CYBERSECURITY ANNUAL REPORT 2023

DEFENCE BELONGS TO HUMANS

Sommario

Introduzione

Anche il 2022 è stato un anno particolarmente significativo per la sicurezza digitale. Eravamo consapevoli che eventi di natura politica, territoriale, infrastrutturale e ideologica potessero alterare il delicato equilibrio che vi è tra il "digitale" ed il "fisico" ma mai avremmo potuto immaginare uno scenario simile.

L'invasione dell'Ucraina per mano delle forze armate russe, evento di proporzioni drammatiche e oggi tristemente noto, ha segnato un passaggio netto nella definizione dei nuovi assetti geopolitici. Tutto questo ha innescato pesanti e profonde ripercussioni su quello che è il panorama della cybersecurity, avendo da un lato dato vita a una serie aggiuntiva di minacce e attacchi informatici, direttamente o indirettamente legati alla situazione contingente, dall'altra ha evidenziato in maniera netta alcuni limiti nelle catene di fornitura, anche nell'ambito delle soluzioni di difesa cibernetica.

Va detto che, oltre agli effetti dovuti alla mutata situazione geopolitica globale, si osservano anche evoluzioni proprie del panorama cibernetico, all'interno del quale le minacce continuano a evolversi, aumentando via via complessità ed efficacia di attacco. Le organizzazioni di tutto il mondo sono state prese di mira da una vasta gamma di attacchi informatici, sia da parte di cyber criminali che di attori statali. Questi ultimi utilizzano tecniche via via più sofisticate per condurre operazioni di spionaggio e sabotaggio a danno di governi, aziende e organizzazioni strategiche, al fine di assicurarsi una posizione di predominio.

Dal punto di vista della prevalenza, anche per quest'anno le minacce di tipo ransomware hanno dominato la scena, confermandosi il pericolo più rilevante per tutti i settori del mercato italiano. Degni di menzione sono stati anche i fenomeni di leak di codice sorgente ai danni di gruppi criminali, quale, ad esempio, quello subìto dal gruppo Conti. Questi fenomeni determinano, spesso, un vero e proprio riassetto nelle gerarchie e nei rapporti di forza dentro ai gruppi criminali e verso gruppi in competizione.

Oltre alla diffusione del ransomware, nel corso del 2022 è stato possibile rilevare prevalenze significative per attacchi di tipo DDoS, per campagne di phishing e per furti di dati sensibili degli utenti. In modo particolare si è osservato l'utilizzo di attacchi DDoS da parte di gruppi di hacktivisti, anche e soprattutto in relazione alla crisi Russo-Ucraina, per supportare oppure contrastare le ragioni dell'invasione russa verso l'Ucraina, a seconda dello schieramento e della propria ideologia.

Inoltre, abbiamo osservato un aumento degli attacchi ai sistemi industriali e di controllo, come quelli utilizzati per il controllo di produzione, per il monitoraggio e il funzionamento di centrali elettriche, oleodotti, reti di distribuzione di energia e, più in generale, infrastrutture critiche per il funzionamento di un Paese. Senza entrare nel merito delle ragioni sottostanti ad attacchi di questo tipo, appare piuttosto netta l'intenzione di portare attacchi in grado di mettere a rischio la sicurezza stessa di una nazione. A quanto sopra occorre infine aggiungere a livello tattico l'impiego di malware avanzati, progettati con il fine di utilizzare vulnerabilità zero-day, ovvero vulnerabilità sconosciute al momento del loro sfruttamento, quindi particolarmente sofisticate da individuare e prevenire.

I dati del rapporto

Per meglio comprendere i dati che seguono, è bene ricordare che Yoroi ha sviluppato i propri servizi di difesa attorno ad asset tecnologici proprietari in grado di assicurare le attività di monitoraggio di sistemi informativi complessi. Tra gli asset impiegati ricordiamo il sensore di network detection Genku, la sandbox Yomi, disponibile

anche sulla nota piattaforma VirusTotal, la tecnologia di Threat Intelligence, composta sia da feed automatici che da analisi e ricerche svolte dai nostri specialisti, e la soluzione di endpoint detection Kanwa. L'utilizzo sinergico di questi asset, integrato con i sistemi di difesa eventualmente presenti all'interno delle infrastrutture dei Clienti, costituisce il fondamento del Cyber Security Defence Center di Yoroi, un servizio avanzato di Managed Detection and Response (MDR) erogato attraverso un team dedicato di analisti su base 24/7.

I dati raccolti durante l'operatività del servizio CSDC, integrati da dati provenienti da fonti OSINT, costituiscono la base di conoscenza sulla quale è stato possibile organizzare le attività di analisi alla base del presente rapporto. È interessante osservare come il disporre di dati provenienti da attività reali di difesa permetta di stabilire relazioni causa-effetto rispetto ad eventi effettivamente accaduti e gestiti, fornendo quindi una maggiore accuratezza e affidabilità rispetto a semplici dati disponibili su fonti aperte o rispetto a rilevazioni esterne.

Le rilevazioni provenienti da reti esterne, d'altra parte, sono dati raccolti da sensori che permettono di fornire una telemetria adatta alla protezione proattiva dei clienti. Anche se questi dati possono fornire informazioni preziose sui cyber attacchi in corso, possono essere facilmente bloccati da protezioni perimetrali come firewalls, proxy, antivirus e antispam.

Utilizzare dati provenienti da incidenti reali di cyber security, invece, permette di ottenere statistiche più accurate e affidabili sui trend dei cyber attacchi e di comprendere meglio come essi colpiscono i diversi settori aziendali. Ciò può essere di grande aiuto per il lettore, che può utilizzare queste informazioni per essere più efficace nel contrastare le minacce di cybersecurity.

Sezione 1: Malware

Nel corso degli ultimi anni, è stato possibile assistere a una costante evoluzione delle minacce informatiche. In prima istanza, nel corso degli anni, si è rilevato un aumento del volume di codice malevolo intercettato dalle tecnologie che Yoroi ha introdotto. Inoltre, le informazioni ottenute analizzando le Tattiche, Tecniche e Procedure (TTP) degli attaccanti, suggeriscono una più netta distinzione tra gli attacchi opportunistici e quelli mirati. Gli attacchi mirati, infatti, hanno dimostrato una maggiore sofisticazione e precisione nella somministrazione del malware. Un esempio di evoluzione in ottica di sofisticazione si può ritrovare nel fenomeno della Double Extortion, che ha mostrato una crescente complessità e organizzazione. Questo fenomeno vede la formazione di gruppi strutturati in vere e proprie bande (gang) che hanno sviluppato malware unici per ogni attacco, quasi come una firma indelebile dell'attaccante.

Oltre ai fenomeni degli attacchi altamente organizzati per colpire un target specifico, nell'ultimo anno abbiamo osservato ed analizzato anche attacchi di tipo opportunistico, diffusi su larga scala, mirati a colpire il maggior numero possibile di aziende e di vittime.

Anche quest'anno il panorama delle minacce informatiche ha fatto vedere che la maggior parte delle problematiche sono state derivate dai cosiddetti "Crimeware" e "Commodity Malware", i quali sono usati come strumento per le fasi iniziali di un attacco informatico.

Nelle prossime sezioni ci sarà un approfondimento su questi specifici argomenti.

Le campagne malware nel 2022

I dati sono stati raccolti da diverse fonti, tra cui il team Yoroi di Cyber Threat Intelligence, il team di Incident Response, la piattaforma Cyber Security Defence Center e i partner. I dati sono stati attentamente esaminati per comprendere meglio le tendenze dei malware e le minacce a cui le organizzazioni sono esposte.

Dalle osservazioni compiute in questo periodo, è stato possibile riscontrare un aumento delle campagne di phishing e delle infezioni di ransomware, nonché una maggiore sofisticazione delle tecniche utilizzate dai criminali informatici.

La detection dei malware

Studiare statisticamente gli andamenti delle famiglie malware permette di contestualizzare e adattare al meglio la protezione dalle minacce informatiche. Uno dei parametri fondamentali per quanto riguarda lo studio delle minacce malware riguarda il fattore n-day, ossia catalogare temporalmente quando un certo campione malware viene scoperto. È però importante differenziare il caso in cui si evidenzia una nuova famiglia malware non nota, oppure nuove versioni di una famiglia malware già nota. A seconda della casistica, si deve organizzare l'addestramento degli strumenti di detection in maniera ottimale.

I risultati mostrano che la maggior parte dei malware individuati da Yoroi sono di tipo 0day, il che indica che i criminali informatici operano preferibilmente generando nuove varianti della stessa famiglia di malware e anche, più raramente, introducendo nuove famiglie di malware.

Questa tattica risulta particolarmente pericolosa in quanto, varianti sconosciute di un malware riescono a essere individuate e bloccate con fatica dalle soluzioni esistenti, non avendo necessariamente al loro interno similarità esplicite con artefatti binari già noti. Alla luce di questa osservazione, bisogna tener conto che una tattica di difesa valida debba necessariamente basarsi su approcci ibridi e adattativi, ossia che usano sia approcci di rilevamento basati su firme, sia approcci basati su Machine Learning e Intelligenza Artificiale, che permettono di identificare famiglie di malware in maniera adattiva. Inoltre, un ulteriore passo potrebbe essere anche quello basato su modelli definiti "anomaly based", ossia in grado di identificare le minacce informatiche a partire dalle modifiche che il malware effettua sul sistema che aggredisce.

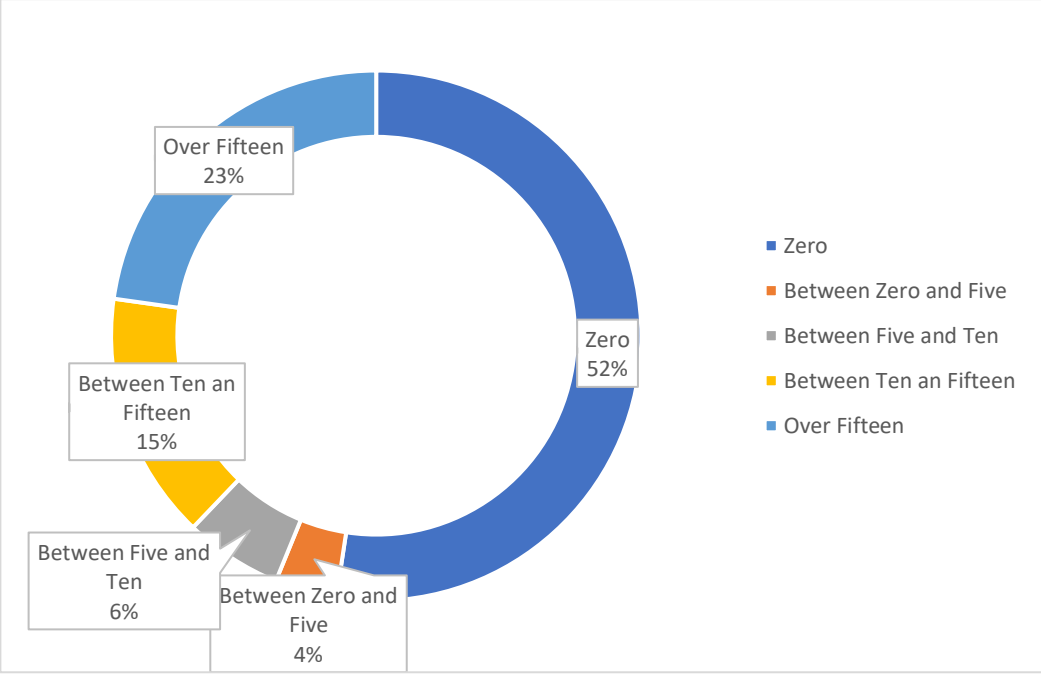

Figura 1: Distribuzione degli n-day malware

I risultati mostrati in Figura 1 indicano come il trend osservato sia sostanzialmente molto simile a quello rilevato nel corso del 2021, evidenziando come il 52,4% dei malware individuati siano di tipo zero-day. Il che significa che gli attaccanti continuano a preferire la generazione di nuovo codice per colpire i propri bersagli. Questi sono particolarmente pericolosi in quanto non possono essere facilmente individuati o bloccati dalle soluzioni di sicurezza esistenti.
Inoltre, il 3,8% dei malware individuati sono di tipo tra zero e cinque giorni, il 5,9% sono di tipo tra cinque e dieci giorni, il 15,1% sono di tipo tra dieci e quindici giorni e il 22,8% sono di tipo oltre quindici giorni.
I dati mostrano che i malware di tipo zero-day rappresentano la maggior parte dei malware individuati, seguiti da quelli di tipo tra zero e cinque giorni. Quando invece si rilevano dei malware che hanno una data n-day superiori ai quindici giorni, vuol dire che gli attori vanno a riutilizzare delle utility già note per compiere le proprie attività malevole, come ad esempio tutti i tool di “privilege escalation” e “movimenti laterali”, che una volta configurati opportunamente sono utili e portano a termine il loro compito, nonostante il fatto che i motori di detection li riconoscano.

Impacted industries

Altro aspetto interessante da analizzare è la presenza di una specializzazione rispetto ai target industriali. In altre parole, è di interesse riuscire a tracciare la distribuzione delle minacce per settore industriale. Comprendere le minacce informatiche che un'azienda potrebbe affrontare è fondamentale per implementare le giuste misure di sicurezza. Uno strumento utile per orientare queste misure è lo studio della distribuzione delle categorie di minacce rispetto ai settori di business.

Grazie a questa attività di analisi, è possibile indirizzare le risorse e le strategie di sicurezza verso le aree maggiormente a rischio, garantendo una protezione adeguata all’azienda. Inoltre, tale analisi può anche fornire informazioni utili per valutare il livello di maturità della sicurezza informatica di un'azienda e per individuare eventuali carenze o aree di miglioramento.

La figura 2 mostra come le minacce informatiche colpiscono i diversi settori industriali che Yoroi difende quotidianamente tramite tecnologie proprietarie.

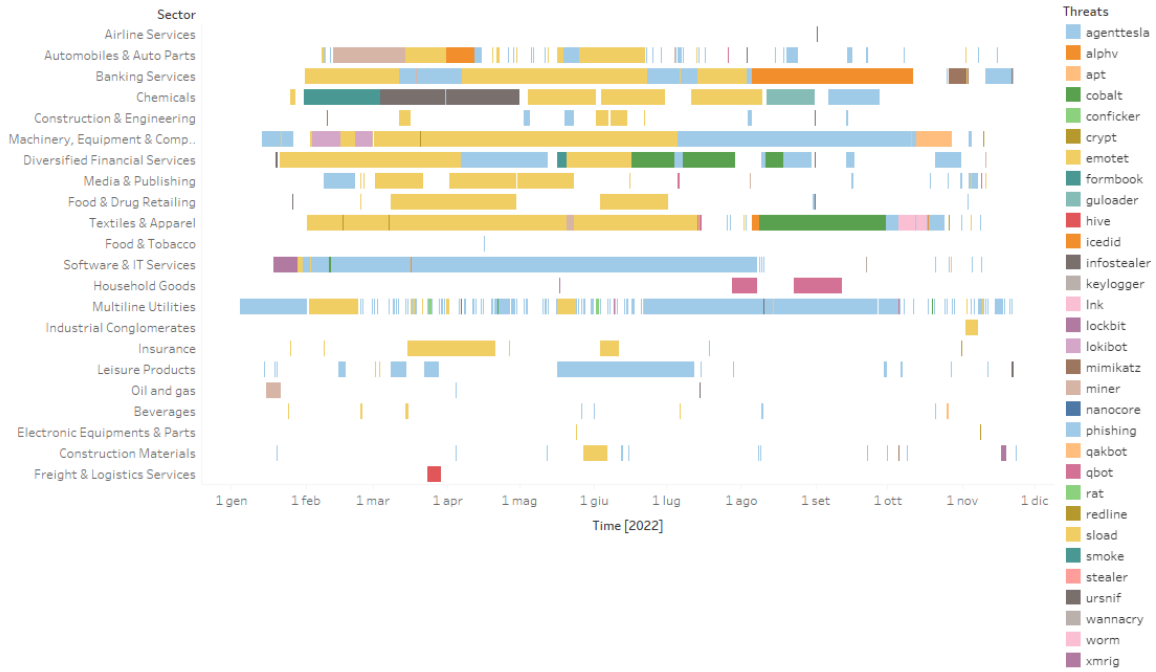

Figura 2: Frequenza delle minacce informatiche in funzione del settore industriale

Dal precedente grafico emerge la presenza di alcune minacce molto frequenti classificabili come prettamente di natura opportunistica, che provano a colpire in maniera indifferenziata ogni organizzazione. Contemporaneamente sono presenti altre minacce orientate a colpire, in maniera più aggressiva, settori specifici. Queste ultime minacce vengono classificate come operazioni di tipo “mirato” (targeted).

Altra interessante osservazione (Figura 2) è che ci sono alcune tipologie di business più esposte a pressioni e attacchi in maniera continuativa rispetto ad altre. Questo significa che gli attaccanti specializzano il metodo di attacco in funzione del tipo di vittima e della motivazione sottostante all’operazione da realizzare. Infatti, alcune tipologie di attacco, presentano periodicità precise e metodi simili, indicando la natura opportunistica dell'operazione. Di altra evidente natura sono gli attacchi realizzati con strumenti più sofisticati e specializzati, al fine di avviare un attacco informatico più complesso e dotato di caratteristiche specifiche.

È molto interessante notare la forte presenza di colori come il “giallo” e l’“azzurro” rispettivamente appartenenti a minacce di tipo “emotet” ed “AgentTesla” in relazione alla rilevante presenza in alcuni settori industriali. Nel caso di Emotet è possibile osservare la sua maggiore presenza nel settore “bancario, assicurativo, finanziario” evidenziando il suo retaggio storico come Trojan Banker. Contrariamente, “AgentTesla” è principalmente presente nei settori industriali (Machinery, Utilities, Fashion) e nel settore Software/IT Services. Quest’ultimo settore (Software / IT) può apparire incoerente con i precedenti in prima istanza, ma se analizziamo nel dettaglio il mercato, è facile osservare che le organizzazioni industriali fanno un forte utilizzo di fornitori appartenenti a settori IT e Software. Molto spesso, infatti, AgentTesla è stato utilizzato per compromettere la filiera di produzione e di approvvigionamento industriale di numerose vittime nel 2022.

La seguente infografica fornisce un'evidenza più dettagliata di questo fenomeno, mostrando come le principali minacce vengono distribuite lungo il periodo temporale di un anno.

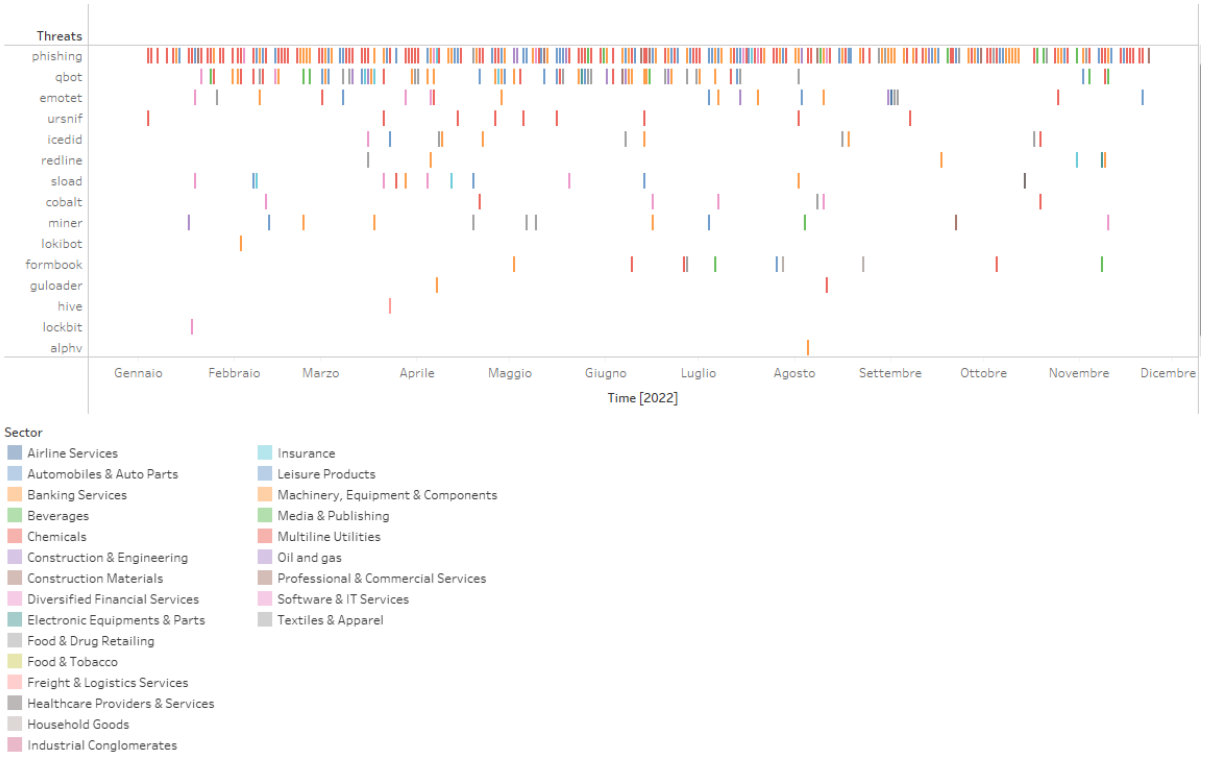

Figura 3: Distribuzione delle minacce informatiche in Italia per settore

La Figura 3 evidenzia un'altra prospettiva rispetto alla precedente figura, ovvero la distribuzione delle minacce informatiche in relazione all'arco temporale (pari ad un anno solare) rispetto ai settori di business attaccati. È possibile evidenziare una ricorsiva stagionalità di alcune minacce relative a specifici settori industriali e al contempo è possibile evidenziarne l'indipendenza di altre.

Anche quest'anno la principale minaccia da affrontare è, senza dubbio, quella del phishing, che colpisce in maniera indiscriminata ogni vittima.

La minaccia del phishing è universale perché può colpire chiunque, indipendentemente dall'età, dall'occupazione o dalla posizione geografica. È facile per gli attaccanti, applicando tecniche di social engineering oppure attraverso informazioni provenienti da social networks, creare messaggi di phishing convincenti e siti web falsi. Poiché tali messaggi e website possono assumere l'aspetto e il comportamento di quelli di aziende o di organizzazioni legittime, un singolo attimo di distrazione può essere fatale per la vittima.

La seconda minaccia più diffusa sono i cosiddetti commodity malware, ossia malware che vengono utilizzati in modo diffuso e che sono facilmente acquistabili online. Questi tipi di malware sono spesso utilizzati dai cyber criminali per diffondere principalmente infostealer, ovvero strumenti capaci di rubare informazioni sensibili – come, per esempio, password e dati finanziari - e loaders, che hanno come ultimo scopo quello di installare altro malware sulle macchine delle vittime.

I commodity malware sono particolarmente pericolosi perché sono facilmente accessibili e possono essere acquistati online da chiunque abbia le competenze tecniche per effettuare un acquisto in un tradizionale e-commerce. Inoltre, poiché questi malware vengono diffusi ampiamente, possono colpire un gran numero di vittime in tutto il mondo. Chiunque può essere una vittima di un attacco di commodity malware, poiché possono essere diffusi attraverso messaggi di posta elettronica di phishing, link dannosi in siti web, o attraverso l'utilizzo di software vulnerabile o non aggiornato.

Tra quelli che sono stati maggiormente osservati nel corso del 2022 ci sono stati in primis Qbot, che ha preso il posto di altri due trojan bancari, i quali la facevano da padrone negli anni passati, ma comunque ancora attivi anche quest'anno: Emotet e Ursnif. In dettaglio, Emotet nel corso del 2021 sembrava essere stato smantellato dalle forze dell'ordine, ma invece si è rivelata solo una pausa di qualche mese, tornando poi a essere più forte che mai; Ursnif, malware che ha ridotto la costanza degli attacchi, ma con un evidente "rebranding" verso l'utilizzo in scenari sempre più mirati, utilizza temi di Phishing sempre più subdoli e che inducono le vittime a cliccarci.

Mano a mano che si scende verso posizioni meno rilevanti nella classifica per diffusione, si evidenziano anche prime tracce di malware molto sofisticati, tipicamente relativi alle ultime fasi della krill chain. Un esempio sono i payload ransomware, i quali vengono rilasciati da parte degli attori malevoli solo al momento finale di un attacco. Dei ransomware e del fenomeno della Double Extorsion ne parleremo più avanti nel relativo paragrafo dove ne approfondiremo i dettagli.

I dati provenienti dal mondo

Dopo aver presentato in sintesi i dati sulle minacce rilevate nel corso del 2022 sui Clienti difesi dalla tecnologia Yoroi, l'attenzione si focalizza ora nell'analizzare le tendenze a livello globale e la distribuzione statistica della diffusione di codice malevolo. I risultati presentati nel seguito sono frutto delle attività di analisi svolta a livello globale dal team di Threat Intelligence di Yoroi.

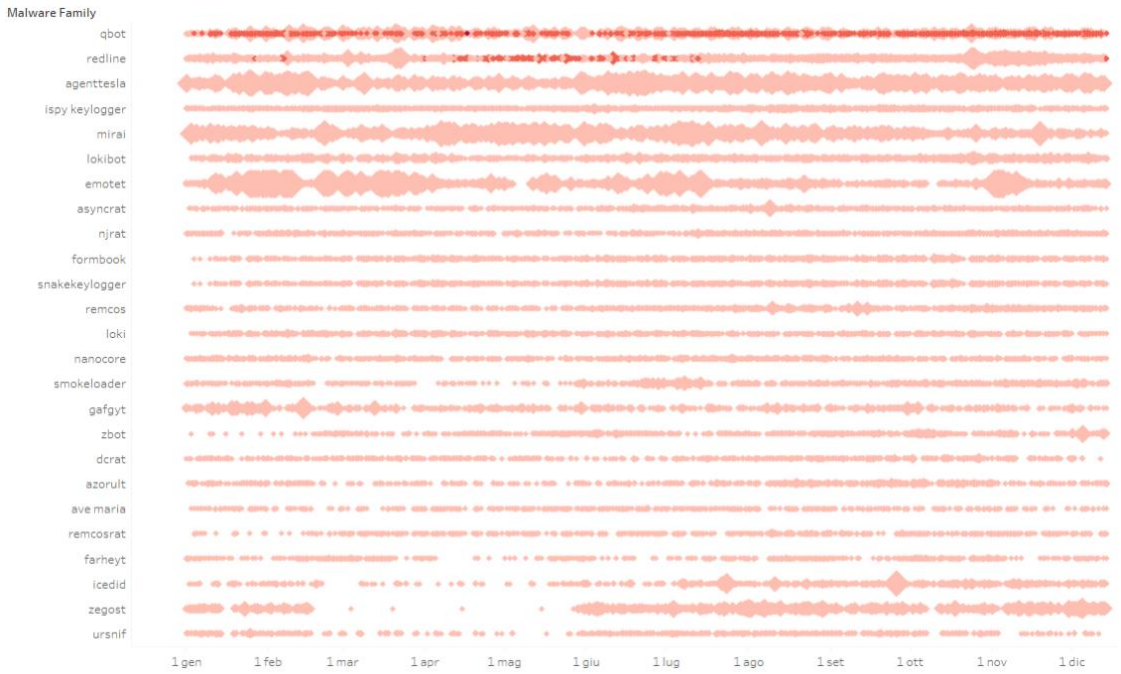

Figura 4: Distribuzione temporale dei principali malware nel mondo

I risultati ottenuti dalle analisi svolte dal team, ponendo in relazione le osservazioni rilevate su scala italiana con i dati disponibili a livello globale, evidenziano la presenza di pattern ricorrenti.

In Figura 4 sono riportati i dati di prevalenza, su scala temporale, delle minacce rilevate a livello globale.

È possibile notare come, anche in questo caso, la minaccia prevalente per il 2022 sia stata Qbot sia per quantità sia per persistenza a livello temporale, interessando sostanzialmente l'intero anno. Emergono però anche delle differenze rispetto ai dati analizzati precedentemente, in particolare è possibile notare come la classifica dei top 25 malware sia tutta composta da crimeware e commodity malware. Questa tendenza è prevedibile in quanto si è in presenza di minacce di tipo "General Purpose", che colpiscono indistintamente qualsiasi target in qualunque parte del mondo.

Un'altra importante differenza tra le osservazioni a livello italiano e quelle globali è rappresentata dai volumi dei dati osservati e dall'importanza di alcune campagne, quali, ad esempio, quelle di AgentTesla e di Emotet, di gran lunga superiori al contesto domestico. A questo va associata anche la tendenza dei gruppi criminali a cambiare target, su base periodica, mantenendo comunque il volume di malspam molto elevato per i vari settori interessati.

Un altro dato di interesse che si evince dalla Figura 4 è la presenza significativa di malware appartenenti alle macro-famiglie di Infostealer e di Keylogger. Questo dimostra il particolare interesse da parte delle comunità criminali per il settore di compravendita di credenziali, necessarie per ottenere gli accessi iniziali alle vittime, per poi accompagnare altre tipologie di attacchi più mirati, soprattutto di tipo ransomware e double extorsion.

La considerazione generale che, quindi, può essere dedotta dalle informazioni che sono state rilevate, è che il grosso del volume di malware, che raggiunge cifre di milioni di campioni malware differenti all'anno, serve a garantire agli attori criminali una via di ingresso privilegiata all'interno delle infrastrutture obiettivo, su cui poi agire in maniera mirata. Per questo motivo, nell'ultimo anno, ha rafforzato il suo potere all'interno dell'ecosistema dell'underground la figura del broker di compravendita degli accessi alle aziende. Questo servizio ha preso il nome di **IAaaS**, ossia **Initial Access as a Service**.

Sezione 2: Le minacce bloccate

Implementare strategie e politiche in grado di ridurre il rischio cyber, assicurando allo stesso tempo l'operatività di un'Azienda, rappresenta una sfida complessa per le organizzazioni, poiché richiede di bilanciare la protezione dei sistemi informativi con la loro fruizione da parte degli utenti. Ciò significa che le organizzazioni devono trovare il giusto equilibrio tra la sicurezza e la facilità d'uso, in modo da proteggere i sistemi senza rendere troppo difficile per gli utenti accedervi e utilizzare i servizi.

Per raggiungere questo obiettivo, le organizzazioni devono affrontare una varietà di incognite, come nuove minacce informatiche emergenti, vulnerabilità sconosciute nei sistemi e comportamenti imprevedibili degli utenti. Inoltre, devono gestire una quantità considerevole di indicatori di compromissione, come avvisi di sicurezza, segnalazioni di vulnerabilità e rapporti di attacchi effettuati.

Gli analisti e i progettisti del sistema di protezione devono lavorare insieme per garantire una buona usabilità per gli utenti senza compromettere la sicurezza dei sistemi. Ciò può includere la progettazione di interfacce utente

intuitive, la formazione degli utenti su come riconoscere le minacce e la creazione di processi di autenticazione robusti per proteggere l'accesso ai sistemi. Allo stesso tempo, si devono anche adottare misure di prevenzione efficaci per bloccare eventuali minacce, come software di sicurezza aggiornati e procedure di sicurezza rigorose.

Il Domain Name System (DNS) è un protocollo applicativo che viene utilizzato nelle reti IP per tradurre gli indirizzi delle risorse (quali ad esempio siti web) in indirizzi IP e viceversa, permettendo agli utenti di utilizzare le risorse messe a disposizione dai sistemi digitando semplicemente il loro nome. Tuttavia, gli attaccanti informatici possono sfruttare il DNS per diffondere malware e condurre attacchi di phishing, reindirizzando gli utenti a siti web falsi o malevoli.

Per proteggere i sistemi dalle minacce legate al DNS, le organizzazioni possono utilizzare tecnologie di "DNS Defense", che sono progettate per monitorare e bloccare i domini malevoli, ovvero quelli utilizzati dagli attaccanti informatici per diffondere malware e condurre attacchi di phishing. Avere un'ottima copertura dei domini malevoli permette alle organizzazioni di prevenire le infezioni a diverse fasi della cosiddetta "Infection Chain", ovvero il percorso che gli attaccanti seguono per diffondere il malware.

Investire in tecnologie di DNS Defense all'avanguardia, quindi, può aiutare le organizzazioni a proteggere i loro sistemi dalle minacce informatiche e a prevenire le infezioni. Tuttavia, è importante notare che queste tecnologie devono essere utilizzate in combinazione con altre misure di sicurezza, come il software di sicurezza aggiornato e le procedure di sicurezza rigorose, per garantire una protezione efficace.

I domini malevoli possono essere utilizzati in diversi modi dai malware. Ad esempio, possono essere utilizzati per scaricare il "payload" del malware, ovvero il codice dannoso, in caso di infezioni multi-stage come Qbot, Emotet o Ursnif. Oppure, possono essere utilizzati per comunicare con il "Command and Control" del malware, ovvero il sistema che gli attaccanti utilizzano per controllare gli impianti infetti. In questo caso, le tecnologie di DNS Defense possono aiutare a prevenire attacchi come Sunburst, visto anche l'anno scorso, che utilizza un sofisticato sistema di algoritmi di DGA (Domain name Generation Algorithm) per la comunicazione con il proprio C2, o aiutare a bloccare comunicazioni di backdoor appartenenti a CobaltStrike, che spesso utilizza il protocollo DNS come mezzo di scambio di informazioni e comandi.

Per affrontare in maniera adeguata queste minacce, le organizzazioni possono utilizzare tecnologie come il DNS Defense di Yoroi per monitorare il traffico di rete DNS e identificare gli attacchi informatici in diverse fasi dell'intrusione. Yoroi utilizza una combinazione di fonti di informazioni, sia pubbliche (OSINT) che private (CLOSINT), e si avvale di un team di analisti che esaminano il malware intercettato sui sistemi dei clienti per arricchire la propria base di conoscenze. Inoltre, Yoroi utilizza processi automatizzati e manuali per correlare e verificare le informazioni ricevute dalle varie fonti.

Utilizzare tecnologie come il DNS Defense di Yoroi può aiutare le organizzazioni a prevenire, identificare e mitigare gli attacchi informatici che sfruttano il traffico di rete DNS.

Nel corso del 2022, la tecnologia di DNS Defense di Yoroi ha intercettato e bloccato 1.743.742 richieste DNS malevole distribuite come in Figura 5.

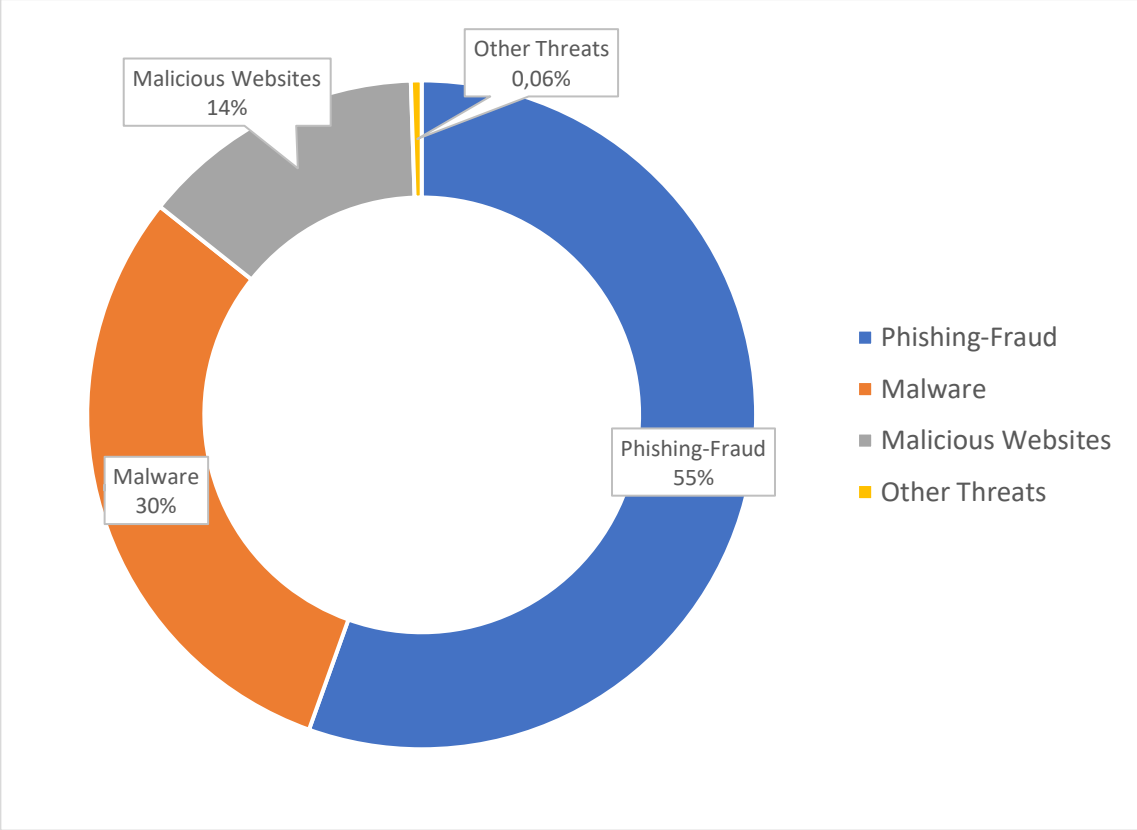

Figura 5: Distribuzione delle minacce informatiche bloccate dalla DNS Defense di Yoroi

In particolare, più della metà delle richieste DNS bloccate appartenevano a domini identificati come fraudolenti o indicatori di attività di phishing in corso. Il restante 30% sono domini legati ad attività di malware (C&C, ...) mentre il 14% sono siti web malevoli. Il trend si conferma essere comunque costante prendendo in considerazione anche quel che è stato osservato gli anni scorsi, confermando la tendenza da parte degli attaccanti a distribuire minacce a più larga scala adottando la tecnica del social engineering, per poi passare ad attacchi sempre più mirati una volta ottenuto il vettore di ingresso iniziale desiderato.

Questo dimostra che per le organizzazioni, un fattore vincente per la propria protezione contro le minacce informatiche è rappresentato da una seria campagna di sensibilizzazione dei dipendenti in materia di security awareness, dove deve essere spiegato che ogni persona che ha a che fare con il contesto aziendale ha un impatto non trascurabile nel contesto della cybersecurity.

Botnets and Opportunistic Activities

Tracciare le infrastrutture degli attaccanti è un'altra sfida che Yoroi quotidianamente affronta. Quando si lavora con tecnologie di DNS Defense per monitorare e bloccare i domini malevoli, è importante prestare particolare attenzione alla gestione delle sorgenti di informazioni. Questo perché alcuni domini malevoli potrebbero essere condivisi con servizi legittimi, ovvero servizi che non hanno intenti dannosi e sono utilizzati in modo lecito.

In questi casi, è necessario agire con cognizione di causa, ovvero fare un'attenta valutazione delle sorgenti di informazioni per determinare se è opportuno mettere in bloccaggio determinati domini o meno. Ciò richiede di fare un'accurata analisi dei dati e di utilizzare processi di verifica accurati per assicurarsi che le informazioni siano corrette. In questo modo è possibile proteggere i sistemi dalle minacce informatiche, senza compromettere l'usabilità dei servizi legittimi.

Di seguito il grafico con la distribuzione delle minacce informatiche che le tecnologie di Yoroi hanno permesso di intercettare in funzione del paese di appartenenza.

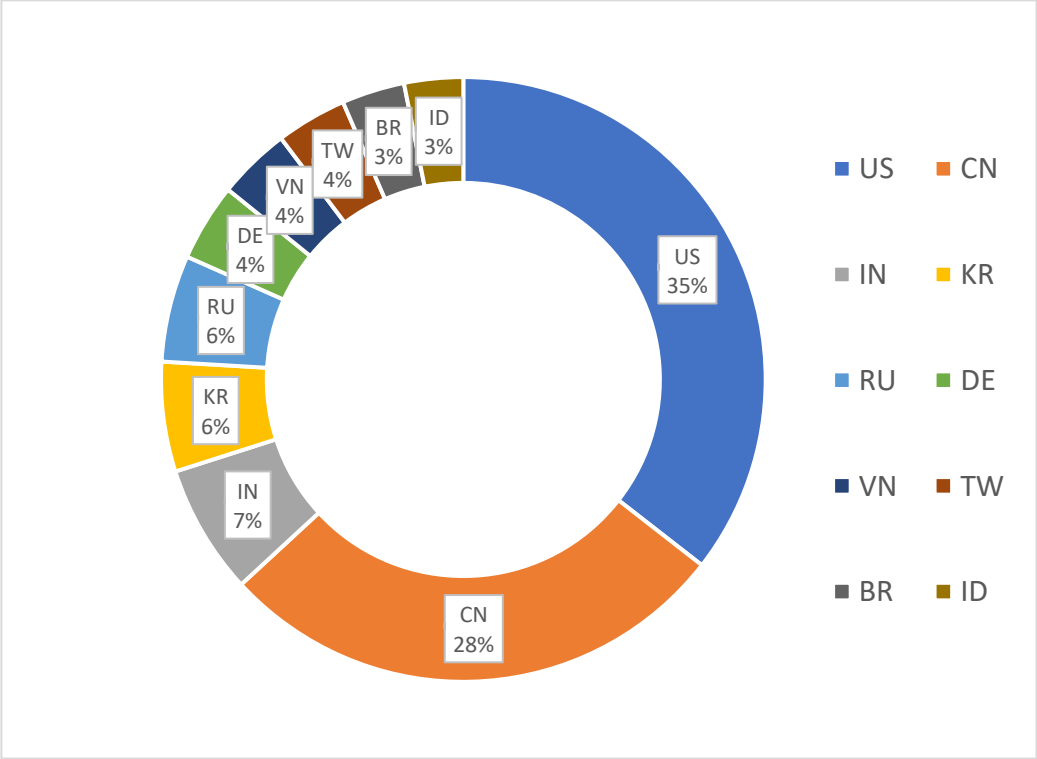

Figura 6: Distribuzione territoriale delle minacce

La distribuzione delle minacce avvenute nel corso del 2022 conferma che la maggior parte delle infrastrutture degli attaccanti risiede in territorio US con il 35% delle minacce registrate. Invece, il 28% delle minacce rilevate e bloccate dalla nostra telemetria proviene dalla Cina, registrando un significativo aumento rispetto all'anno scorso. Il terzo posto quest'anno è stato guadagnato dagli attacchi proveniente dall'India con il 7% del totale.

Il conflitto Russo-Ucraino: attacchi mirati e botnet

Gli importanti avvenimenti di attualità ci impongono di approfondire gli attacchi provenienti dalla Russia e a fornire loro una contestualizzazione. Durante le osservazioni afferenti al periodo precedente, la Russia deteneva il terzo posto della classifica, mentre in quest'ultimo periodo di osservazione, a seguito dell'attuale conflitto, si è potuta osservare una netta ascesa di tali minacce afferenti al perimetro Russo.

Un'altra attività afferente all'ascesa del conflitto Russo-Ucraino si è manifestata con la presenza di nuovi malware di tipo Wiper, altamente sofisticati, realizzati per compiere atti di sabotaggio molto precisi contro le infrastrutture critiche dell'Ucraina. Alcuni degli Wiper più sofiticati sono stati analizzati tempestivamente dal team ZLab di Yoroi al fine di offrire una risposta completa e immediata alla minaccia in corso. Nella seguente immagine viene mostrato uno dei cicli di cifratura più interessanti dell'anno, ovvero quello adottato da HermeticWiper.

Figura 7: Estratto dell'analisi di HermeticWiper

Non tutte le minacce rivolte all'Ucraina sono state di tipologia "Wiper"; infatti, un importante fronte di attacchi rilevanti nel contesto cibernetico sono stati attacchi di tipologia dimostrativa o ideologica da parte di collettivi filorussi come, per esempio, il famigerato gruppo Killnet, che ha effettuato numerosi attacchi di tipo DDoS (Distributed Denial of Service), attraverso botnet. Tali attacchi non hanno colpito solo obiettivi ucraini ma sono stati sferrati anche contro tutte le nazioni che hanno supportato l'Ucraina durante questo conflitto. In questo caso, però, occorre precisare che gli attacchi, benché massivi a livello infrastrutturale, dipendevano direttamente dallo stato Russo, ma geograficamente sono stati effettuati in modalità "distribuita" tramite botnet distribuite, per definizione, in maniera capillare in tutto il mondo e non solo nei paesi Russofoni.

Per questi motivi la minaccia proveniente dalla Russia va bene contestualizzata e messa a confronto con quella che è la realtà, e quindi non solo in riferimento al piano cyber. Il CERT di Yoroi, durante l'apice del conflitto, ha

partecipato attivamente a call di allineamento con gli altri CERT globali, in particolare nell'ambito della rete **Trusted Introducer,** di cui è membro certificato già dal 2020.

Sezione 3: Le minacce E-mail

Anno dopo anno, il mezzo e-mail si conferma essere quello preferito da parte degli attaccanti per far breccia all'interno dei sistemi informatici di ignare vittime. Questo è dovuto principalmente alla loro efficacia nel superare le misure di sicurezza perimetrali, ovvero le tecnologie e le politiche che vengono utilizzate per proteggere una rete informatica dalle minacce esterne. Le e-mail, infatti, utilizzano anche tecniche di social engineering per convincere le persone a cliccare su un link o allegato dannoso, permettendo così all'infezione di diffondersi all'interno della rete.

Le e-mail sono anche un mezzo molto "scalabile", poiché possono essere inviate ad un gran numero di destinatari in modo rapido e facile. Inoltre, gli attaccanti possono utilizzare utenze infette per la propagazione delle minacce, in modo da aumentare la probabilità che esse vengano aperte e consultate. In genere, le minacce che si osservano su malspam sono delle campagne massive effettuate da commodity malware e malware che vengono usati per effettuare le prime operazioni di backdooring, per poi passare a software di intrusione manuale, una volta ottenuto un punto di accesso iniziale.

In altri casi, invece, può capitare che l'allegato malevolo possa contenere direttamente del malware riconducibile ad attività APT, quindi altamente mirata. Questi casi Yoroi li ha intercettati e analizzati all'interno di thread di PEC, la Posta Elettronica Certificata. Il motivo dell'attacco era contestualizzato al conflitto russo-ucraino, che a livello di attenzione dell'opinione pubblica ha polarizzato particolarmente l'interesse, superando addirittura il tema della pandemia del COVID-19 che ha dominato le scene degli anni 2020 e 2021.

Inoltre, di particolare rilevanza è stata l'evoluzione delle tecniche di attacco degli attori criminali apprezzate durante gli ultimi anni. Essi si sono accorti che utilizzare i documenti Office con macro non è una strategia efficace per portare avanti le campagne di malspam, per cui sarà affrontato anche l'aggiornamento dell'evoluzione delle tecniche di dropping del malware.

Analisi delle campagne mail

Le campagne di malspam sono configurate per colpire allo stesso modo piccole e grandi organizzazioni, ad esempio inviando e-mail di finte fatture con documenti Office malevoli che richiedono l'abilitazione delle macro per la visualizzazione del contenuto. Quando un utente abilita le macro, il malware viene eseguito e il dispositivo viene infettato.

Una volta preso il controllo di tali dispositivi, è possibile utilizzare questi ultimi per attaccare obiettivi di alto valore tramite e-mail di spear-phishing. Lo spear-phishing è una forma di phishing mirato, che utilizza messaggi di posta elettronica personalizzati per convincere la vittima a cliccare su un link o allegato dannoso. Gli attacchi spear-phishing sfruttano temi specifici e l'accesso a caselle di posta fidate per rendere le e-mail più credibili.

Questo fino ad ora era lo scenario più comune che veniva affrontato, ma, come verrà approfondito nei prossimi paragrafi, le catene di attacco che partono dalla malspam hanno subìto una notevole evoluzione negli ultimi anni con tecniche sempre più esotiche e sofisticate.

Analizzando i dati provenienti dalla telemetria del Cyber Security Defense Center di Yoroi, si è riscontrata una variazione significativa nelle strategie di attacco da parte di attori malevoli. Di seguito le statistiche relative ai dati collezionati nell'anno 2022.

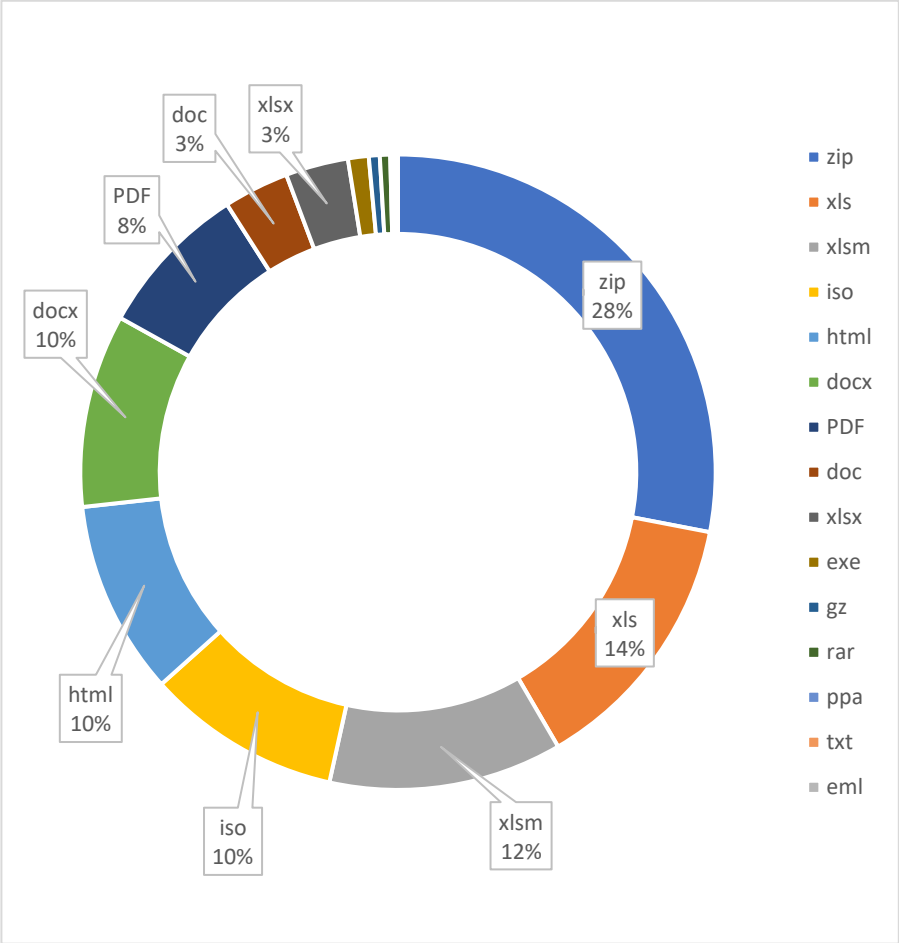

Figura 8: Distribuzione degli allegati malevoli

La distribuzione delle minacce condivise via mail mostra subito che, quest'anno come non mai, gli attaccanti hanno cambiato strategia per la modifica della catena di attacco, diversificando il modo di operare. Infatti, l'allegato più comune identificato durante l'anno di competenza include con il 28% il formato "zip". I formati archivio hanno avuto un'impennata clamorosa di utilizzo da parte degli attaccanti per il fatto che ad oggi i sistemi di detection delle minacce sono addestrati robustamente per riuscire a individuare quali sono i documenti malevoli. Quindi, lato attaccante, per evitare di essere rilevati immediatamente, hanno trovato un escamotage tanto semplice quanto efficace: hanno deciso di comprimere il documento con un archivio protetto da una password in modo tale che gli strumenti di analisi automatizzata non possono ispezionare il file.

Yoroi per questo motivo ha adottato nelle proprie SandBox un sistema di identificazione della password all'interno del corpo della e-mail e una successiva attività di brute forcing per estrarre il documento compresso.

Il secondo e terzo posto della classifica sono occupati dai formati Office di Excel, rispettivamente XLS con il 14% e XLSM con il 12%. Qui ritornano i file di Office che gli anni passati hanno tormentato le caselle di posta elettronica di tutto il mondo. Nello specifico, sono sia file con le macro, sia i file di XLM macro, diventate famose a partire dal 2019.

Con il 10% ciascuno di distribuzione abbiamo poi i file di Word, sempre presenti e adottati tutti per ogni tipologia di minaccia, che hanno subìto un grave calo dell'adozione da parte degli attaccanti dopo l'annuncio di Microsoft di disabilitare di default le macro dagli applicativi di office. Ma questo ha "incentivato" gli attaccanti a trovare altri mezzi, tra cui la vulnerabilità, la CVE-2022-30190, conosciuta anche con l'alias **Follina**.

I formati che realmente hanno segnato quest'anno come distribuzione sono quelli delle ISO, HTML: i primi sono stati usati come archivi con una metodologia simile a quella degli zip riutilizzando una tecnica molto nota e diffusa nel 2017-2018 (si invita il lettore a prendere visione dei report di quell' epoca); invece gli HTML sono dei file di markup che, attraverso la tecnica del "HTML Smuggling" permettono di effettuare il download automatico di ulteriori componenti dalla rete. Questi sono spunto poi di riflessione per il paragrafo successivo dove discuteremo dell'evoluzione delle tecniche di drop degli attaccanti.

Un altro elemento rilevante presente negli allegati di posta elettronica è il formato PDF, con il suo 8% di distribuzione sulla telemetria Yoroi. Questi possono essere utilizzati in due modi diversi per arrecare danno alle vittime: il primo è quello di sfruttare le vulnerabilità che costantemente emergono per i lettori di tale formato; l'altra invece è quella di contenere un link malevolo che permette il download dalla rete dell'effettivo componente malevolo.

L'evoluzione delle drop chain e il risveglio degli altri formati

Il 2022 ha segnato un'evoluzione significativa della drop-chain, ossia di tutta la catena per inoculare malware all'interno dei sistemi informatici della vittima. La stretta di Microsoft nell'avvisare l'utente della presenza di codice macro nei documenti Office e la presenza di strumenti di emulazione di documenti sempre più efficace, ha spinto gli attaccanti a investire nello sviluppo di nuove tecniche sempre più complesse e performanti al fine di aggirare tali ostacoli.

Da un lato resta sempre presente con un impatto non trascurabile lo sfruttamento delle vulnerabilità "zero click", ovvero vulnerabilità che non necessitino di particolari azioni da parte dell'utente se non la semplice apertura del documento. "Follina" (CVE-2022-30190) è il principale esponente di questo settore. Il 30190 del 2022 è un bug che interessa il vendor Windows, in particolare il suo prodotto Microsoft Office. Tale falla consente l'esecuzione di codice arbitrario attraverso MSDT (Microsoft Support Diagnostic Tool), uno strumento di diagnostica del supporto tecnico di Microsoft che gli utenti possono utilizzare per ricevere assistenza in caso di problemi. La vulnerabilità è stata prima sfruttata in modalità 0-day a partire da Aprile 2022, quando inizialmente è stato osservato lo sfruttamento di una particolare tecnica di "Template Injection", fino a maggio, quando è stata ufficialmente riconosciuta come vulnerabilità a sé stante, e continua a essere usata tutt'oggi in attacchi altamente specializzati.

Dall'altro lato nel 2022 è stato possibile osservare un allungamento delle catene di infezione da malware con una maggior attenzione da parte degli attori criminali nel provare a proteggere i documenti malevoli e i loro loader con involucri che, sia secondo gli apparati di protezione, sia secondo gli utenti, potrebbero essere definiti più affidabili rispetto agli altri. Infatti, si è osservato come utilizzando archivi, che siano ZIP, ISO, VHD o altri, si riduca

notevolmente la detection dei sistemi di difesa della vittima. Per funzionare, tale tipologia di allegato malevolo prevede una maggiore interazione da parte dell'utente. L'utente necessita di aprire l'archivio e di effettuare "click" sul documento contenuto. Questo significa che gli attaccanti sono stati forzati a migliorare notevolmente le proprie capacità di social engineering al fine di convincere le vittime ad aprire gli archivi, e inserire le password contenute nel testo dell'e-mail. Come tendenza generale è possibile osservare un progressivo aumento di complessità e sofisticazione delle catene di attacco, conseguenza naturale del generale aumento di consapevolezza della minaccia da parte degli utenti.

Altri formati di file confermati altamente pericolosi e ampiamente utilizzati dai criminali informatici possono essere classificati come formati esotici di tipologia XLL. Di tali file abbiamo trattato ampiamente nel report dell'anno scorso. Un altro formato ampiamente utilizzato soprattutto nelle campagne di fine anno sono stati i file di tipologia "link" LNK, ovvero file di collegamento utilizzati da Microsoft Windows. Essi molto spesso sono stati individuati all'interno degli archivi protetti che, tramite la tecnica del side-loading ,ha permesso al sistema malevolo di eseguire codice sulla macchina vittima sfruttando componenti legittimi di altri applicativi.

L'abuso dei framework di Command and Control da parte degli attaccanti

Da quanto è emerso dal panorama delle minacce informatiche, quella della Double Extorsion si è rivelata essere una minaccia sempre più condotta da operatori umani. Essi usano allo stesso modo degli esperti di sicurezza informatica, strumenti di red teaming per penetrare, soggiornare ed esfiltrare informazioni all'interno della rete vittima. Nel corso degli ultimi anni, abbiamo tracciato numerose intrusioni informatiche ponendo particolare attenzione agli strumenti utilizzati. Gli strumenti più adottati dagli attaccanti, soprattutto nelle fasi centrali dell'attacco, hanno subìto un notevole cambiamento rispetto agli anni precedenti.

Inizialmente, la maggior parte degli strumenti adottati da attori criminali provenivano dalla rete, erano open source e largamente diffusi in comunità. Alcuni di questi strumenti sono stati realizzati da ricercatori-affiliati o da ricercatori-indipendenti al fine di migliorare l'ecosistema digitale. Tuttavia, rilasciando pubblicamente tali strumenti, anche attori malevoli non hanno tardato ad adottarli per velocizzare e migliorare la loro capacità di penetrazione e al contempo per depistare il loro operato.

Metasploit è sicuramente uno dei framework di exploiting più affermati e anche uno dei più anziani in assoluto. Sviluppato a partire dal 2003 esso è uno strumento di riferimento per chi vuole partire dalle prime armi e cimentarsi nelle pratiche del penetration testing. Allo stesso tempo è stato ampiamente utilizzato da attori avversari sia motivati da lucro come FIN7, sia sponsorizzati da stati "canaglia" come il noto gruppo APT Kimsuki. Un altro strumento ampiamente utilizzato nel panorama del "dual usage", ovvero strumenti utilizzati sia per attaccare che per difendere, è il noto Meterpreter, sofisticata backdoor in grado di compiere operazioni molto complesse in maniera quasi trasparente agli apparati di sicurezza di prima generazione.

Empire è un ulteriore strumento di Post-Exploitation. Il post-exploitation è l'insieme di tutte quelle attività che avvengono dopo l'installazione di una backdoor. Questo strumento è utilizzato per la propagazione all'interno del perimetro aziendale, in quanto contiene numerosi moduli adatti a effettuare attività di privilege escalation di movimento laterale. Inoltre, le comunicazioni con il C2, attraverso questo strumento, sono protette tramite algoritmi di cifratura, rendendo così difficile l'analisi del contenuto del traffico. Anche in questo caso, sono stati

tracciati numerosi attaccanti che fanno uso di Empire, sia in ambito Cyber-Crime, come FIN10 e Wizard Spider, sia in ambito APT, come APT41 e Turla.

Oltre a questi strumenti appena elencati, ve ne son altri non facilmente utilizzabili se non a seguito di una licenza che prevede un corrispettivo economico. Tali framework sono stati implementati durante gli anni da organizzazioni professionali o da privati professionisti per migliorare e velocizzare assesment tecnologici e di perimetro. Tuttavia, i Threat Actors accedono a tali strumenti, sia compromettendo attraverso tecniche di cracking software acquistati da terzi, sia cercando versioni compromesse direttamente online (torrente, canali telegram, forum). In caso di attori criminali sponsorizzati da Stati, essi possono acquistare tali strumenti tramite società fittizie (o amiche) nelle quali scaricare il costo della licenza facendo sembrare tale acquisto legittimo.

Cobalt Strike è senza dubbio, ancora una volta, lo strumento di post-exploitation più adottato nel 2022. Infatti, benché nato come strumento di supporto per le attività di red teaming, Cobalt Strike ha riscosso un enorme successo grazie a due fattori principali:

- L'interfaccia di gestione che permette di tenere sott'occhio tutto lo stato di avanzamento della compromissione del perimetro aziendale;
- I beacon, agent altamente evasivi e sofisticati, installati sulle macchine della vittima e che ricevono i comandi dal Command and Control.

Per tali ragioni, la comunità si è concentrata soprattutto negli ultimi 4 anni a studiare approfonditamente questo tool in quanto, anche a seguito di svariati leak di versioni craccate del software, è stato sempre più adottato ed è diventato di fatto uno standard per gli attacchi informatici. Allo stesso tempo, tanto più Cobalt Strike diventava sempre più usato dai criminali tanto maggiore è stata l'attenzione da parte di analisti e di organizzazioni operanti nel settore della difesa, portando a numerose nuove soluzioni per identificare beacon evasivi e per neutralizzare il suo operato. Nel corso degli anni sono state individuate anche alcune vulnerabilità nel codice e sono stati realizzati strumenti per decodificare i file di configurazione del beacon permettendo ai difensori di prendere il controllo del server di C2 e di bloccare la minaccia sul nascere.

Brute Ratel è uno strumento di red teaming e adversarial simulation molto simile a Cobalt Strike, sviluppato da Chetan Nayak, un esperto red teamer che ha lavorato sia in Mandiant che CrowdStrike. Essendo l'ultimo sviluppato cronologicamente, il prodotto ha cercato di unire alcuni punti di forza degli strumenti elencati precedentemente. L'idea di base è quella di ricalcare il modello di aggressione fornito da Cobalt Strike, con un sistema basato su agent snelli e altamente evasivi, rilevato da pochissimi apparati di difesa, ma con caratteristiche migliorate nella post-exploitation. Esso è emerso agli onori della cronaca quest'anno quando diversi gruppi sia cybercrime che APT hanno iniziato a usarlo al posto di Cobalt Strike come strumento principale di post esploitation. Il primo caso riportato è stato quello ad opera del gruppo paramilitare russo APT29 che ha usato Brute Ratel nel maggio del 2022 tramite delle tecniche sofisticate di sideloading. Tale tecnica ha permesso di sfruttare delle applicazioni legittime per caricare codice malevolo proveniente da una libreria precedentemente posizionata (o caricata) sulla macchina vittima. Successivamente, è stata divulgata anche una versione lecita di tale framework, ma che prontamente è stata compromessa (cracking) dai criminali informatici, in modo da poter essere usata agevolmente per i loro scopi.

Sezione 4: I trend di attacco del 2022

Attaccanti sempre più professionisti e meno amatoriali, attaccanti abili nell'implementazione di tecniche di agile development attraverso le quali continuano a migliorare e sofisticare artefatti già modulari e ben ingegnerizzati. L'inevitabile economia sommersa del cyber crime in netta ascesa a causa del mercato del ransomware porta sempre più sviluppatori di Malware e attaccanti professionisti a fare del crimine informatico un vero e proprio lavoro. Investimenti e tempo a disposizione sempre maggiore a favore degli attaccanti, sia criminali che "statali", alimentano inesorabilmente un mercato di attacchi, vittime, economie sommerse, ma anche di nuove soluzioni e nuove figure professionali.

Una continua tendenza osservata durante il 2022 continua a essere la Double Extorsion, che trova nuove evoluzioni in modo vertiginoso, comprendendo colpi di scena davvero sorprendenti. Primo tra tutti il leak del codice sorgente di Conti e il conseguente abbandono del progetto, a favore della nascita di altri "progetti" di Double Extorsion. Questo avvenimento dimostra come nessuno è immune dalle criticità indotte dalla crescita. Infatti, nessuna organizzazione trova beneficio dalla crescita esagerata (hyper-growth) la quale lascia sempre profonde cicatrici. Anche organizzazioni criminali che si trovano CAGR (indici di crescita) a doppia cifra devono affrontare problemi comuni a molte organizzazioni legittime, come a solo titolo esemplificativo: dipendenti infedeli, fuga di personale e difficoltà nella governance e nell'organizzazione interna.

Gli attacchi di tipologia DDoS (Distributed Denial of Service) sono un'altra minaccia crescente e alquanto inaspettata. La tipologia di DDoS è variegata e a sua volta composta da innumerevoli tecniche e tecnologie per specializzare o contestualizzare l'impatto. In generale essa prevede che i cyber criminali inviino un gran numero di richieste al server per sovraccaricarlo e renderlo inaccessibile. Questi attacchi possono causare perdite significative per le aziende colpite, in termini di tempo di inattività, di mancato guadagno e di danni reputazionali. Durante il 2022 questa tipologia di attacco è stata ampiamente utilizzata da attivisti digitali (hacktivisti) per supportare la Russia nella guerra ibrida contro l'Ucraina. La semplicità di effettuare tali attacchi ha permesso ad un vasto numero di "hacktivisti" di partecipare e di contribuire alla diffusione di questi semplici attacchi. Nonostante la semplicità sono state numerose le organizzazioni (sia pubbliche che private) che hanno riscontrato problemi e che hanno visto vacillare alcuni dei servizi da loro proposti.

Gli attacchi di ingegneria sociale sono un'altra tecnica utilizzata dai cyber criminali di cui si è osservata una forte ascesa durante il periodo di analisi. A seguito di una prima fase di social intelligence, ovvero raccolta delle informazioni sulla/sulle vittima/e, l'attaccante sfrutta le informazioni in possesso per indurre il target a divenire vittima. Ad esempio, possono fingere di essere un amico o un collega di fiducia per convincere l'utente a fornire informazioni personali o accedere a sistemi protetti. Prendendo spunto da questo repentino incremento, Yoroi ha deciso di condurre una ricerca scientifica in tale ambito, dove sono stati approfonditi tutti gli aspetti del phishing e come questi possono essere "ingegnerizzati" per la creazione di phishing-kits. Sono state utilizzate tecniche di Artificial Intelligence (Machine Learning) per automatizzare l'identificazione di framework di sviluppo di phishing al fine di mappare comportamenti e collaborazioni tra i principali attori operanti nel settore del "social engineering".

Ransomware e Double Extorsion nel 2022

Il Double Extortion è una tecnica di attacco in vigore da alcuni anni. Nella sua forma originale prevedeva come azione di estorsione, a seguito di un pagamento in criptovalute, la restituzione dei file che silentemente venivano cifrati, rendendoli così inutilizzabili. Con l'evoluzione delle tecniche di difesa cibernetica le organizzazioni definite "target" (ovvero possibili bersagli) hanno adottato sistemi di resilienza dei dati rendendo questo tentativo di estorsione non troppo efficace. Per questo motivo l'evoluzione degli attacchi ha spinto gli attaccanti alla

realizzazione di ulteriori forme di estorsione. La seconda forma di estorsione, avvistata pubblicamente nel 2019, consiste nel minacciare la vittima della pubblicazione dei file rapiti e solo successivamente cifrati. Una terza forma consiste nel bloccare l'erogazione dei servizi essenziali dell'organizzazione vittima mentre un'ultima forma di estorsione anche nota come "public shaming" (vergogna pubblica) consiste nella pubblica diffamazione, da parte dell'attaccante, delle scarse e inefficaci capacità di difesa cibernetica della vittima.

Nonostante l'evoluzione abbia agevolato anche le organizzazioni che, come Yoroi, operano nella difesa digitale, il tracciamento dei criminali informatici operanti nel settore della Double Extortion può essere particolarmente complesso per le seguenti ragioni:

- **Anonimato**: i criminali spesso utilizzano metodi per rimanere anonimi, come l'utilizzo di reti VPN o TOR, rendendo difficile identificare la loro posizione geografica e l'origine dell'attacco.
- **Pagamenti**: i criminali spesso chiedono il riscatto in criptovalute, che sono più difficili da tracciare rispetto alle transazioni con carte di credito o bonifici bancari.
- **Server**: i criminali spesso utilizzano server remoti, magari in paesi con leggi meno severe sulla cyber criminalità, per ospitare i loro siti web e gestire le comunicazioni con le vittime, rendendo difficile per le autorità localizzare e arrestare i responsabili.
- **Complessità**: i criminali spesso utilizzano tecniche avanzate per cifrare i dati e rendere difficile la decrittazione, rendendo difficile per le autorità recuperare i dati rubati senza pagare il riscatto.

Alla luce di quanto sopra, appare chiaro come tracciare le campagne di Double Extorsion sia una delle attività più impegnative emerse negli ultimi anni. Le motivazioni delle gang ransomware ormai sono diventate chiare, così come è diventato chiaro il loro modus operandi e il loro obiettivo. In primo luogo, i criminali informatici hanno scoperto che questa metodologia è molto redditizia, poiché aumenta le possibilità di ottenere il riscatto, diversificando le fonti di reddito. In secondo luogo, le aziende e le organizzazioni sono sempre più vulnerabili agli attacchi informatici a causa della crescente quantità di dati sensibili che archiviano e gestiscono, ed a causa di una crescita molto significativa della superficie di attacco.

Purtroppo, le pratiche normalmente utilizzate per mitigare gli effetti degli attacchi ransomware (quali ad esempio disporre di copie di backup offline) non sono sufficienti a mitigare il rischio di estorsione derivante dalla minaccia, da parte dei criminali, di rendere pubblico il contenuto dei dati sottratti alla vittima. La sfida diventa quindi la capacità di intercettare in tempo le intrusioni, minimizzando o eventualmente annullando la possibilità di estrazione di dati da parte degli attaccanti. In caso di incidente, invece, è importante saper rispondere in maniera tempestiva aiutando la vittima a ristabilire il normale funzionamento dei sistemi e ad assicurare la business continuity quanto prima.

Dal punto di vista operativo, Yoroi pone particolare impegno all'analisi delle attività di ogni gruppo ransomware conosciuto, attraverso indagini di Cyber Threat Intelligence e attività di Malware Reverse Engineering sui campioni disponibili. Questo approccio si è rivelato molto efficace sia nell'identificare attività di attacco nelle fasi iniziali dello stesso, sia nella gestione e nella risoluzione degli incidenti da parte del team di Incident Response.

Nel corso del 2022, sono state tracciate oltre 110 attività ransomware sul perimetro italiano in modalità double extorsion, alle quali è seguita anche, in alcuni casi, la pubblicazione dei leak delle vittime. È interessante osservare la distribuzione statistica delle vittime di attacco rispetto ai settori merceologici interessati, come mostrato in Figura 9.

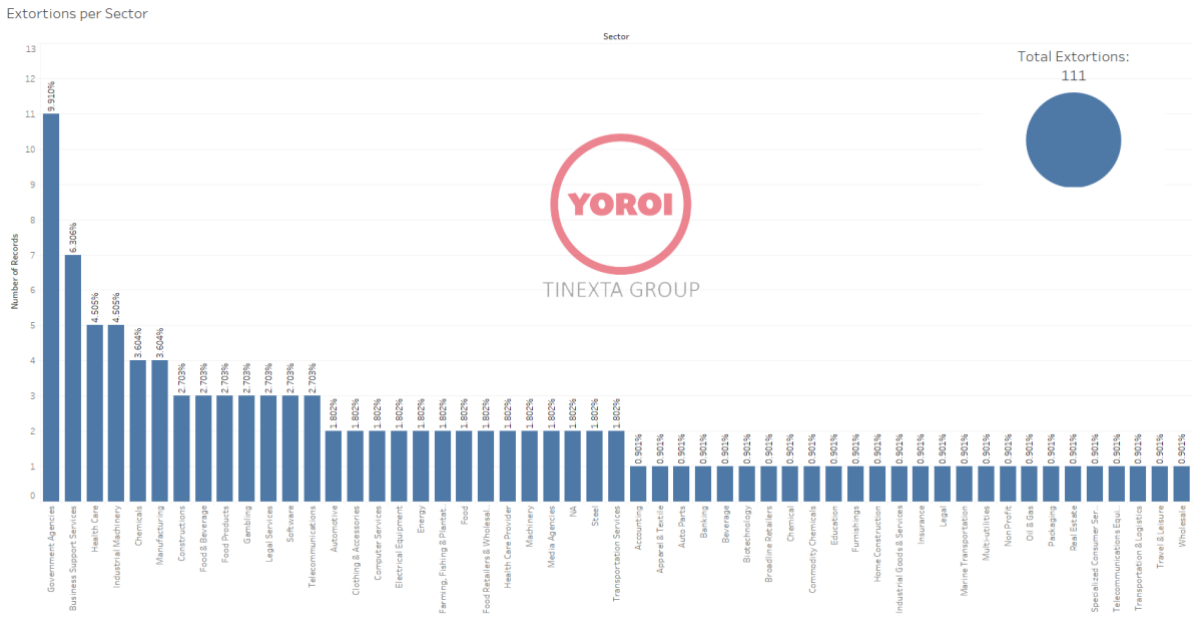

Figura 9: Distribuzione delle estorsioni per settore merceologico colpito

In base alle nostre osservazioni, quasi il 10% delle estorsioni rilevate riguardano pubbliche amministrazioni. Questo dato appare significativo e trova riscontro anche nei casi resi noti nelle cronache quali, ad esempio, il caso riguardante la Regione Lazio tra agosto e settembre 2021, che ha portato all'attenzione del grande pubblico come infrastrutture e dati di elevata importanza possano essere facilmente esposti ad attacchi gravi. In analogia a questo, anche nel corso del 2022 vi sono stati casi di comuni italiani e di pubbliche amministrazioni sottoposti ad attacchi ransomware e double extorsion. È bene ricordare, inoltre, che questo fenomeno non è confinato all'Italia ma si osserva a livello globale, se pur con ovvio effetto scala. Una considerazione plausibile in tal senso è che spesso gli attori criminali decidono di colpire questi target per l'elevato valore simbolico che rappresentano, oltre al fatto che molto sovente le infrastrutture e le applicazioni utilizzate in ambito pubblico sono datate e con problemi di manutenzione.

Oltre al settore pubblico, al secondo e al terzo posto troviamo i settori di servizi di supporto al business e il settore della sanità. L'ambito sanitario è, nuovamente, un settore estremamente critico: da una parte è facile intuire che i dati custoditi in questo ambito sono particolarmente sensibili, dall'altra il settore sconta una cronica carenza di fondi strutturali che si riflette in infrastrutture cyber spesso non adeguate.

Altra indicazione statistica di interesse nello studio del fenomeno Double Extorsion è senza dubbio quella relativa alla classifica dei gruppi ransomware più attivi del 2022. Di seguito viene presentata la distribuzione degli attacchi ransomware in funzione della gang criminale.

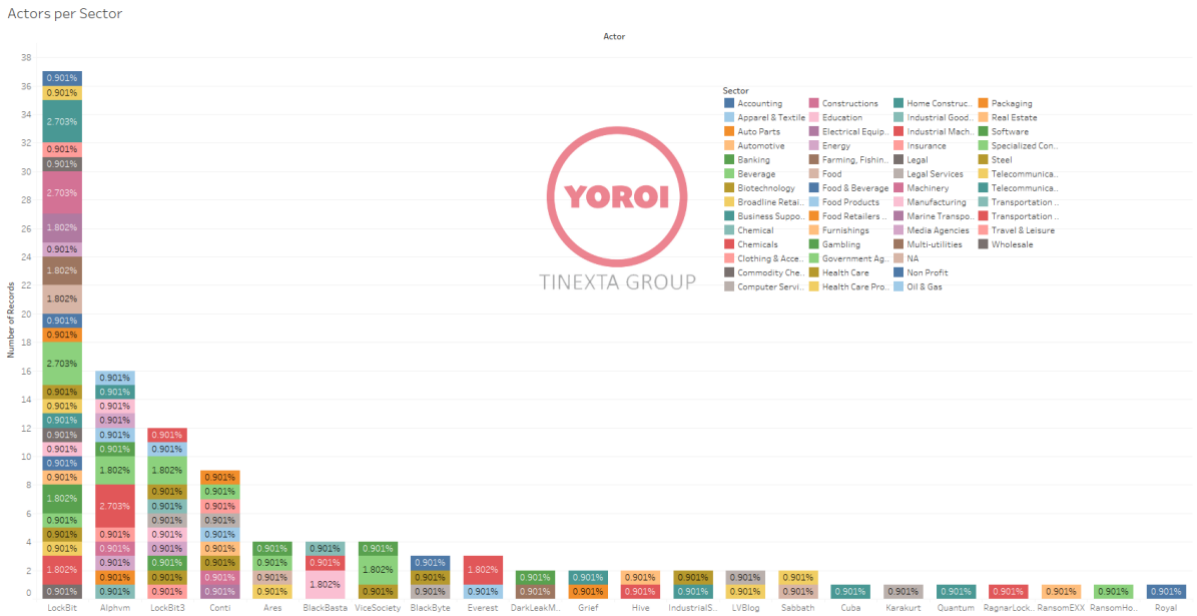

Figura 10: Distribuzione degli attacchi Double Extorsion in funzione del gruppo ransomware

Osservando i dati riportati in Figura 10 è immediato notare la prevalenza dell'attore Lockbit in attacchi di tipo Double Extorsion. Lockbit è la gang che ha colpito indiscriminatamente ogni settore industriale, senza alcuna particolare preferenza per un settore specifico. È interessante notare inoltre come Lockbit abbia investito nella propria immagine e nella propria reputazione probabilmente più di tutti gli altri gruppi, creando vere e proprie campagne di marketing per attirare quanti più criminali possibile all'interno delle proprie fila. Anche a livello organizzativo interno è interessante notare come il gruppo Lockbit sia strutturato secondo logiche aziendali: vi sono leader che pianificano e coordinano le attività e figure specializzate, come sviluppatori di malware, hacker, esperti di marketing ed esperti di finanza. Si sono registrati anche casi di affiliati che forniscono supporto, anche logistico interno, alle attività della gang rispetto a un target in cambio di una percentuale del riscatto.

Al secondo posto della classifica troviamo Alphvm, conosciuto anche come BlackCat. Questo gruppo, nato probabilmente dai gruppi REvil e BlackMatter, in poco più di un anno di attività è diventato uno dei più pericolosi e aggressivi sulla scena mondiale. Oltre alle attività ben note, questo gruppo ha messo a disposizione una pagina con indicizzazione dei contenuti trafugati alle vittime, ovvero consente a chiunque di ricercare parole chiave, informazioni e file provenienti da quanto sottratto alle proprie vittime. Questa capacità mette ancora più pressione alle vittime che sanno che quanto loro sottratto potrà essere facilmente trovato da chiunque; l'intento criminale è chiaro ed evidente e mira a massimizzare la probabilità che una vittima sia disponibile a pagare il riscatto per assicurarsi di non comparire in questa sorta di motore di ricerca. Trattandosi poi di una novità che sembra dare i frutti sperati, anche altri gruppi, primo tra tutti Lockbit, hanno deciso di adottare questo approccio così da beneficiare degli stessi effetti di pressione sui loro target.

È interessante ricordare anche le attività del gruppo Hive, specializzato nel colpire settori critici e infrastrutture sanitarie. A riprova di quanto sopra, basti ricordare l'attacco portato a marzo 2022 a Ferrovie dello Stato che ha causato in Italia una serie di disservizi sui canali digitali di acquisto dei biglietti e di altri servizi; una vicenda che ha avuto una forte eco mediatica. La stessa specializzazione si è osservata a livello globale, a iniziare da un'azienda ospedaliera della California, prima vittima di doppia estorsione, i cui file vennero pubblicati sulla loro pagina. L'osservazione dello sviluppo di questo attore da parte del nostro team di intelligence ha evidenziato una

progressiva evoluzione sotto il profilo TTP (Tactics, Techniques, and Procedures). I risultati di queste osservazioni sono riportati nell'articolo presente sul nostro blog con il nome di "On the Footsteps of Hive Ransomware".

Un altro attore malevolo che vale la pena di tenere sotto controllo è Royal Ransomware, gruppo nato nel corso del 2022, che ha dimostrato una notevole aggressività in pochissimo tempo. Seppure dal punto di vista TTP e di infrastruttura utilizzi soluzioni meno sofisticate rispetto a gruppi più famosi, si è dimostrato efficace e temibile e ha meritato particolare attenzione da parte del nostro team di intelligence. In particolare, nel nostro report "Reconstructing the last activities of Royal Ransomware" pubblicato sul nostro blog, mostriamo proprio come in pochissimo tempo questo attore criminale sia stato in grado di crescere notevolmente in volume di vittime e anche per quanto riguarda la sofisticazione degli attacchi informatici in questione. Nel 2023 ci aspettiamo che questo attore criminale possa subire un'ulteriore evoluzione, diventando così uno dei più pericolosi attori dei prossimi tempi.

Infine, un altro evento che ha influenzato notevolmente il mondo delle Double Extorsion, causando anche dei riposizionamenti nei rapporti di potere e nelle gerarchie tra i gruppi stessi, è stata la pubblicazione del codice sorgente di Conti Ransomware. Nel dettaglio, tra la fine di febbraio 2022 e gli inizi di marzo, un utente di Twitter con l'alias "conti_leaks" ha iniziato a condividere informazioni fondamentali sull'organizzazione del gruppo, pubblicando non solo l'identità di alcuni membri appartenenti alla gang, ma anche il codice sorgente di una delle ultime versioni del ransomware, che poi il team di ricercatori di Yoroi ha analizzato. Le conseguenze di questo evento sono state molteplici: da un lato si è palesata una fine "ufficiale" dell'attività legata a Conti, dall'altra si è assistito alla nascita del gruppo Monti che utilizza le stesse TTP di Conti e che ha sfruttato il leak per dotarsi della tecnologia necessaria per supportare le proprie operazioni.

Sezione 5: Una ricerca targata Yoroi, Phishing Kits

Alla luce di quanto presentato nelle sezioni precedenti, la minaccia degli attacchi di tipo phishing assume una rilevanza importante nel panorama degli attacchi cyber. Il phishing è una forma di attacco informatico che mira a ingannare gli utenti per ottenere da loro informazioni sensibili, o per indurli a eseguire particolari azioni, attraverso l'uso di tecniche di social engineering. Gli attaccanti utilizzano varie forme di comunicazione, come e-mail, messaggi di testo, social media o chiamate telefoniche, per far sembrare che la loro richiesta sia legittima e provenga da una fonte attendibile, come un'istituzione finanziaria o un'azienda.

Il phishing può essere di diversi tipi:

- Phishing di tipo "Spear": mira a gruppi specifici di persone, come dipendenti di un'azienda, utilizzando informazioni raccolte da fonti aperte sui social media;
- Phishing di tipo "Clone": utilizza siti web falsi che imitano quelli legittimi, solitamente chiedendo all'utente di inserire informazioni personali o di effettuare transazioni bancarie;
- Phishing di tipo "Whaling": mira a individui specifici, come dirigenti aziendali o rappresentanti delle istituzioni finanziarie, utilizzando messaggi mirati e personalizzati.

Spesso l'obiettivo dell'attività di phishing è ottenere da parte dell'utente l'apertura di un file contenente un payload malevolo, o l'apertura di un link o di una pagina costruita ad arte per eseguire codice sulla macchina della vittima.

Il phishing è un fenomeno in crescita perché rappresenta un modo semplice ed economico per gli attaccanti di ottenere informazioni personali sensibili da un gran numero di potenziali vittime e/o di diffondere malware. Con l'aumento del numero di utenti della rete internet e la disponibilità sempre maggiore di informazioni personali online, gli attaccanti hanno una vasta gamma di obiettivi a cui indirizzare i loro attacchi. La tecnologia sta diventando sempre più avanzata, il che significa che gli attacchi di phishing sono sempre più realistici e convincenti. Inoltre, gli utenti diventano sempre più dipendenti dalla tecnologia e dalle transazioni online, il che li rende più vulnerabili e sempre più esposti agli attacchi di phishing. La globalizzazione e l'utilizzo di più dispositivi e piattaforme rendono anche più difficile per gli utenti riconoscere quali comunicazioni sono attendibili e quali no. Infine, l'impatto della pandemia ha ulteriormente aumentato il numero di attacchi di phishing, poiché gli attaccanti hanno visto un'opportunità per sfruttare la paura e l'incertezza causate dalla situazione.

Inoltre, va considerato che tali attacchi:

- Sono economici: gli attacchi di phishing possono essere eseguiti con mezzi relativamente semplici e a basso costo, come l'invio di e-mail o la creazione di siti web falsi.
- Sono facili da automatizzare: gli attacchi di phishing possono essere automatizzati per inviare grandi quantità di e-mail o messaggi di testo in poco tempo.
- Sono difficili da rilevare: gli attacchi di phishing possono essere progettati per essere molto simili alle comunicazioni legittime, rendendo difficile per le vittime riconoscere l'attacco, e spesso adottano dei meccanismi tecnologici altamente sofisticati per eludere i sistemi di protezione aziendale.
- Sono efficaci: gli attacchi di phishing possono essere molto efficaci nel convincere le persone a fornire informazioni riservate o a scaricare software dannoso.

Per queste ragioni, Yoroi ha deciso di fronteggiare tale minaccia procedendo in due modalità: la prima è quella di tracciare tutte le campagne phishing viste in Italia dalla nostra telemetria; la seconda invece è adottare il metodo scientifico per poter identificare i kit di phishing.

I dati della telemetria Yoroi hanno permesso di ottenere la seguente statistica:

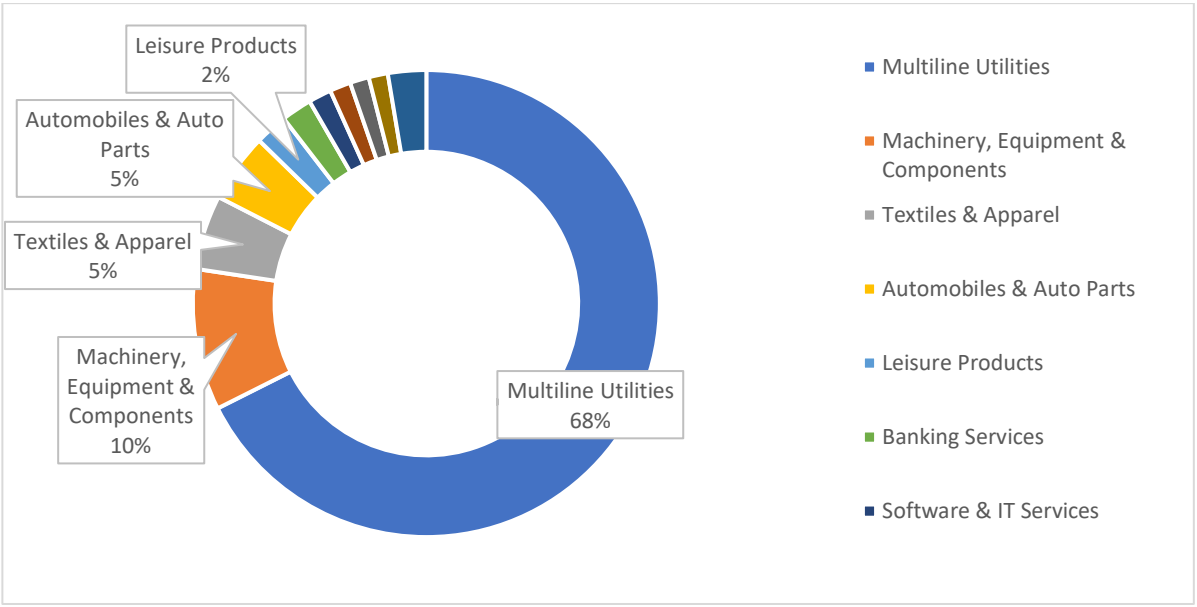

Figura 11: Distribuzione dei Phishing in Italia per settore industriale

In Italia si può notare come le aziende di servizio siano quelle più colpite dal fenomeno del phishing, con oltre i due terzi di tutte le minacce intercettate. La motivazione può essere ricercata dal fatto che questo settore merceologico utilizza in maniera massiva le strumentazioni informatiche; per questa ragione è molto probabile che vi siano in queste aziende informazioni di valore e attrattive per i criminali informatici, prima tra tutte le credenziali di accesso. Inoltre, è plausibile immaginare che un'azienda che fonda la propria operatività su tecnologie informatiche sia molto preoccupata in caso di attacchi che ne interessino le stesse, e quindi potenzialmente più propensa a compromessi offerti dai criminali informatici.

Al secondo posto troviamo il settore meccanico, che rappresenta uno dei settori di maggiore rilevanza per il tessuto industriale italiano ed è composto in misura preponderante da piccole e medie imprese, che operano sovente come terze parti di catene produttive complesse. In questo caso l'interesse delle organizzazioni criminali informatiche è duplice: da un lato si tratta di obiettivi semplici, spesso dotati di poca o nulla struttura di sicurezza, dall'altro, proprio il fatto di essere parti di catene produttive complesse assicura agli attori malevoli la capacità di escalation all'interno di sistemi più grandi e complessi.

Proprio all'interno di questo contesto operativo si colloca la ricerca portata avanti da Yoroi in collaborazione con le Università di Bologna e di Modena e Reggio Emilia. Il lavoro di ricerca si concentra sui kit di phishing. I kit di phishing sono strumenti pronti all'uso che consentono una rapida implementazione di campagne malevole: vengono distribuiti nel dark web e rappresentano una seria minaccia per la sicurezza informatica, in quanto garantiscono la possibilità di effettuare attacchi di phishing sofisticati anche ad attori non esperti.

Mentre in letteratura sono presenti molti lavori che si concentrano su funzioni specifiche dei kit o sono focalizzati principalmente sugli obiettivi di rilevamento, nel lavoro di ricerca svolto il focus si concentra su una metodologia di classificazione basata su oltre 2000 kit di phishing recenti.

La metodologia proposta si basa su due approcci complementari. La classificazione deterministica esegue un'analisi statica del codice sorgente dei kit di phishing ed estrae informazioni sulle tecniche di evasione e

offuscamento adottate. Raggruppando i kit in base alle firme presentate, è possibile dimostrare che gli autori dei kit tendono a mantenere le stesse abitudini di codifica nel tempo.

Nonostante il basso numero di falsi positivi, questa prima fase deterministica non è in grado però di rilevare le nuove funzioni che i threat actor possono introdurre. Per questo motivo, proponiamo anche l'adozione di classificatori basati su machine learning (ML), addestrati a rilevare kit dotati di tecniche di evasione e offuscamento. L'ipotesi è che il piccolo gruppo di attori più prolifici tenda a non cambiare le proprie abitudini di programmazione e a riutilizzare parti di kit precedenti in nuovi prodotti. I risultati sperimentali hanno confermato questa ipotesi, attraverso molteplici scenari che dimostrano che i metodi di apprendimento automatico proposti portano a classificatori robusti che apprendono gli schemi tipici della maggior parte dei kit evasivi e offuscati, non richiedono un gran numero di esempi nel training set e sono anche in grado di classificare correttamente i kit che impiegano tecniche nuove, non viste durante l'addestramento.

Questo lavoro di ricerca deve essere considerato come un contributo iniziale all'analisi dei kit di phishing, che rappresentano un problema consistente della moderna criminalità informatica. Il lavoro futuro potrà sfruttare i risultati ottenuti in una duplice direzione: il miglioramento degli strumenti di rilevamento attraverso l'analisi delle tecniche di evasione e offuscamento considerate; la progettazione e la valutazione di operazioni di threat intelligence più avanzate basate sui profili degli autori e sui loro schemi adottati.

Riteniamo estremamente significativo e degno di nota, infine, osservare il lavoro di ricerca proposto come un esempio di collaborazione virtuosa tra il mondo accademico e la realtà industriale del Paese: riteniamo infatti che solo attraverso questo tipo di collaborazione sia possibile non soltanto migliorare la qualità della ricerca, corroborandone i risultati con ricadute pratiche, ma anche incrementare significativamente la competitività delle nostre Aziende, al passo con i più ambiziosi competitor internazionali.

Cosa ci aspetta nel 2023

Anche il 2023 rappresenta un'importante sfida per il settore dell'informazione e della trasformazione digitale. I trend osservati suggeriscono le seguenti predizioni:

1. L'incremento di reti internazionali di cooperazione al contrasto della criminalità informatica. Organizzazioni come le Interpol espanderanno le proprie competenze operative internazionali giocando un ruolo fondamentale nel settore della repressione criminale.
2. Osserveremo per il quinto anno consecutivo un importante problema nel reclutamento di risorse opportunamente addestrate, sottolineando ancora una volta l'importante divario tra risorse umane operanti nel settore della cybersicurezza e quelle di cui la società avrebbe necessità.
3. Centri di ricerca, Università e centri di formazione estenderanno la loro offerta formativa nel settore della cybersecurity.
4. Organizzazioni no-profit inizieranno un vasto ma significativo interesse alla difesa digitale.
5. La presenza di un'organizzazione pubblica specifica per la difesa delle infrastrutture critiche Italiane forzerà le organizzazioni appartenenti al perimetro strategico cibernetico ad un continuo miglioramento.
6. La NIS2 offrirà un perimetro più ampio e offrirà alle aziende una più ampia opportunità di crescita nel digitale.

7. Le minacce Double Extortion continueranno ad essere uno dei principali problemi nel perimetro cyber del 2023.
8. I settori industriali continueranno a essere i principali bersagli da parte di attori malevoli che intravedono semplici guadagni e la bassa probabilità di arrecare danni reali, oltre che possibilità di "escalation" all'interno di complesse catene di fornitura.
9. Gli attacchi di tipo supply chain aumenteranno di frequenza e di intensità, con particolare focus su attacchi portati sempre più spesso a componenti software che compongono sistemi complessi.
10. Si osserveranno gruppi criminali operare con un "codice di condotta pubblico" al fine di evitare di attaccare enti di prima assistenza (pronto soccorso, ospedali, organizzazioni non di interesse).
11. L'intelligenza artificiale verrà ampiamente utilizzata da attaccanti e da difensori per aumentare lo loro capacità di offesa e difesa e al fine di "migliorare il fattore di scala".
12. L'integrazione di strumenti di sviluppo con strumenti di AI, permetteranno ad attaccanti di offuscare il codice in modo mai visto prima e di realizzare strumenti (e template di comunicazione) con una sofisticazione realmente allarmanti.
13. Il PNRR Europeo offrirà ai governi la possibilità di realizzare strumenti e infrastrutture sempre più sofisticate e resilienti, con capacità di adattabilità al cambiamento significativo.

"*Il modo migliore per predire il futuro è crearlo!*" (Abramo Lincoln)

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

Yoroi S.r.l. società soggetta ad attività di direzione e coordinamento esercitata dalla Tinexta S.p.A.

Yoroi ® è un marchio registrato

Registrazione N°: 016792947

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

TF-CSIRT
Trusted Introducer