molti falsi positivi o non essere rappresentativo per un'area geografica, mentre le rilevazioni di reti esterne potrebbero essere facilmente bloccate da protezioni perimetrali come: NG-x, Proxy, Antivirus, Anti-Spam ecc.

I dati utilizzati in questo rapporto, invece appartengono ad incidenti realmente accaduti.

Mentre riportare statistiche sulle tendenze generali utilizzando i dati di rete e OSINT è interessante per avere una panoramica generale dei cyber attacchi, avere statistiche su incidenti reali potrà aiutare il lettore ad essere maggiormente incisivo nel contrasto alle minacce. I dati utilizzati sono stati estratti da incidenti gestiti al fine di adattarsi meglio alla realtà dei reali attacchi di cyber security e di come hanno colpito i verticali di business analizzati.

Sezione 1:

Malware

Il volume del codice malevolo intercettato dalla tecnologia Yoroi è in costante crescita rispetto agli anni precedenti. Inoltre, le informazioni ottenute, studiando a livello strategico le TTP degli attaccanti, suggeriscono una più netta suddivisione tra attacchi di tipo opportunistico ed attacchi di tipologia mirata. Infatti, attacchi *targeted* (ovvero di tipologia mirata) hanno registrato un ulteriore avanzamento nella sofisticazione e nella precisione della somministrazione di malware: basti pensare a quello che sta accadendo nel fenomeno sempre più grave della Double Extortion, che sta riscontrando evoluzioni sempre più drammatiche, così come approfondito nel paragrafo 4. Tale fenomeno vede la formazione di gruppi organizzati in vere e proprie gang cresciute sia di numerosità che di complessità fino alla realizzazione di malware univoci per ogni attacco, quasi a rappresentare una firma indelebile dell'attaccante.
Oltre al fenomeno degli attacchi altamente organizzati per colpire un target noto, anche nell'anno trascorso abbiamo osservato e analizzato attacchi di tipo opportunistico e distribuiti in larga scala, così da colpire quante più aziende e persone possibili. Il ritorno meno atteso, ma più devastante per le aziende Italiane, è stato senza dubbio Emotet, il quale pareva essere stato "spento" attraverso una nota operazione di polizia inter-governativa ad inizio 2021 ma che poi ha rivisto una nascita pochi mesi dopo.

I malware zero-day

La telemetria offerta dalla piattaforma Yoroi ha permesso di estrarre una serie di statistiche riguardo attacchi di tipo "zero-day Malware", ovvero Malware non noti alle firme dei sistemi antivirus. Tuttavia, essere dei Malware "non noti" non significa affermare che essi siano completamente invisibili ai sistemi di protezione: significa piuttosto che essi non sono presenti tra le minacce note delle basi di dati dei sistemi di difesa. Quindi, attraverso strumenti opportuni è possibile classificare la legittimità di un artefatto sospetto. La tecnologia di Yoroi permette di analizzare un vasto numero di artefatti e stabilirne la validità. Il processo definito permette a Yomi, la nota Sandbox di Yoroi, di segnalare eventuali file dannosi rilevati attraverso avanzati strumenti di analisi Malware automatizzati. Parallelamente, le appliance di rete permettono di intercettare sia i payload sia i pattern di comunicazione malevoli che tentano di diffondersi in rete. Tale processo permette di bloccare quanto le prima le minacce sul nascere.
Le informazioni provenienti dall'insieme delle tecnologie Yoroi consentono di creare statistiche rappresentative del campione osservato e di compiere analisi predittive che consentono di ottimizzare la protezione della nostra base utenti. Durante questo processo, come parte della pipeline di analisi automatica, Yomi Sandbox controlla e segnala se i file dannosi sono potenzialmente rilevati dalle tecnologie antivirus nel momento specifico in cui il Malware viene diffuso nell'organizzazione di destinazione. Questo fornisce una visione preziosa di come il Malware Zero-Day si evolve nel tempo e di come si propaga in modelli di business differenti.
In particolare, grazie alle appliance di rete e ai sistemi di telemetria, riusciamo ad implementare un processo che permette la rilevazione di minacce 0-day (zero-day Malware) sul nascere, ovvero minacce che non hanno firme note studiate appositamente per effettuare il "bypass" di strumenti di protezione tradizionali. Il seguente diagramma mostra la classificazione delle minacce "malware Zero" e "Malware N-day" intercettate dalla tecnologia Yoroi nell' anno 2021:

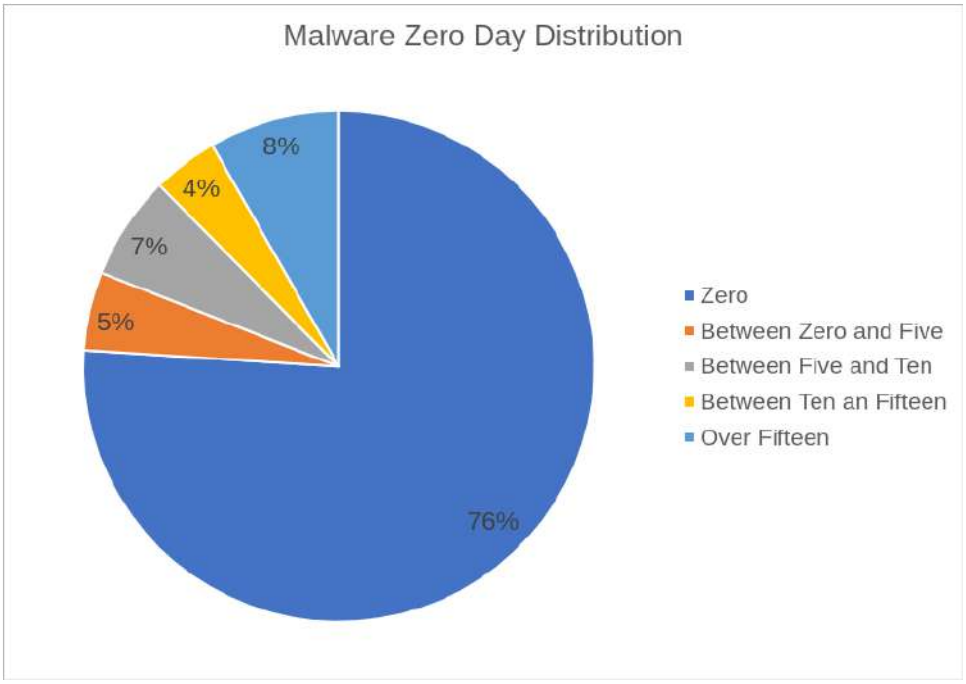

Figura 1. Distribuzione tipologie di Malware

I dati estratti durante l'anno di riferimento presentano una distribuzione in linea con quella degli anni precedenti. Possiamo quindi affermare che il 76% delle minacce Malware attuali sono di tipo 0-day, ovvero possiedono caratteristiche univoche rispetto alla famiglia di appartenenza. Questo non significa che essi siano scritti completamente da zero, ma vuol dire che gli sviluppatori hanno avuto la capacità di creare una Fabbrica di codice malevolo (Malware Factory), sfruttando tecniche di metamorfismo e polimorfismo, che ormai contraddistinguono la totalità dei Malware. La tipologia di Malware 0-day ha sicuramente maggiori possibilità di riuscire ad oltrepassare le difese perimetrali rispetto ad artefatti malevoli noti.
Gli sforzi compiuti dagli attori criminali consistono pertanto nel creare vettori di attacco sempre più evasivi, mutando forma e funzionalità degli stessi, a ogni iterazione o in ogni stato di avanzamento di attacco.
Il restante 24% dei Malware osservati è distribuito in modo uniforme sui motori che ne effettuano il detection. Questo dato si discosta dal report precedente ove la numerosità dei sottoinsiemi era assai differente. Tale informazione mostra che i sistemi tradizionali AV basati su signature statiche e su signature dinamiche tendono a un miglioramento che via via negli anni raggiunge un valore asintotico.
Un'ulteriore grandezza da tenere in considerazione è la classificazione degli zero-day Malware, ovvero comprendere come tali Malware sono distribuiti su tipologia di artefatto.

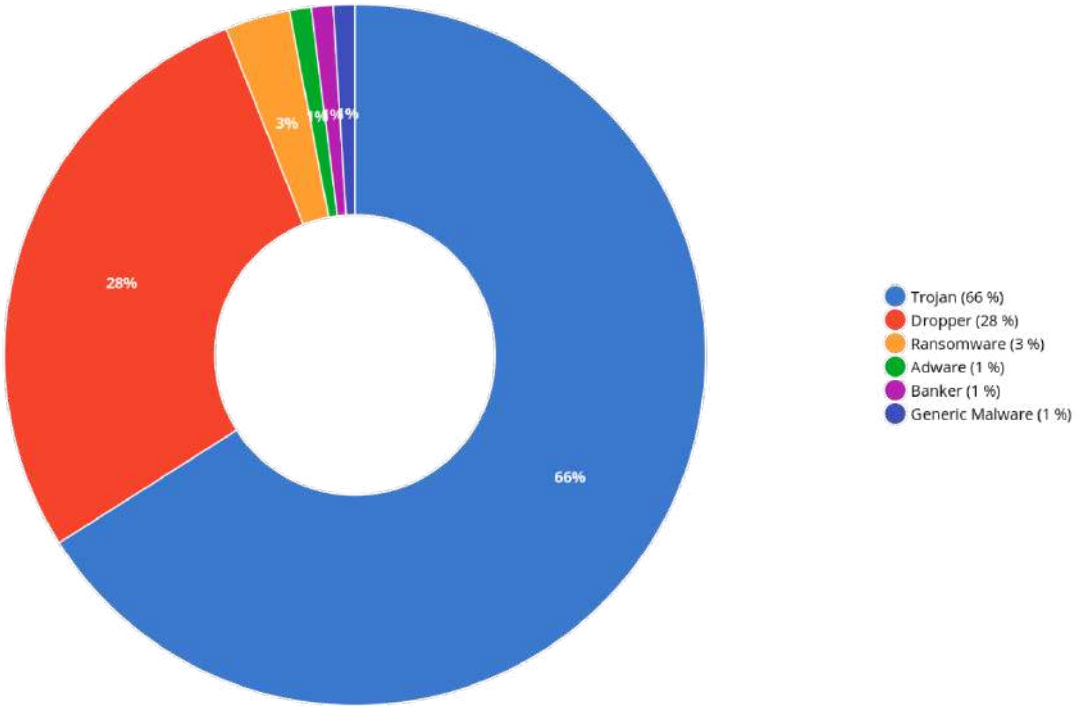

Figura 2. Tipologie di minacce 0day

Come possiamo notare dalla Figura 2. Il 66% dei Malware zero-day è classificabile come Trojan ed il 28% come Dropper. Tale dato conforta l'osservazione precedente. Di fatto Trojan e Dropper appartengono al primo step della catena di attacco e per questo motivo necessitano di essere "trasparenti".
Non sorprende poi che la mole di campioni intercettati di Trojan e Dropper sia di gran lunga superiore a quella dei ransomware, che ricopre un piccolo 3% dei rilevamenti, poiché, come ampiamente discusso, il rilascio del ransomware risulta essere una delle ultime fasi di un attacco informatico.

I settori colpiti

Comprendere chi sono i propri avversari aiuta notevolmente l'analista ad orientare le difese aziendali. Per questo motivo risulta molto interessante lo studio della distribuzione delle famiglie di Malware rispetto ai settori di business. Parallelamente a tale studio è possibile inferire quali settori siano più soggetti ad attacchi e quali settori lo siano meno, oppure desumere quali settori siano maggiormente difesi rispetto ad altri. Grazie all'utilizzo di sorgenti interne ed esterne, Yoroi ha rilasciato un nuovo servizio (approfondito nella sezione 5) attraverso il quale è possibile studiare il grado di esposizione di una determinata organizzazione. Tale strumento risulta essere di primaria importanza in un contesto come quello attuale in cui gli attacchi alla "catena di produzione" si presentano in costante ascesa.
La seguente illustrazione rappresenta la distribuzione delle aziende colpite da attacchi informatici nel corso dell'ultimo anno:

Figura 3. Distribuzione attacchi su verticali

Come si evince dalla Figura 3, la distribuzione degli attacchi è molto variegata e copre, senza particolari problematiche, l'intero corso dell'anno. Abbiamo alcuni settori, in particolare quello relativo ai servizi finanziari e quello della produzione di macchinari, che presentano una vista "più costante" rispetto ad altri settori.
I principali motivi collidono nello scopo di attacco.
Ogni settore specifico porta in dote un motivo di attacco differente, per esempio: per i settori finanziari, il "driver" principale dell'attacco è la motivazione economica. Organizzazioni operanti nel settore finanziario da un lato sono fortemente oggetto di attacchi ma parallelamente sono anche organizzazioni dotate dei più elevati standard di sicurezza, proprio per scongiurare perdita di reputazione e/o fuga di denaro dalle casse dei propri clienti.
Per quanto riguarda i settori di produzione di macchinari, il contesto è abbastanza diverso. Di fatto l'obbiettivo degli attaccanti è racchiuso nella capacità di sabotare il lavoro in modo da poter procedere con un successivo ricatto ideologico.

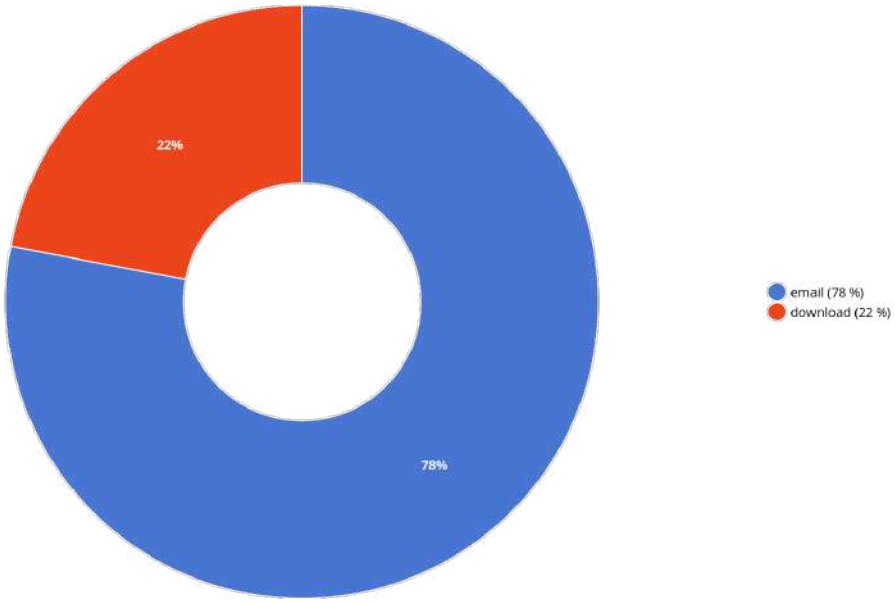

Figura 4. Distribuzione attack vectors

Il phishing e lo spear phishing sono i vettori più adottati nel 2021 come inizio di una catena di attacco.
A differenza dell'anno precedente, è stato osservato un aumento repentino del "drop and execute" con la conseguente adozione di attività di "Download" di componenti malevoli.
In questo contesto, è possibile osservare un cambio di tendenza registrato rispetto agli anni precedenti. Tale cambiamento si manifesta attraverso il differente approccio da parte degli attaccanti di allegare link a file malevoli piuttosto che allegare direttamente i file stessi nella e-mail (o messaggistica). L'utilizzo di Content Delivery Network, come per esempio (ma non limitato a) Discord, Google Drive, Microsoft Onedrive e pasties vengono utilizzati come repository di payload malevoli rendendo ancora più difficile il corretto riconoscimento. L' attuale inefficacia di sistemi perimetrali come Firewall o Proxy/Gateway nella corretta classificazione e conseguente rimozione di file dannosi, associata alla continua curiosità dell'individuo che imperterrito vuole soddisfarla aprendo link e documenti senza troppe remore, continua ad agevolare la proliferazione di tali Malware all'interno delle nostre realtà aziendali.

Diffusione e Movimenti Laterali

Il manuale del "buon aggressore digitale" prevede come seconda fase di attacco l'espansione nel contesto aziendale. A seguito di una prima intrusione, l'attaccante necessita di espandere il proprio dominio il più possibile invadendo la rete della vittima. Tale attività permette all'aggressore di raggiungere il più elevato numero di risorse possibile e, di conseguenza, di massimizzare il suo profitto, in caso di estorsione, o di aumentare il livello dominio, in caso di spionaggio o distruzione.
Parallelamente, aggressori motivati finanziariamente, necessitano di massimizzare i propri guadagni aumentando il numero di vittime e al contempo riutilizzando simili artefatti malevoli. Per questo motivo risulta interessante studiare la propagazione delle minacce in differenti settori di business.
Le metriche relative alla durata e alla propagazione sono calcolate attraverso strumenti di monitoraggio continuo offerti dalla soluzione Yoroi denominata Cyber Security Defence Center.
Comprendere l'andamento delle minacce, ovvero la loro propagazione da un verticale di business all'altro, aiuta gli analisti a prevedere attacchi e offre la possibilità di orientare strumenti di difesa attiva.

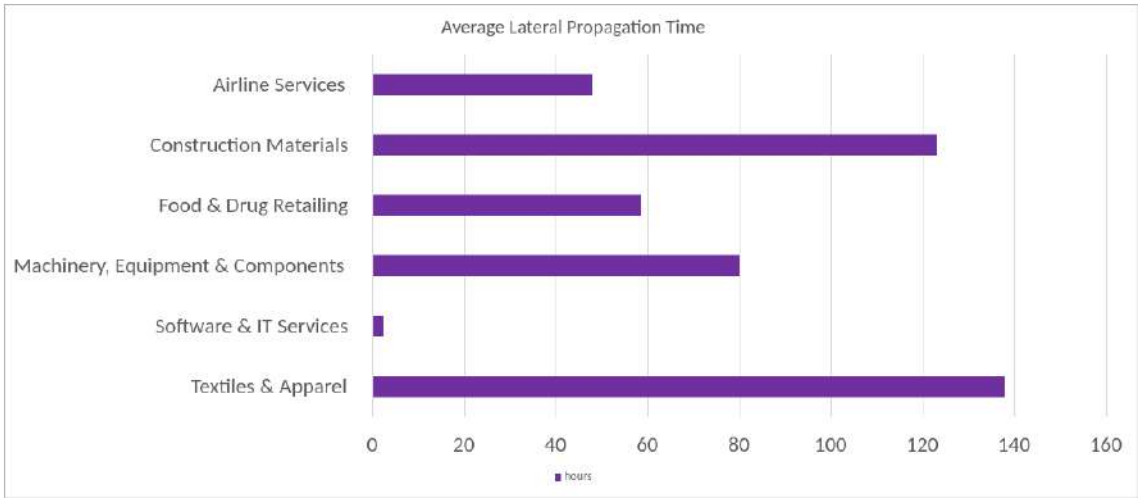

Figura 5. Tempi medi di propagazione laterale

La Figura 5 mostra i tempi medi di propagazione raggruppati per verticali di business.
La chiave di lettura del grafico è molto semplice e dipendente dal contesto. Maggiore è la complessità di rete, tipica di organizzazioni "poco digitalizzate" o di organizzazioni di ampie dimensioni strutturate nel tempo (Textiles and Apparel, Construction Materials, Machinery Equipment and Components), maggiore è l'impegno richiesto da parte dell'attaccante sia in fase di discovery che in fase di propagazione. Per questo motivo i tempi di propagazione su tali organizzazioni risultano nettamente superiori rispetto ai tempi di movimento laterale su organizzazioni più digitalizzate come per esempio (ma non limitato a): Software and IT Service e Airline Service. La media di

propagazione dei 5 settori di riferimento è di circa 10 giorni uomo. Questo dato risulta significativo sia per il team IT che per quello cybersec.

Malware Operations nel contesto italiano

La complessità degli odierni strumenti di delivery di codice malevolo ha offerto agli attaccanti la possibilità di realizzare processi automatici sempre più sofisticati e difficili da essere individuati. In questa sezione viene rappresentata la situazione sull'area geografica italiana, realizzata attraverso l'analisi dei risultati della telemetria raccolta dalla tecnologia Yoroi e grazie alle numerose operazioni di Cyber Threat Intelligence.

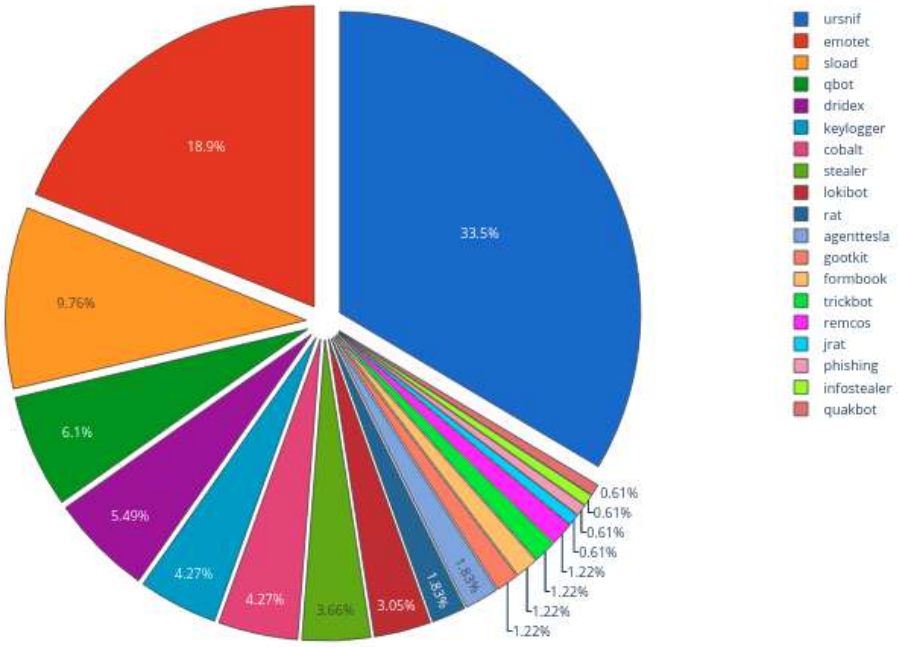

Figura 6. Distribuzione delle principali famiglie di minacce tra le ondate di attacchi malware nel 2021

Anche quest'anno, proprio come evidenziato l'anno scorso, la maggioranza di Malware presenti nelle organizzazioni sono di tipologia Trojan Bancari. Il principale vettore di ingresso è rappresentato da Ursnif con una presenza del 33.5% sul totale e la presenza di Emotet per il 18.9% dei campioni. Tali Trojan sono vettori di ingresso, poi ampiamente utilizzati per installare impianti malevoli di varia natura. La modesta presenza di Emotet, se confrontata sul 2020, è giustificata dall'imponente operazione di "takedown" effettuata a Gennaio del 2021, la quale è stata in grado di rallentare drasticamente la diffusione ma non la totale presenza sul panorama internazionale.
Ursnif si conferma come primaria minaccia da affrontare all'interno del panorama cibernetico italiano. Nel corso degli anni Ursnif ha costantemente aggiornato le tecniche di consegna del payload, grazie ad un'affascinante creatività nelle sue campagne di phishing. Esse vengono attivate da social engineering per poi proseguire su fogli di calcolo al fine di giungere all'utilizzo di payload sviluppati in PowerShell, macro XML spesso nascoste in immagini steganografate. Ursnif risulta essere uno dei pochissimi Malware che mantiene una certa costanza di propagazione rispetto agli ultimi 5 anni in analisi. Tale persecuzione temporale potrebbe essere la risultante di numerosi operatori affiliati, di origine italiana, al gruppo criminale tracciato come TA544. In genere, altre minacce, nel corso degli anni seguono un pattern discreto, ovvero vedono tempi di stop più o meno lunghi, prima di ripartire con costanza.
Emotet, secondo classificato nella nostra classifica, presenta tale caratteristica. Come analizzato nel report dell'anno precedente, a gennaio 2021 un intervento congiunto di forze dell'ordine proveniente da più Paesi ha permesso di inibire la minaccia informatica. Tuttavia, quello che gli eventi ci hanno mostrato, è che Emotet ha avuto solamente una fase di riassestamento, il che significa che le persone arrestate in realtà erano solo una

piccola parte dell'intera organizzazione che si nasconde dietro la minaccia. Emotet ha adottato uno schema di consegna più uniforme: usualmente, l'infezione si avvia attraverso script dannosi o file di documenti macro-abilitati.
Le e-mail dannose in genere contengono un marchio familiare, con il logo "Microsoft Office 365", progettato per assomigliare ad un'e-mail legittima e cercano di convincere gli utenti a effettuare "clic" sul file dannoso utilizzando come contenuto un tema di attualità come per esempio: "La tua fattura", "Comunicazione COVID-19", "Dettagli di pagamento" oppure attività inerenti alla spedizione di un pacco imminente, da parte di comuni organizzazioni di trasporto. Dopo aver abilitato le macro, uno script PowerShell inizia a scaricare il componente dannoso: (tipicamente) una DLL da siti Web precedentemente compromessi, con URL personalizzati appositamente creati per la campagna di attacco.
Il terzo classificato risulta essere sLoad con il 9.76%. Esso è una delle poche famiglie di Malware che sfruttano le comunicazioni PEC per infettare le postazioni di lavoro sensibili: questo è un ottimo mezzo per sfruttare la social engineering, in quanto la vittima ritiene che la posta sia stata precedentemente convalidata dall'autorità di certificazione. In realtà, la posta certificata contiene spesso un archivio zip malevolo contenente un file Script Visual Basic dannoso, che scarica dalla rete ed esegue ulteriori script Powershell. La particolarità di sLoad è la fase iniziale di appoggio, in cui lo script Powershell raccoglie informazioni sulla macchina vittima e solo dopo quella fase di ricognizione, il vero payload (dannoso) viene scaricato ed eseguito nel momento in cui l'attore criminale è cosciente della possibilità di raggiungere il risultato desiderato.
Una nuova posizione di rilievo per quanto riguarda il panorama cyber italiano risulta essere occupata da QBot con il 6.1% delle infezioni registrate. Esso è un altro noto Malware bancario, che fino a qualche tempo fa non era molto diffuso in Italia. Esso ha lo scopo molto simile a quello di Emotet, con la creazione di una sofisticata botnet a supporto e che a un certo punto dell'infezione può scaricare anche backdoor molto usate come Trickbot e CobaltStrike.
Trickbot e Cobalstrike sono ad oggi gli strumenti numero uno di supporto per i criminali informatici per quanto riguarda le operazioni di Red Team e di intrusione più sofisticata. Essi sono i mezzi più malleabili e usabili in ogni occasione e che tutto sommato adottano numerosi gruppi di Double Extortion per compiere le operazioni di privilege escalation e di movimenti laterali.
Altre minacce costanti nel panorama italiano sono i Malware info stealer, come Lokibot, AgentTesla e altri. Questo tipo di Malware può essere utilizzato sia come strumento per attacchi opportunistici sia per attacchi mirati. Nel primo caso, i gruppi criminali informatici sfruttano tali strumenti al fine di creare basi di conoscenza per eseguire frodi o altri tipi di attacchi come per esempio il credential stuffing. Contrariamente, quando sono utilizzati per attacchi mirati, gli aggressori sfruttano tali componenti per compiere operazioni di ricognizione, dove è fondamentale ottenere le informazioni sull'infrastruttura della vittima e possibilmente anche recuperare le password di alcune utenze.

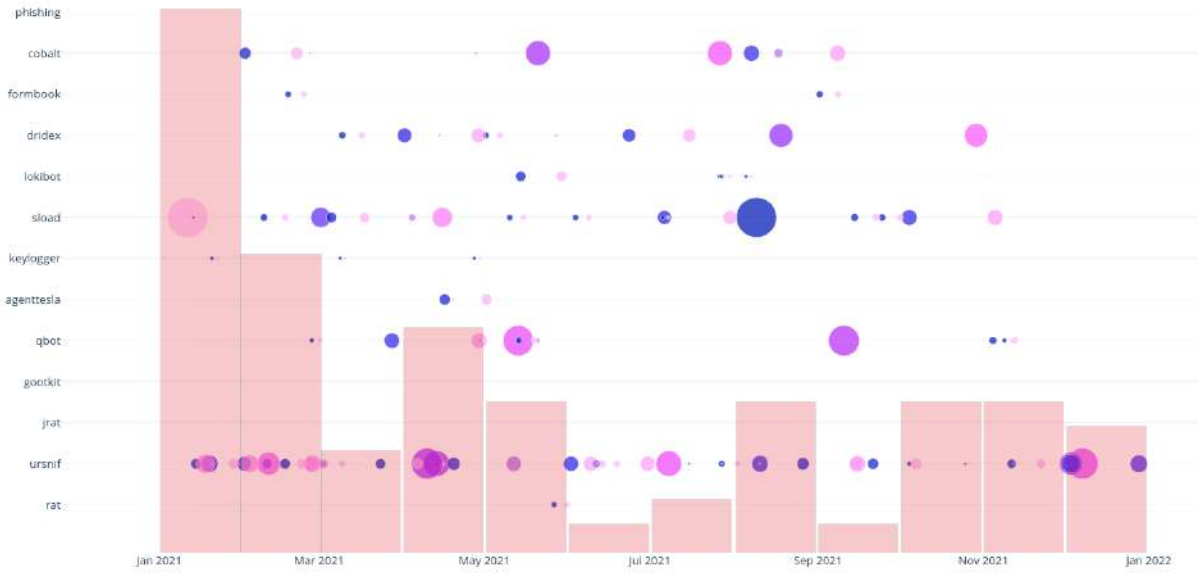

Figura 7. Campagne malware in Italia

Sezione 2:

Minacce bloccate

La prevenzione è una delle operazioni più complesse in ambito cyber defense in quanto esiste una numerosa varietà di incognite da tenere in considerazione nella gestione del compromesso tra usabilità da parte degli utenti e protezione dei sistemi informativi. È necessario inoltre calibrare e gestire in maniera opportuna tutta la mole di indicatori di compromissione che quotidianamente emerge nel panorama cyber. La vera sfida per gli analisti e per i progettisti del sistema di protezione è quella di garantire un giusto livello di usabilità per gli utenti ed un'elevata sicurezza in termini di blocchi preventivi.
Per questo motivo Yoroi ha investito per progettare e implementare una tecnologia di DNS Defense che sia quanto più all'avanguardia possibile per il monitoraggio e il blocco di domini malevoli.
Avere un'ottima copertura dei domini malevoli permette di evitare le infezioni a vari livelli della cosiddetta Infection Chain che guida gli attaccanti nel loro percorso di attacco. Il dominio può essere usato allo stesso modo sia per scaricare payload, quando ci troviamo di fronte a infezioni multi-stage, sia per comunicare con il Command and Control degli impianti.
Nel primo caso, abbiamo la possibilità di intercettare, ad esempio, le fasi di un infezione come per esempio Emotet e Ursnif, oppure inibire all'utente l'accesso a una pagina di phishing.
Nel secondo caso, è possibile evitare l'attacco da parte di Malware come quelli osservati con Sunburst, che adottava un sofisticatissimo sistema di algoritmi di DGA (Domain name Generation Algorithm) per la comunicazione con il proprio C2, oppure bloccare numerose comunicazioni di backdoor appartenenti a CobaltStrike, che adotta in molte configurazioni il protocollo DNS come mezzo di interscambio tra informazioni e comandi.
Per queste ragioni, riuscire ad avere un metodo per affrontare in maniera adeguata il traffico di rete DNS permette di prevenire, identificare e mitigare gli attacchi informatici nelle varie fasi dell'intrusione. La tecnologia di Yoroi di DNS Defense viene costantemente alimentata da sorgenti variegate, ma allo stesso tempo esse vengono correlate e validate sia attraverso dei processi automatizzati che manuali: Yoroi aggrega feed provenienti sia da fonti OSINT che CLOSINT. Inoltre, la base informativa di Yoroi è arricchita da un lavoro di analisi Malware svolto dai nostri analisti sulle minacce intercettate sui nostri clienti.
Nel dettaglio, la tecnologia di Yoroi ha permesso di intercettare ben 1.487.818 connessioni verso domini classificati come malevoli. Di seguito la suddivisione delle principali minacce:

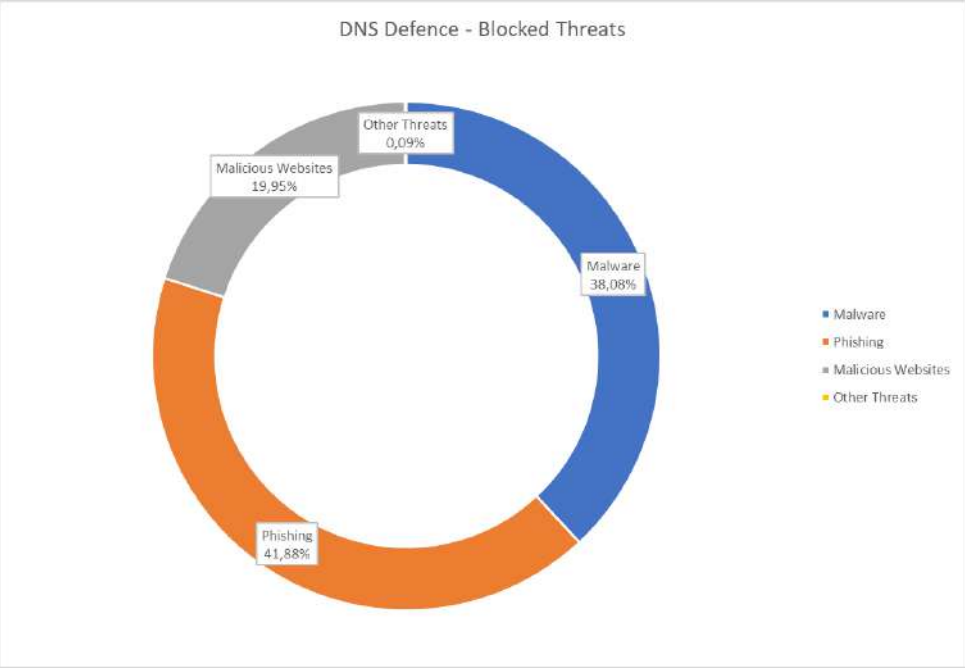

Figura 8. Distribuzione degli attacchi di phishing

Il grafico delle minacce bloccate mostra come la distribuzione della DNS Defense fornita da Yoroi copra e rimarchi il panorama cyber della sicurezza informatica. In particolare, le tre macro-minacce informatiche attuali sono Phishing, Malware e Siti Web Malevoli.
Durante l'anno appena trascorso il phishing, con il 41.88% degli attacchi bloccati, è la minaccia numero uno da affrontare. La problematica delle frodi informatiche è una grave piaga e sicuramente il problema resterà di grande diffusione perché gli attori criminali sono consapevoli che, sfruttando l'ingegneria sociale, hanno una possibilità di ingresso privilegiato sia all'interno delle difese perimetrali aziendali, sia a quelle più strettamente personali.
Sicuramente questo fornisce un grande spunto di riflessione e un'opportunità di miglioramento per i prossimi anni per quanto riguarda la formazione del personale in materia di security awareness. Infatti, riuscendo a preparare in maniera opportuna gli utenti più esposti alle frodi, si riduce drasticamente l'esposizione cyber aziendale.
Il secondo gruppo per volumi di richieste bloccate sono i malware con una prevalenza pari al 38.08%. In questa categoria consideriamo tutte le famiglie di codice malevolo, a partire dai Trojan, arrivando ai ransomware, passando per gli info-stealer e così via. In questo caso, la sola formazione del personale non è sufficiente per definire in maniera marcata la protezione del perimetro aziendale, ma è necessario unire ulteriori misure di difesa, come ad esempio tutte le appliance perimetrali, quali firewall, anti-malware ecc. Inoltre, l'approccio ottimale prevede anche l'inserimento di risorse altamente formate ad affrontare questa tipologia di problematiche, e di qui nasce la necessità di affidarsi a servizi Cybersecurity Defence Center.
La terza macro-famiglia di minacce bloccate sono i siti web dannosi con il 19.95%. In questo caso abbiamo soprattutto due possibili situazioni da considerare:

- la prima sono i siti web compromessi da attori per compiere attacchi di "Watering hole" per permettere agli avversari di colpire la catena del valore di un determinato settore, in modo da spingere l'installazione di codice malevolo tramite canali legittimi. Questa tipologia di tattica è frequente da rilevare tra i gruppi APT ben assestati, che dispongono di ingenti risorse da investire per la progettazione e implementazione di piani complessi di attacco;
- la seconda riguarda attacchi prettamente opportunistici, quali adware, malvertising, click fraud e altri. In questo caso, l'obiettivo è quello di essere quanto più "general purpose" possibile in modo da attingere ed ingannare quante più persone possibili.

Da tener presente è il fatto che il grafico prende in considerazione il singolo dominio bloccato e non un attacco informatico completo nella sua interezza che, allo stato, è composto da numerosi stage ma nella quasi totalità dei casi è avviato da un attacco di social engineering in tutte le sue forme. Il phishing è ciò che rappresenta la maggiore percentuale degli attacchi bloccati nel 2021.

Botnet e Attacchi Opportunistici

Una delle sfide che raccoglie Yoroi nella protezione dei propri clienti è lo studio della reputazione degli indirizzi e delle sorgenti da cui potrebbero provenire degli attacchi.
In generale, la piattaforma di Yoroi traccia in modo organizzato e strutturato gli IP esterni, soprattutto quelli che cercano di compiere attacchi opportunistici su larga scala, che possono effettuare tentativi di DDoS oppure tentativi di sfruttamento delle vulnerabilità del momento.
E' da considerare il fatto che spesso le attività malevole sono condotte anche tramite strumenti che permettono di nascondere la reale sorgente, come ad esempio VPN, bulletproof hosting, servizi di DynDNS, rete Tor ecc.
In questi casi, bisogna prestare particolare attenzione nella gestione delle sorgenti, perché potrebbero essere host condivisi con servizi legittimi; è quindi importante agire e mettere in bloccaggio le sorgenti con cognizione di causa.
Ad ogni modo, la telemetria offerta da Yoroi ci ha permesso di ottenere il seguente grafico della distribuzione geografica da cui provengono gli attacchi:

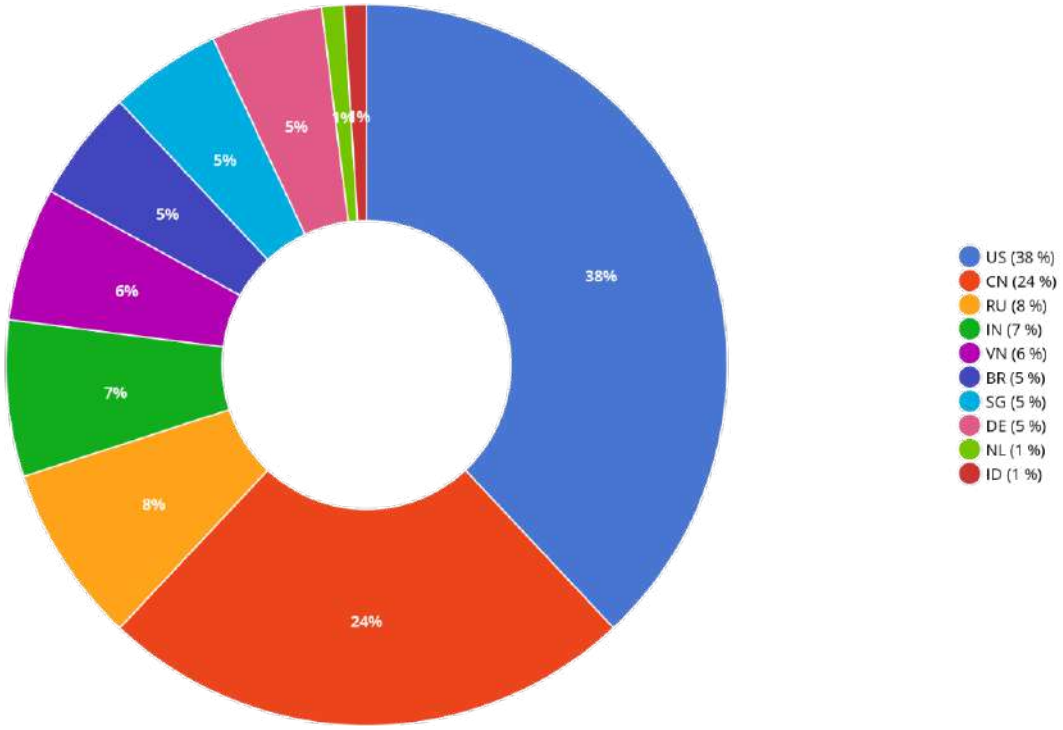

Figura 9. Distribuzione geografica degli attacchi

Osservando la distribuzione, gli Stati Uniti occupano anche quest'anno il primo posto con il 38% della quota, aumentando rispetto all'anno 2020 (34%). Inoltre, i tentativi provenienti dalla Cina (CN) sono rimasti costanti rispetto all'anno scorso al 24%. Il terzo posto è conservato dalle infrastrutture russe, che dalla nostra telemetria contengono l'8% delle comunicazioni malevole.
Tuttavia, come anticipato, anche in questo caso bisogna considerare il fatto che la Top 3 delle infrastrutture malevole sono da considerarsi tali per il fatto che esistono strumenti appositi per l'offuscamento dell'IP.
Inoltre, questi dati potrebbero essere utili per comprendere l'importanza di una strategia di reputazione IP *geofenced*, che deve considerare i paesi con cui esistono relazioni commerciali. Infatti, se l'azienda ha una propria attività negli Stati Uniti e non in Cina, ad esempio, si potrebbero bloccare tutte le connessioni in entrata da CN. In questo modo, infatti, è possibile mitigare molti attacchi opportunistici.
Il blocco di origini specifiche per le connessioni in ingresso potrebbe essere una buona strategia di difesa proattiva congiuntamente ad altre mitigazioni come la reputazione DNS e la soluzione di firma di rete.

Sezione 3:

La minaccia dalle Email

Come osservato durante gli anni passati, anche quest'anno gli avversari continuano a usare le email come mezzo preferito per la diffusione di codice malevolo. Esse sono un mezzo molto efficace per superare non solo le misure perimetrali di difesa, ma in molti casi permettono agli attaccanti di sfruttare anche le tecniche di social engineering per convincere le persone a cliccare e far partire l'infezione dall'interno. Seppure la mail non sia il mezzo più sofisticato per la distribuzione di minacce informatiche possiede altri vantaggi, tra i quali la scalabilità e la possibilità di sfruttare utenze già infette come mezzo di propagazione. Entrambi questi comportamenti sono stati accertati attraverso i servizi di Mail Protection forniti dalla piattaforma di Yoroi.
Ad esempio, la minaccia sLoad, molto presente in Italia, si diffonde tramite PEC (Posta Elettronica Certificata) e ha la capacità di inserirsi in thread di email realmente esistenti per essere più credibile agli occhi della vittima. Per quanto riguarda le mail opportunistiche inviate su larga scala, è impossibile non citare le due maggiori minacce attuali: Ursnif ed Emotet le quali si basano su botnet ed exploit kits per la loro diffusione.
Occorre ricordare che l'anno appena trascorso è stato caratterizzato dalla lotta contro la pandemia da COVID-19. In relazione alla situazione pandemica, sono state rilevate una vasta quantità di minacce informatiche che sfruttano detta tematica per aumentare la diffusione di mail malevole. Tuttavia, a differenza del 2020, anno che ha visto la nascita dello "smart working" diffuso con la conseguente emergenza della sicurezza dei dispositivi domestici, il 2021 ha fatto registrare un netto miglioramento e conseguente diminuzione di attacchi ai dispositivi domestici.

Analisi sulle campagne Email

Anche nel 2021, gli attori malevoli continuano a preferire le email e la messaggistica come vettore di diffusione del malware: per il quinto anno di fila, le mail malevole rappresentano una parte rilevante dei cyber-attacchi. Le strategia più utilizzate dagli attaccanti per sfruttare il vettore email sono le campagne di spam malevolo denominate "malspam". Alimentate da bot infetti tramite exploit kit, le campagne di malspam sono configurate per colpire singoli individui e piccole organizzazioni, ad esempio tramite mail di finte fatture con documenti Office malevoli che richiedono l'abilitazione delle macro per la visualizzazione del contenuto. Una volta preso il controllo di questi dispositivi, gli attaccanti prendono di mira obiettivi di alto valore tramite e-mail di spear-phishing che sfruttano temi specifici e l'accesso a caselle di posta fidate.
Inoltre, il 2021, proprio come il 2020, è un anno che sarà ricordato come caratterizzato dal contrasto alla pandemia da COVID-19 su larga scala. Anche i cyber criminali hanno sfruttato la pandemia per far apparire mail malevole più impattanti sulla sfera emotiva delle loro vittime, utilizzando argomentazioni inerenti a vaccini, Green Pass e nuove regolamentazioni. Inoltre, la situazione pandemica ha costretto le aziende ad adottare cambiamenti immediati, come il lavoro smart, parzialmente remoto o completamente remoto. Queste pratiche, spesso attuate in regime emergenziale, hanno influito negativamente sulla sicurezza degli utenti che, in molti casi, operavano fuori dal perimetro di sicurezza offerto dalla propria organizzazione.
Esaminando la telemetria raccolta dall'infrastruttura di monitoraggio del Cyber Security Defence Center, possiamo confermare che i documenti di Microsoft Office sono il vettore di consegna del malware più rilevante, rappresentando il modo più comune per diffondere il primo stadio della catena di infezione del malware. Infatti, i documenti Microsoft Word (35%) e i fogli di calcolo Excel (33,2%) rappresentano congiuntamente il 68,2% di tutti gli allegati maligni intercettati dai servizi Yoroi di email Protection.

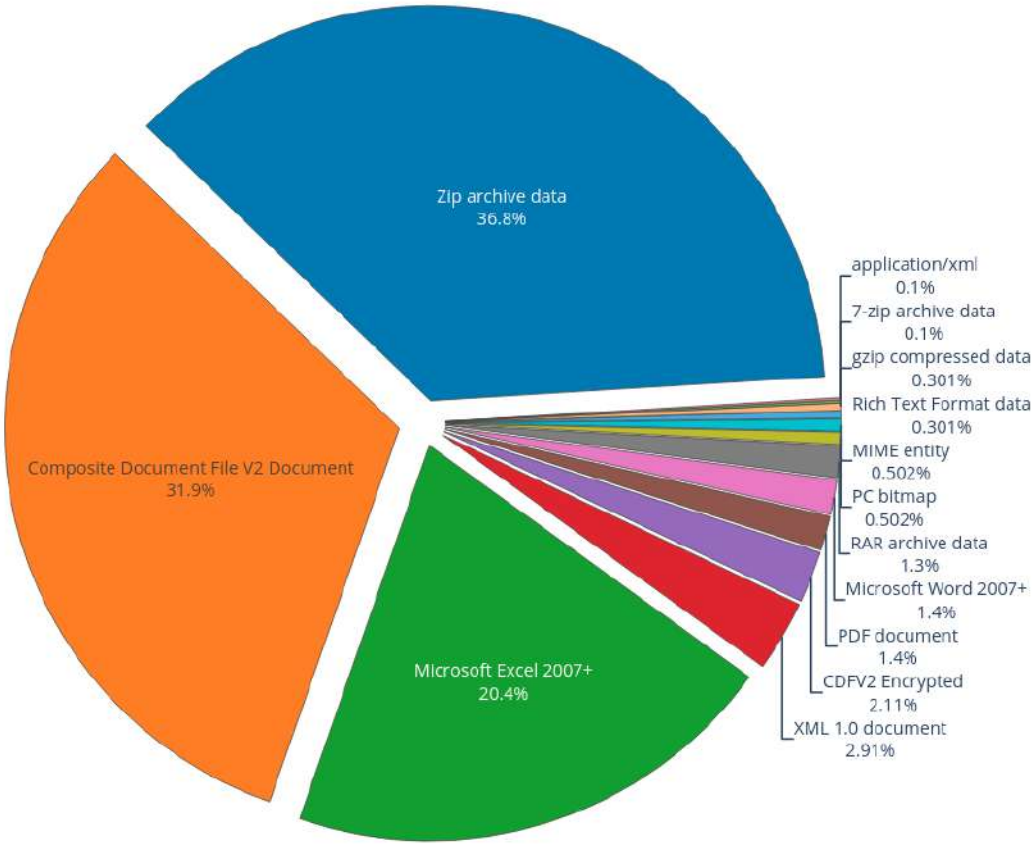

Figura 10. Distribuzione dei tipi di allegati malevoli

La percentuale di documenti dannosi in generale è ancora più alta. Infatti, una delle ultime tattiche adottate dai cyber criminali è quella di comprimere gli allegati all'interno di un file di archivio (zip, gzip o rar, 7zip) e crittografarli con una password menzionata all'interno del corpo della mail. È un metodo abbastanza semplice, ma rimane una tattica molto efficace e su cui gli avversari fanno sempre più riferimento.
L'abuso delle XLM Macro 4.0., tecnologia legacy ma ancora supportata nelle moderne suite di Office, che approfondiremo nel prossimo paragrafo, si conferma essere una delle principali tecniche per preparare documenti malevoli nel 2021.
Tuttavia, la nostra tecnologia di sandbox, Yomi, può analizzare questo tipo di tecniche e rilevare gli allegati dal comportamento dannoso essendo aggiornata quotidianamente sulle nuove tecniche di evasione e anti-rilevamento adottate dai criminali.
Un altro punto interessante da analizzare sono le tecniche di ingegneria sociale utilizzate dagli aggressori per attirare l'utente ad effettuare clic sul collegamento o sull'allegato dannoso. Anche quest'anno abbiamo eseguito diversi studi su email e sui contenuti dei testi, utilizzando algoritmi di machine learning per effettuare il clustering delle principali campagne di malspam. La Figura 11 mostra i cluster tematici delle campagne di malspam.

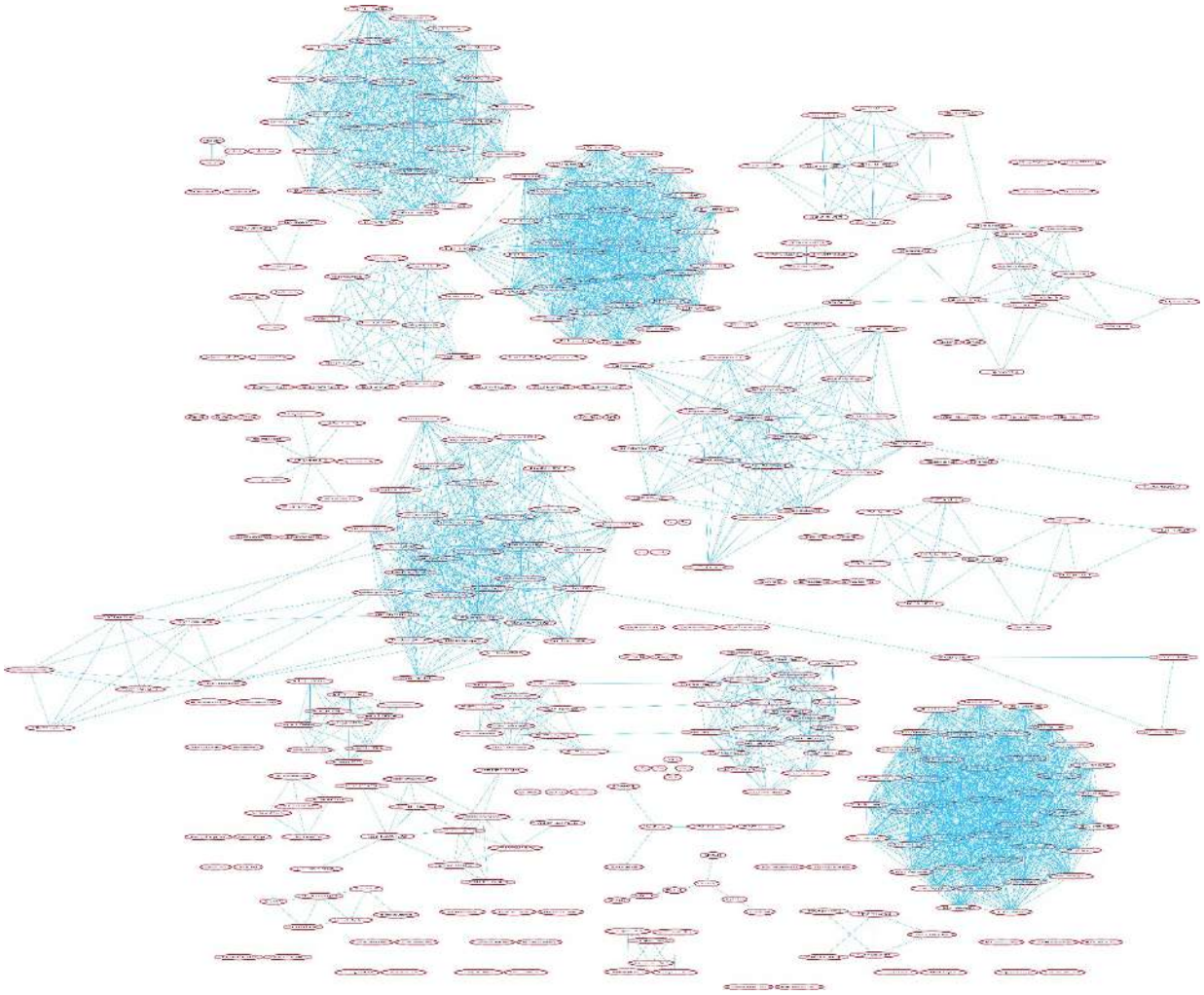

Figura 11. Analisi di clustering delle mail di malspam

L'analisi di elaborazione del linguaggio naturale ha rivelato che quest'anno vi sono state almeno otto diverse campagne di malspam. L'anno scorso (2020) ne erano evidenziate un numero maggiore: questo fenomeno di "addensamento" porta a dedurre, con alta probabilità, che i criminali hanno effettuato analisi preventive per meglio comprendere quali potessero essere i temi da utilizzare maggiormente perché di maggiore impatto, concentrando quindi temi molto più significativi per i target in oggetto.
Gli argomenti individuati sono molto simili se paragonati all'anno precedente. Nello specifico segnaliamo:

- Fatture e ordini;
- Consegna e tracciamento dei pacchi;
- Moduli fiscali;
- Certificati medici;
- Curriculum vitae;
- Risposte ai thread precedenti;
- Messaggi generici come: "Ciao, spero che tu stia bene", "Per l'attenzione di", "Lavoro d'ufficio".

Oltre a temi generici, come quelli appena elencati, proprio per la prevalenza di interesse verso i temi pandemici, sono state intercettate numerose campagne di malspam aventi come tema parole o frasi attinenti al dominio pandemico stesso. Quindi, proprio come l'anno passato, sono state individuate numerose mail preparate in maniera opportuna aventi i seguenti oggetti:

- Fatture e ordini su Covid-19;
- Informazioni, istruzioni o procedure sulle precauzioni Covid 19;

- Campagne di ristrutturazione;
- Campagne di cashback;
- Ritardi nei pagamenti.

Concludendo, quest'ultimo fenomeno lascia pensare a quanto il legame tra sicurezza e protezione si stia assottigliando. Un evento che accade all'interno del mondo reale ha conseguenze significative all'interno del mondo cibernetico e viceversa.
In Yoroi crediamo nell'educazione digitale e nella consapevolezza della sicurezza informatica per rendere entrambi i mondi più sicuri.

L'evoluzione delle minacce che sfruttano Office

Il principale vettore di propagazione di malware, come discusso nei precedenti capitoli, resta il vettore Microsoft Office, ampiamente utilizzato come strumento di lavoro. Durante il 2021 è stata individuata una significativa tendenza da parte degli attori criminali a sperimentare nuove tecniche per lo sfruttamento dello strumento di produzione di documenti elettronici più usato al mondo per diffondere codice malevolo.
Nel corso del 2021, oltre alle ormai classiche macro, gli attori criminali hanno trovato il modo di sfruttare altre caratteristiche dell'ambiente di sviluppo di Microsoft Excel per l'esecuzione di codice remoto. Questo ci ha offerto lo spunto per la produzione di una timeline per tracciare l'evoluzione delle minacce informatiche che sfruttano Office.

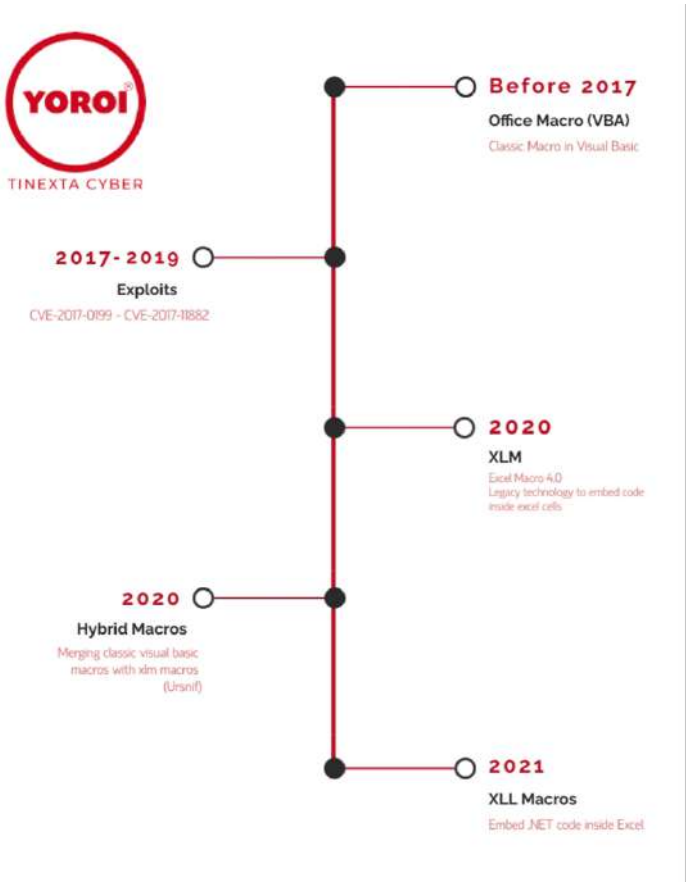

Figura 12. Timeline TTP Documenti Malevoli

La timeline riportata è presa da una ricerca condotta dal nostro gruppo di Threat Intelligence, il quale, osservando quotidianamente campagne di malspam che sfruttano documenti preparati ad-hoc per contenere codice malevolo, hanno deciso di costruire una mappa di quelle che sono le metodologie più note per il trasporto di payload malevoli su file Microsoft Office.
La timeline inizia considerando quello che è accaduto prima del 2017, dove la maggior parte dei documenti malevoli erano costruiti utilizzando macro in Visual Basic, le quali sono degli script adottati in maniera legittima per

automatizzare alcune operazioni elementari all'interno di documenti complessi, ma allo stesso tempo possono essere sfruttate per eseguire codice e quindi possono essere sfruttate dagli attaccanti per avviare codice malevolo.
Il 2017 invece è stato l'anno del rilascio di due gravi codici di exploit per sfruttare delle vulnerabilità dei componenti di Office, le quali sono state usate estensivamente sia da attaccanti attivi in ambito Cyber Crime che in ambito APT. Esse sono le CVE-2017-0199 e CVE-2017-11882: la prima permette a un attaccante di scaricare ed eseguire dei file HTA dalla rete internet; la seconda è una vulnerabilità legata a lacune nella gestione della memoria per il componente Equation Editor presente in tutti gli applicativi della suite di Office, che, sfruttata opportunamente, permette di eseguire codice arbitrario da remoto.
Tra il 2018 e il 2020 abbiamo osservato che gli exploit appena descritti erano stati adottati in maniera massiva; ma anche il ritorno delle macro, le quali hanno subìto un'evoluzione notevole per quanto riguarda le tecniche di offuscazione dei payload, aggiungendo, all'interno della catena di infezioni, ulteriori livelli e stage intermedi di script, composti anche da diverse tecnologie.
All'inizio del 2020 è emersa una nuova tecnica: lo sfruttamento delle XLM Macro 4.0, una tecnologia legacy presente all'interno di Microsoft Excel già dal 1992 e compatibile anche con le attuali versioni di Excel. Il motivo per cui questa tecnologia è diventata così tanto pervasiva è il fatto che, facendo delle analisi empiriche, questa tipologia di script è estremamente efficace nell'elusione dei motori di classificazione degli anti-malware. Quindi, i creatori di malware si sono impegnati nel miglioramento della tecnica, combinandola con le più canoniche macro in Visual Basic, creando così un approccio ibrido nello sfruttamento dei documenti di Excel. Questo comportamento lo osserviamo ancora oggi, ed è adottato soprattutto dagli attori criminali di TA-544, la gang che è dietro allo sviluppo e al mantenimento del famoso trojan bancario Ursnif.
L'ultima tendenza evidenziata all'interno dell'attuale panorama cyber è lo sfruttamento di un'altra caratteristica di Microsoft Excel, che permette di caricare ed eseguire codice di terze parti implementato in C/C++ e .NET. Questa "capacità" (feature) di Excel si chiama Excel Add-In File; di fatto, il codice che viene caricato ed eseguito è quello di una libreria, una vera e propria DLL, con l'unica differenza che l'icona proposta sembra essere dell'applicativo di foglio elettronico.

Sezione 4:

Evoluzione delle Tecniche di Attacco

Yoroi ha molto a cuore il tema dello studio delle tendenze di attacco degli avversari cyber perché, grazie a queste tipologie di analisi, è possibile riuscire a fare delle previsioni accurate su quello che può accadere nel futuro prossimo.
Se affermiamo che la parola chiave dell'anno 2021 è "conferma", ci possiamo aspettare delle attività compatibili con i modelli osservati anche per tutto il 2022. Infatti, le due maggiori problematiche a livello di sicurezza informatica che sono state osservate nel 2020 e poi confermate nel 2021, sono state il fenomeno della "Double Extortion" e il fenomeno degli attacchi alla Supply Chain. Ci si attende con buona probabilità che anche nel corso del 2022 questa tipologia di attacchi sia nel pieno delle forze, in quanto la maturità di sfruttamento di tali meccanismi risulta essere adeguato.
In questa sezione ci vogliamo concentrare sullo studio e sull'analisi di questi fenomeni e avanzare una previsione per l'anno 2022 e per i successivi.

Double Extortion: il nuovo standard criminale

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: abbiamo una strutturazione complessa con una separazione dei compiti abbastanza rigida, del tutto simile a una organizzazione aziendale.
Ciascun gruppo di Ransomware as-a-service di alto profilo come quelli studiati, ha all'interno del suo organico le seguenti figure:

- 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 a livello elevato all'interno della comunità.

Per mantenere in piedi un'organizzazione del genere, è ovvio che deve esserci una leadership di altissimo 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 tutte le questioni di turnover e di infiltrazione di personalità sotto copertura.
Inoltre, vi sono altri temi affrontati da questa tipologia di gruppi criminali: in particolare, come accedere al perimetro aziendale della vittima.
In questo caso esistono numerose soluzioni per risolvere tale problema, ma comunque suddivisibili in due categorie:

- Affidarsi a "servizi" esterni definibili come "Initial Access as-a-service", forniti, ad esempio, dai grandi gruppi che stabiliscono accessi silenti e persistenti all'interno dei perimetri aziendali tramite trojan alquanto sofisticati; oppure tramite attività di compravendita di exploit adatti a colpire determinate tecnologie;
- Prevedere una soluzione interna di sviluppo di tecniche e procedure per ottenere gli accessi nei confronti degli attaccanti.

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 mancanza di pagamento del riscatto, gli operatori minacciano attacchi di Denial of Service sui sistemi della vittima, impedendone il ripristino, grazie al fatto che possibilmente 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.

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 prevedete una certa formalizzazione delle problematiche di cyber sicurezza una volta che una certa organizzazione deve trattare dati provenienti da ogni tipo di customer. Per quanto riguarda le politiche aziendali è necessario compiere ancora significativi sforzi di miglioramento nella gestione di una "Cyber-Crisis", che deve prevedere il lavoro congiunto di politiche aziendali e di tecnologie di protezione per la mitigazione di problematiche del genere.
In definitiva, se ormai consideriamo come standard le attività da Double Extortion, è necessario allo stesso modo considerare e valutare l'azione.
Quindi, il problema da porsi è come riuscire a gestire in maniera opportuna queste situazioni per affrontare nel migliore dei modi anche i vincoli operazionali che necessariamente accadono in ogni realtà aziendale, che possono essere dovute sia alla 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 aziendale: per esempio, in ambienti aziendali complessi, l'adozione delle best-practice potrebbe tradursi solo in costosi esercizi di rispetto di standard e di 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. Questo non è una scelta dovuta al fatto di preferire un qualcosa rispetto all'altro, ma semplicemente 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.

Attacchi al perimetro: le tecnologie più a rischio

Nonostante non sia uno dei vettori più utilizzati, lo sfruttamento delle falle tecnologiche da parte di attori malevoli - specie sul perimetro esterno - è gradualmente aumentato di popolarità nel 2021. La prevalenza di questo fenomeno è cresciuta al punto da divenire uno dei vettori di ingresso più utilizzato da chi compie estorsioni ransomware. È infatti appurabile direttamente, attraverso la frequentazione di canali e chat nel deep web, che numerosi organizzazioni criminali stanno investendo ingenti somme di denaro e di risorse umane alla ricerca di vulnerabilità sulle tecnologie aziendali. Nel corso del 2021, numerosi Vendor sono stati vittima di attacchi attraverso i loro prodotti, sia in maniera diretta come nell'eclatante caso di Kaseya, sia in maniera indiretta, con lo sfruttamento di gravi falle ritrovate all'interno dei loro apparati hardware e software.

Fortinet FortiGate

Le appliance Fortinet Fortigate sono tra i più diffusi firewall di nuova generazione negli ambienti SME e Medium Enterprise. Specie dopo la pandemia del 2020, sono frequentemente utilizzati come Gateway SSL VPN per abilitare i paradigmi di smart working.
Tra le falle Fortigate più abusate dagli attori criminali a doppia estorsione troviamo senz'altro la CVE-2018-13379: una problematica di path-traversal che permette di leggere file arbitrari di sistema, anche privilegiati, senza alcuna autenticazione. La falla è diventata particolarmente famosa a Novembre 2020, quando aggressori digitali hanno rilasciato pubblicamente una lista di 87 mila firewall FortiGate vulnerabili online. Il problema principale è stato nella tipologia di file che potevano essere letti attraverso tale vulnerabilità. E' stato possibile leggere credenziali di accesso di numerose VPN aziendali, direttamente all'interno del perimetro dell'organizzazione. Questo fenomeno è stato osservato in alcune estorsioni cyber nelle quali è stata utilizzata come vettore di ingresso.
Gli effetti della falla si sono fatti sentire anche nel 2021. A settembre sono state pubblicate all'interno di circuiti criminali le credenziali aziendali di migliaia di organizzazioni in tutto il mondo prelevate proprio sfruttando questa falla. Si fa notare che in questa lista sono presenti circa mille aziende italiane.

Pulse Connect Secure

Altra tecnologia sulla quale numerosi cyber criminali hanno investito sono i moduli SSL VPN di Pulse Connect Secure. Anch'essi sono stati presi particolarmente di mira dal cyber crimine.
Specialmente la falla CVE-2019-11510 affligge i moduli SSL VPN in Pulse Secure Pulse Connect Secure (PCS) e permette ad un attaccante privo di autenticazione di ottenere file di sistema privilegiati contenenti informazioni molto sensibili, come credenziali di accesso e token di sessione attivi. Benché risalente a quasi due anni fa, questa falla viene tutt'ora utilizzata anche dagli affiliati al gruppo cyber criminale REvil/Sodinokibi, gli autori del più violento attacco supply chain del 2021 ai danni di Kaseya.

SonicWall

Altra serie di apparati altamente profittevoli agli occhi degli autori di cyber estorsioni sono le funzionalità NetExtender VPN e Secure Mobile Access dei firewall perimetrali SonicWall.
Le falle più bersagliate in questo caso sono molteplici: si va dalla CVE-2019-7481 che permette letture arbitrarie di file di sistema da attaccanti esterni, a SQL-Injection come la CVE-2021-20016 sull'interfaccia utente in http, che permette di recuperare informazioni sensibili, credenziali e sessioni, oltre che esecuzioni di codice da remoto durante la lettura della user agent del client come per la falla CVE-2019-7482.
Questa serie di vulnerabilità è stata utilizzata per attacchi ransomware da vari gruppi criminali durante tutto il periodo di osservazione. L'efferatezza degli attacchi è stata tale da costringere il produttore a emanare avvisi espliciti sul rischio ransomware collegato all'utilizzo di versioni vulnerabili dei firewall SonicWall.

Palo Alto

Anche i firewall enterprise Palo Alto sono nei radar dei gruppi cyber criminali più efferati che seguono le pratiche di doppia estorsione.
Questa volta però la falla abilitante a vari attacchi cyber è stata la CVE-2019-1579, una pericolosa vulnerabilità che affligge la componente GlobalProtect Portal / Gateway Interface dei firewall di nuova generazione Palo Alto. In questo caso li demone "sslmgr" del gateway SSL utilizzato per l'handshake di tutte le connessioni cifrate ricevute dal Palo Alto - anche prima dell'autenticazione utente - permette ai cyber criminali di eseguire dei comandi direttamente sul sistema.

Citrix ADC / NetScaler

Le tecnologie Citrix Application Delivery Controller (ADC) e Citrix Gateway (NetScaler) stanno alla base di numerose architetture di rete Enterprise e sono da tempo utilizzate per garantire connettività ad applicativi aziendali interni.
I gateway Citrix sono stati particolarmente interessati dagli attori criminali ransomware per via della combinazione di una serie di falle: la CVE-2020-8193 che premette di bypassare l'autenticazione utente, e le falle CVE-2020-8195 e CVE-2020-8196, che permettono invece di recuperare contenuti potenzialmente sensibili dell'appliance in maniera del tutto non autorizzata.
Inoltre, all'inizio del 2020, le appliances Citrix Netscaler di tutto il mondo sono state bersagliate da numerosi tentativi di attacco della falla CVE-2019-19781, una pericolosissima vulnerabilità che abilita attaccanti remoti a eseguire codice arbitrario sulle infrastrutture Citrix esposte ad internet, utilizzato dai criminali per guadagnare accesso alle reti aziendali.

F5 BIG-IP

Gli apparati BIG-IP sono de facto standard per molte realtà enterprise nella realizzazione di architetture web sicure. Negli ultimi due anni le tecnologie BIG-IP di F5 sono state oggetto di attenzioni ricorrenti da parte dei gruppi cyber criminali, specialmente riguardo a due gravi falle.
La CVE-2021-22986, una vulnerabilità nelle interfacce REST del componente iControl che permette ai cyber criminali di eseguire comandi diretti sull'appliance, creare, cancellare e manipolare file all'interno del sistema, condizione in grado di causare una compromissione totale del sistema.

Exchange Server

Microsoft Exchange Server è da decenni la soluzione email on premise più diffusa per gli ambiti enterprise. I servizi Exchange sono frequentemente raggiungibili da internet specie grazie alle funzionalità Outlook Web Access.
Nonostante il lungo servizio in auge, a Marzo 2021 la tecnologia Exchange Server è stata pesantemente afflitta da una serie di criticità. A seguito dello sfruttamento delle stesse, Microsoft Exchange è passato dall'essere un caposaldo delle infrastrutture aziendali a rappresentare un delicato rischio da gestire per l'azienda, uno dei principali bersagli per numerosi cyber criminali. Lo spartiacque di questo nuovo modo di vedere Exchange Server on premise è stato senz'altro "ProxyLogon". Si tratta in realtà di una particolare combinazione di più falle: la CVE-2021-26855 che permette il bypass dell'autenticazione utente e la personificazione dell'amministratore del servizio, e la CVE-2021-27065 che permette di scrivere file arbitrari sul sistema, come ad esempio codici webshell e backdoor nascoste attivabili dall'esterno.
In tanti hanno sfruttato le falle ProxyLogon. In origine gruppi APT come Hafmium (TH-270), in seguito botnet automatizzate come LemonDuck (TH-127), ma anche gruppi cyber criminali altamente specializzati nella conduzione di doppie estorsioni come Revil/Sodinokibi (TH-200).
Questa tendenza che affligge la tecnologia Exchange Server non accenna ancora a diminuire. La storia si è infatti ripetuta mesi dopo con le falle "ProxyShell". Anche in questo caso si tratta di una concatenazione di particolari vulnerabilità che, insieme, mettono in ginocchio il server di posta, in particolare il bypass delle access control list della CVE-2021-34473, l'escalation di privilegi della CVE-2021-34523 e - nuovamente - una scrittura file arbitraria con la CVE-2021-31207 che, se messe in fila, permettono di installare backdoor sui sistemi Exchange Server esposti su internet.

VMWare vCenter

Le tecnologie VMWare sono di frequente la piattaforma abilitante per il modello dei private cloud, fondamentali quando il cloud pubblico non può cogliere i requisiti che caratterizzano certi verticali di business.
Da inizio estate 2021 è cominciata, da parte di cyber criminali, la caccia grossa alle istanze vSphere esposte su internet. Molti estorsori digitali, tra cui anche le gang specializzate nelle pratiche di doppia estorsione, si sono adoperate per mappare e attaccare le versioni VMWare vCenter vulnerabili a CVE-2021-21985: una particolare falla nel frontend HTML5 di vSphere che permette ai criminali di eseguire codice sui server VMWare dell'azienda sfruttando un plugin vulnerabile attivo di default, il tutto senza alcuna credenziale richiesta.
Ancora prima, anche la CVE-2021-21972 aveva destato particolari attenzioni. Le interfacce vROP dei vCenter Server sono infatti state pesantemente bersagliate da attacchi cyber volti a eseguire malware direttamente sulle infrastrutture di virtualizzazione.

Log4j

Verso fine 2021 è emersa quella che è sembrata per gli addetti ai lavori una grave catastrofe nell'ambiente della cybersecurity, un software open source usato all'interno di praticamente tutti i progetti scritti in linguaggio Java, sia in ambito open source che in ambito Entreprise: Log4j.
Essa è una libreria di logging adottata in moltissimi progetti, in quanto costruita per essere del tutto compatibile con tutti i progetti Java e allo stesso tempo essere sia ready-to-use che facile da usare.
La vulnerabilità è stata considerata così disastrosa perché generando opportunamente una richiesta verso un servizio scritto in Java che usa tale libreria, è possibile eseguire codice arbitrario sul backend che interpreta tale richiesta. Per tutto il dicembre 2021, dove gli attacchi erano in massa, il team del CSDC di Yoroi è stato attivo H24 per il monitoraggio dei tentativi di attacco per tale vulnerabilità.
Questo caso è un ottimo spunto di riflessione per quanto riguarda l'adozione di codice sviluppato da terze parti: come lo si deve considerare? E quando si tratta invece di codice open source, come si affronta il problema? I quesiti sono abbastanza complessi da sviscerare, ma sicuramente la prima soluzione a cui si deve pensare è il fatto che è necessario adottare in primo luogo un piano consistente di vulnerability management e in secondo luogo affidarsi alle reti CERT, le quali hanno il compito di approfondire e di rilasciare bollettini di sicurezza ogni qualvolta emergono delle falle di sicurezza di tale rilevanza.

Sezione 5:

L'Esposizione Cyber della Supply Chain in Italia

Ogni business si basa su catene del valore che spesso trascendono gli stessi confini aziendali. Le filiere produttive sono sempre più complesse, intricate ed estese: alla base di un qualsiasi prodotto o servizio si possono trovare decine o centinaia di organizzazioni del tutto eterogenee, da microimprese a grandi gruppi, interconnesse tra loro. Ognuno di questi enti, questi piccoli nodi nell'intricato grafo di relazioni commerciali che formano la catena di supply chain aziendale, hanno un ruolo e con esso dei rischi associati. Nell'ultimo anno, uno di questi rischi in particolare si è manifestato con grande sorpresa: il rischio cyber.

Le tecniche di infiltrazione caratteristiche degli attacchi ransomware a doppia estorsione hanno infatti portato alla luce il clamore della transitività del rischio cyber: incidenti come l'attacco Kaseya, che tramite la supply chain del software ha inflitto gravi danni a migliaia di aziende in tutto il mondo, hanno palesato il costo nascosto della non gestione di questo nuovo vettore.

Per questo, Yoroi, nel 2021, ha realizzato un indice di sintesi per monitorare il rischio cibernetico nella supply chain: lo **«Yoroi Cyber Exposure Index»**. Uno strumento disegnato per offrire una 'vista di esposizione' che un attaccante può utilizzare come step iniziale e che risulta indicativo della probabilità di riuscita dell'attacco stesso. Questo indice viene utilizzato da numerosissime aziende italiane per monitorare il rischio cyber nella loro rispettiva filiera produttiva, in modo discreto, senza azioni intrusive su infrastrutture terze e con captazioni da fonti esterne alle aziende.

Nel corso del 2021, Yoroi ha raccolto oltre 4452 punti di valorizzazione dell'incide CEI su migliaia di aziende parte della supply chain dei principali gruppi industriali italiani, con l'obiettivo di individuare le principali aree di origine del rischio cyber della supply chain che transitivamente affligge le aziende più strutturate.

Le analisi hanno preso in considerazione le tre tipologie di dimensionali che compongono l'indice CEI di Yoroi.

In primis, il fattore d'incisione espositivo: ovvero quanto una particolare tipologia di fornitori impatta in termini di aumento della superficie informatica esposta al rischio, misurazione che raccoglie in sé la risposta alla domanda "in che misura un partner industriale in un certo settore mi espone indirettamente ad attacchi?".

Gli indici CEI aggregati raccolti nel corso del 2021, mostrano che l'interconnessione delle reti informatiche tra clienti e fornitori è in molti casi particolarmente forte, tanto da equivalere ad un aumento della superficie informatica aziendale stessa. In particolar modo, i dati CEI del 2021 rivelano che mediamente, includere una società di procurement nei propri fornitori equivale ad un aumento del 14.7% della superfice cyber aziendale; per fornitori di IT e provider digital certificati, l'aumento di superfice è del 11.4% e 16.4%; nel caso di partner in settori tecnologici elettronici e provider di servizi finanziari è del 6.75% e 6.16%.

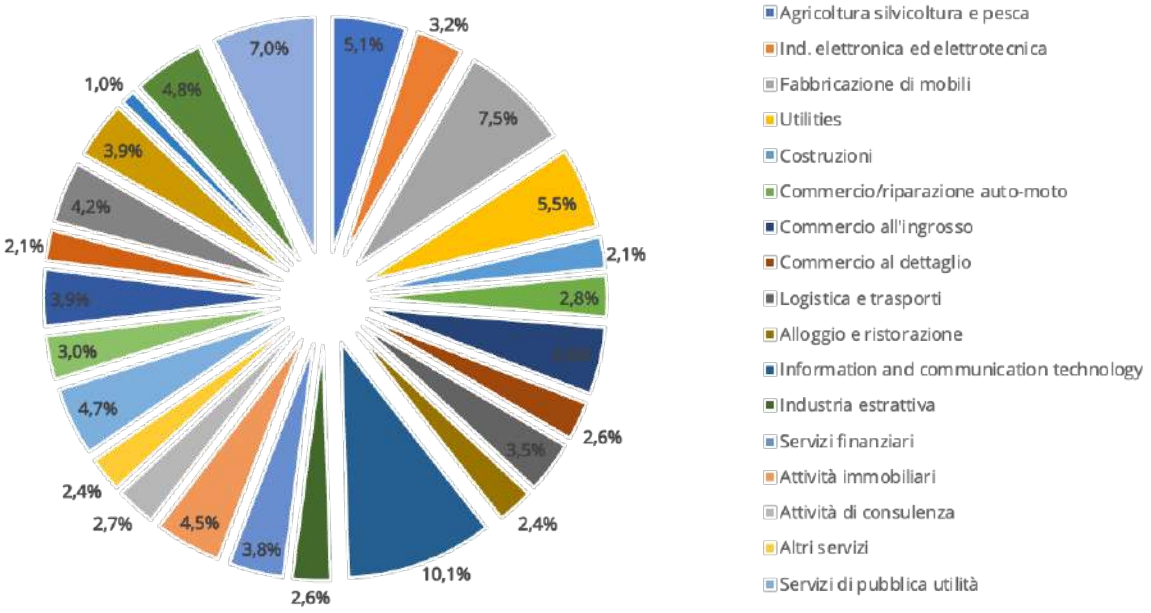

Figura 13. Esposizione per settore merceologico – Aziende Large

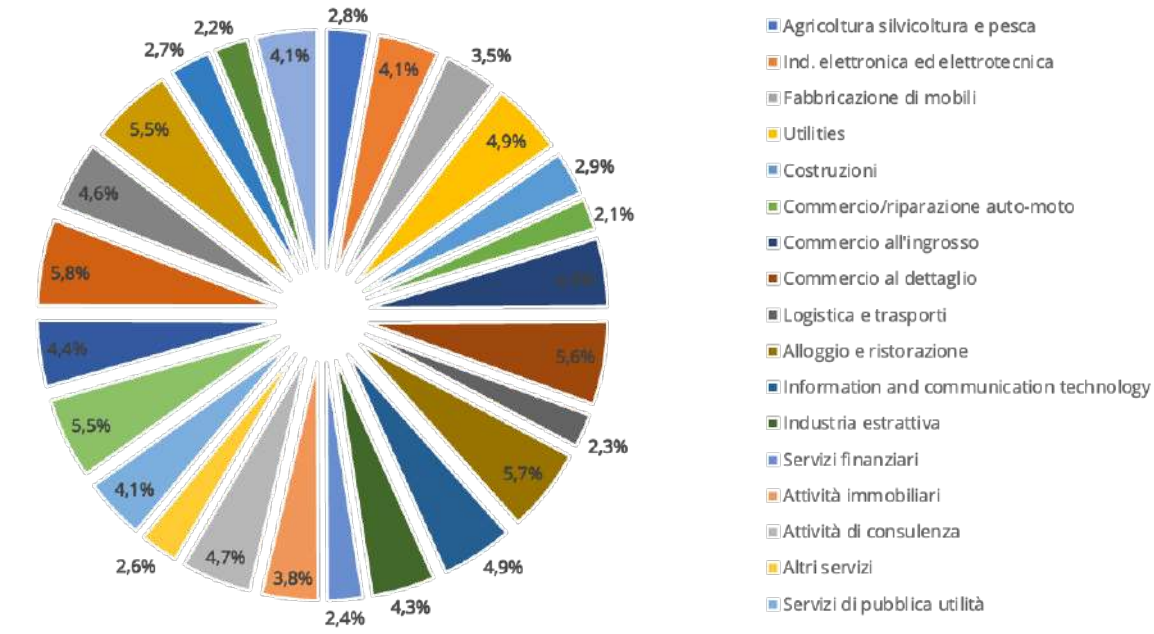

Figura 13bis. Esposizione per settore merceologico – Aziende Mid

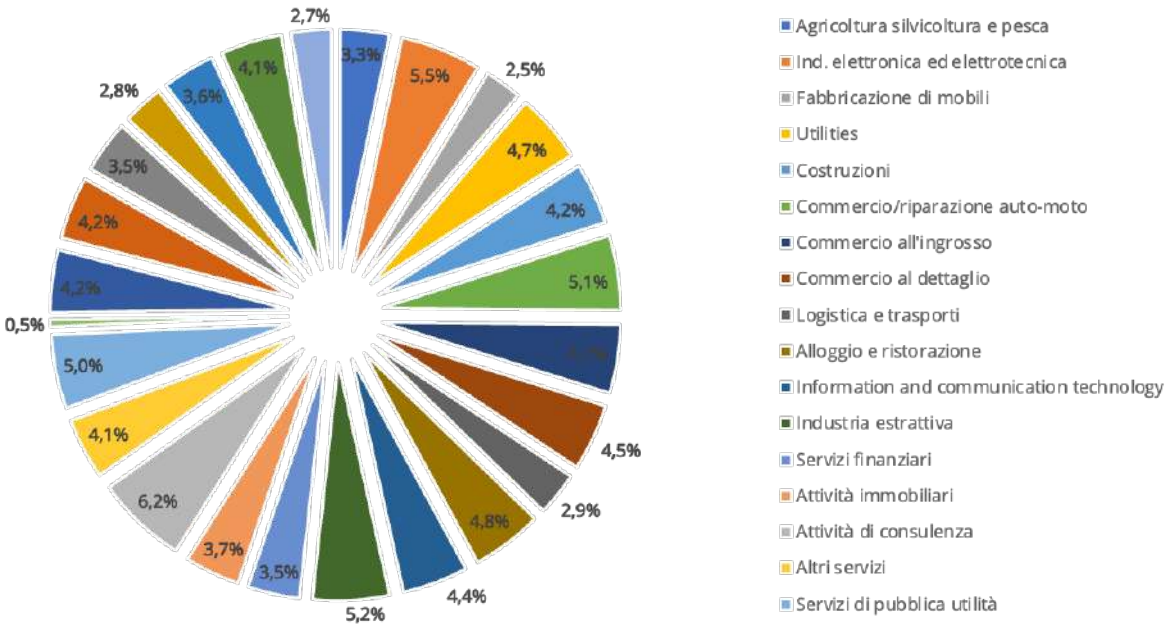

Figura 13ter. Esposizione per settore merceologico – Aziende Small

La seconda dimensione degli indici CEI calcolati sul 2021 è relativa ai volumi di record all'interno dei data leak contenenti informazioni relative alle aziende sottoposte al monitoraggio del CEI di Yoroi. I record monitorati dal CEI sono essenzialmente pezzi di informazione, nomi a dominio, indirizzi email e credenziali che compaiono nelle collezioni di dati scambiate all'interno del dark web criminale.
La presenza di occorrenze di una certa azienda è indice della circolazione di informazioni legate a quest'ultima e di un rischio maggiore di attacchi cyber, proprio a causa della natura criminale degli ambienti in cui circolano questi dati. Dalle analisi CEI nell'anno 2021 è emerso un forte rischio per il settore delle società di procurement e per il settore minerario ed estrattivo, dove occorrenze di email e infrastrutture compaiono nel 47.4 % e 24.5% dei casi registrati, seguite dalle società di digital trust, specialmente attive con servizi di firma elettronica B2B e B2C. In questo caso, però, la forte esposizione che raggiunge quota 22.5%, è riconducibile all'ampio bacino di utenti che utilizzano questi servizi: un grande numero più PMI e microimprese.

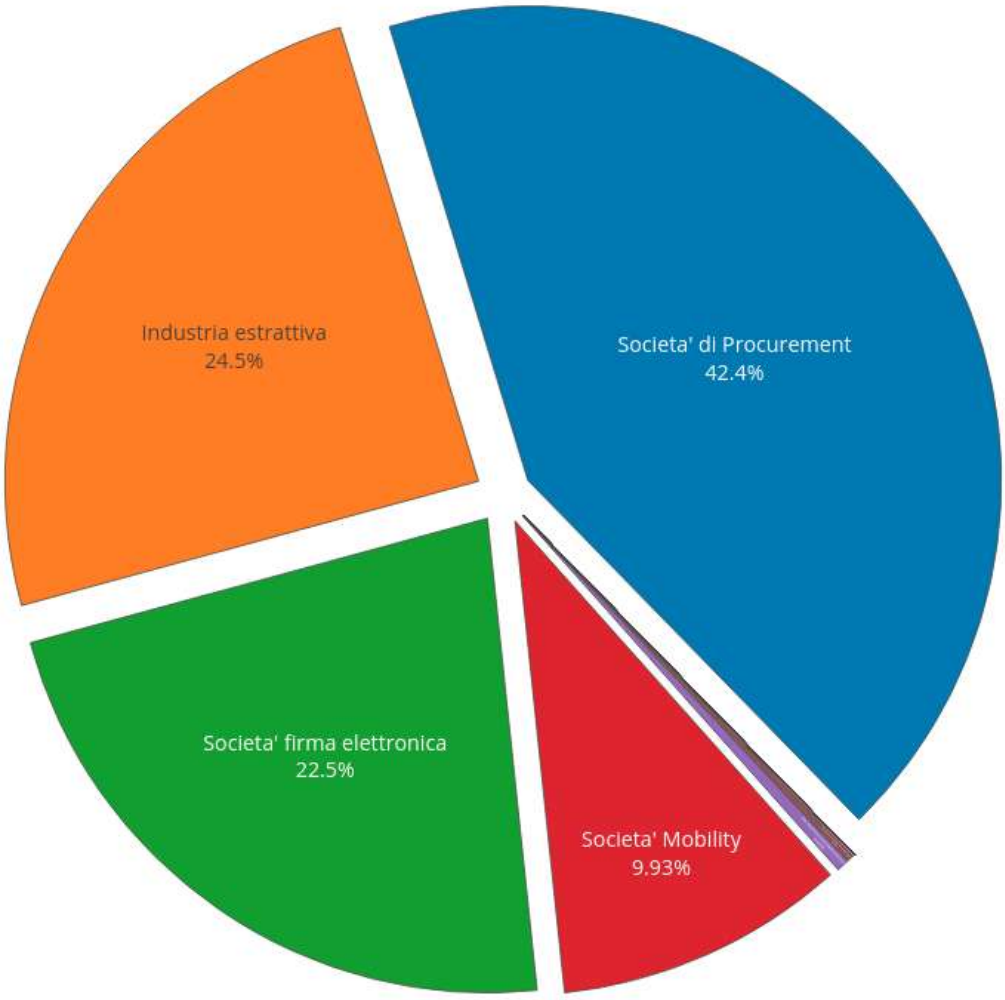

Figura 14. Data Leak per settore merceologico

Altra dimensione studiata dall'indice CEI di Yoroi nel 2021 è la distribuzione delle potenziali falle sul perimetro internet delle organizzazioni, misurazione che fornisce un indicatore sull'attrattività delle infrastrutture informatiche esposte agli occhi di potenziali malintenzionati: elemento collegato a una maggiore probabilità di ricevere tentativi di attacco esterno, proprio a causa dei dati e delle informazioni in merito agli asset IT aziendali reperibili da fonti esterne, raccolti con metodologie similari a quelle utilizzate dagli attaccanti durante le fasi di ricognizione, step iniziale della catena di attacco cyber criminale.
In questo frangente risultano particolarmente attenzionabili dai malintenzionati tre settori più di altri: il settore del digital trust e dei provider di firma elettronica, i quali sono interessati dal 78.9 % degli indici CEI osservati nel 2021; il settore delle società di procurement con il 12.1 % del totale; le società di mobility con il 9.0%, settore particolarmente attivo dopo l'istituzione dell'obbligatorietà della figura del mobility manager a maggio del 2021 da parte del ministero dei trasporti italiano.

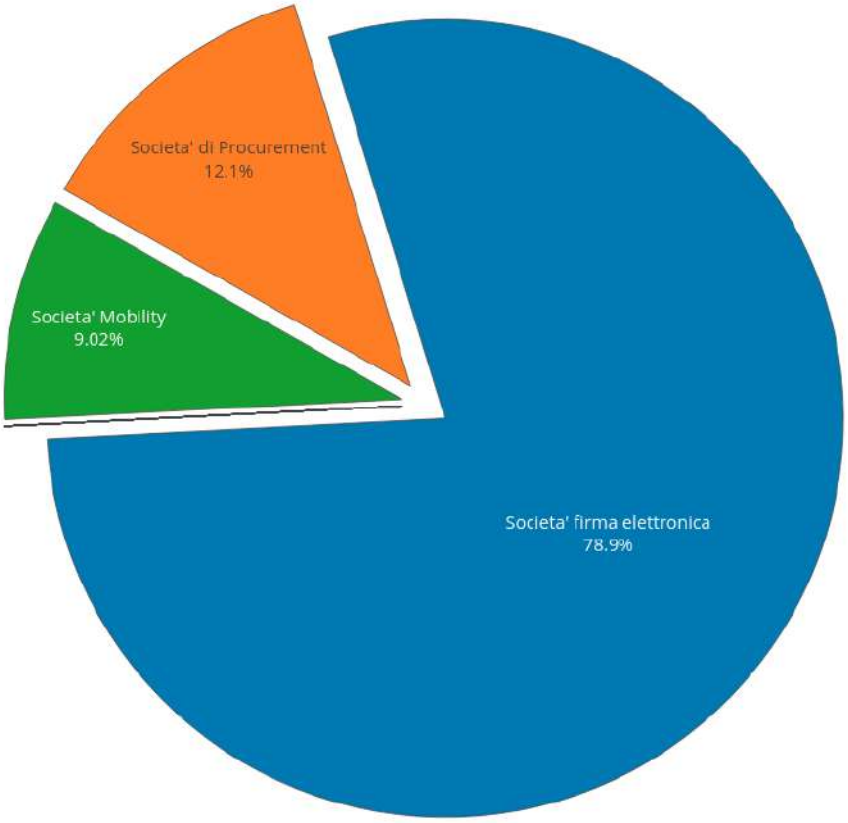

Figura 15. Vulnerabilità per settore merceologico

Conclusioni

Anche nel 2021 i due maggiori fenomeni osservati a livello di sicurezza informatica sono stati quello della “Double Extortion” e quello degli attacchi alla Supply Chain.

La telemetria offerta dalla piattaforma Yoroi ha permesso di estrarre una serie di statistiche riguardo attacchi di tipo “zero-day Malware”, ovvero Malware non noti alle firme dei sistemi antivirus, essendo il 76% delle minacce Malware di tipo 0-day.

In questo contesto, il phishing e lo spear phishing sono i vettori più adottati nel 2021 per avviare la catena di attacco.

Come evidenziato nel 2020, la maggioranza dei Malware individuati in Italia appartengono alla tipologia dei Trojan Bancari. Il principale vettore di ingresso è rappresentato da Ursnif con una presenza del 33.5% sul totale e la presenza di Emotet per il 18.9% dei campioni.

Tuttavia, durante il 2021, il phishing, con il 41.88% degli attacchi bloccati, è stata la minaccia numero uno da affrontare. Il secondo gruppo per volumi di richieste bloccate sono i malware con una prevalenza pari al 38.08%. La terza macro-famiglia di minacce bloccate sono i siti web dannosi con il 19.95%.

Per quanto riguarda Botnet e Attacchi Opportunistici, in base alle nostre osservazioni esiste una distribuzione tipica dell’origine delle incursioni in cui gli Stati Uniti come territori d’origine occupano anche quest’anno il primo posto con il 38% della quota, aumentando rispetto all'anno 2020 (34%). Inoltre, i tentativi provenienti dalla Cina (CN) sono rimasti costanti rispetto all’anno scorso al 24%. Il terzo posto è conservato dalle infrastrutture russe, che dalla nostra telemetria contengono l’8% delle comunicazioni malevole.

Anche nel 2021, gli attori malevoli continuano a preferire le email e la messaggistica come vettore di diffusione del malware: per il quinto anno di fila, le mail malevole rappresentano una parte rilevante dei cyber-attacchi. Esaminando la telemetria raccolta dall'infrastruttura di monitoraggio del nostro Cyber Security Defence Center, possiamo confermare che i documenti di Microsoft Office sono il vettore di consegna dei malware più rilevante. Durante il 2021 è stata individuata una significativa tendenza da parte degli attori criminali a sperimentare nuove tecniche per lo sfruttamento dello strumento di produzione di documenti elettronici più usato al mondo per diffondere codice malevolo.

Nonostante non sia uno dei vettori più utilizzati, lo sfruttamento delle falle tecnologiche da parte di attori malevoli - specie sul perimetro esterno - è gradualmente aumentato di popolarità nel 2021.
Nel corso del 2021, numerosi vendor sono stati vittima di attacchi attraverso i loro prodotti, sia in maniera diretta come nell’eclatante caso di Kaseya, sia in maniera indiretta, con lo sfruttamento di gravi falle ritrovate all’interno dei loro apparati hardware e software.

Verso la fine del 2021 è emersa quella che è sembrata, per gli addetti ai lavori, una grave catastrofe nell’ambiente della cybersecurity, un software open source usato all’interno di praticamente tutti i progetti scritti in linguaggio Java, sia in ambito open source che in ambito Entreprise: Log4j.
Per tutto il dicembre 2021, dove gli attacchi erano in massa, il team del CSDC di Yoroi è stato attivo H24 per il monitoraggio dei tentativi di attacco per tale vulnerabilità.

Gli attacchi alla supply chain sono stati di particolare rilevanza. Ogni business si basa su catene del valore che spesso trascendono gli stessi confini aziendali. Le filiere produttive sono sempre più complesse, intricate ed estese: alla base di un qualsiasi prodotto o servizio si possono trovare decine o centinaia di organizzazioni del tutto eterogenee, da microimprese a grandi gruppi, interconnesse tra loro.
Ognuno di questi enti, questi piccoli nodi nell’intricato grafo di relazioni commerciali che formano la catena di supply chain aziendale, hanno un ruolo e con esso dei rischi associati.

Una delle caratteristiche più importanti del Cyber Security Annual Report di Yoroi riguarda i dati.

I dati utilizzati in questo rapporto, appartengono ad incidenti realmente accaduti.

Per fargli fronte nel prossimo futuro, secondo Yoroi, è necessario compiere ancora significativi sforzi di miglioramento nella gestione delle “Cyber-Crisis”, diventando capaci di sviluppare politiche aziendali e tecnologiche di protezione per prevenirli e contenerli.

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


Y


Y


Y


Y