CYBERSECURITY ANNUAL REPORT 2021

Indice dei contenuti

Introduzione

Yoroi difende le aziende e le organizzazioni nello spazio digitale fin dall'inizio della sua esistenza, migliorando la sua tecnologia giorno dopo giorno e le sue capacità di analisi. Seguire le minacce, gli attori delle stesse e il modo in cui cambiano nel tempo ha un ruolo centrale nel ciclo di apprendimento continuo che abbiamo creato in azienda e aiuta i nostri analisti di cyber sicurezza ad avere una migliore efficacia sul contrasto alle minacce.

Crediamo nella condivisione delle informazioni come una delle principali armi difensive dell'umanità. Ogni anno investiamo tempo per estrarre, raccogliere e descrivere ciò che abbiamo imparato negli ultimi dodici mesi. Quest'anno abbiamo deciso di migliorare il nostro Yoroi Cybersecurity Report bilanciando analisi qualitative e quantitative in un unico breve documento accessibile a chiunque ne abbia bisogno. A questo scopo siamo lieti di presentare lo Yoroi Cybersecurity Report 2021.

Un nuovo decennio si è avvicinato alla nostra storia e qualcosa di nuovo si nasconde in nuovi cyber attacchi mentre le azioni di minaccia consolidate persistono nel colpire le organizzazioni di tutto il mondo. L'attuale rapporto è costruito per evidenziare ciò che è nuovo rispetto a ciò che è consolidato negli ultimi mesi, abbiamo deciso di concentrare il rapporto 2021 sulle seguenti sezioni

Sezione 1: Malware. Gli autori descrivono la sofisticazione della catena del malware in continuo aumento, con particolare attenzione al malware mirato. La sezione caratterizzata da Yoroi sul malware Zero-Day è migliorata adottando una visione ampia su ciò che è coperto e ciò che non è coperto dai comuni sistemi antivirus. Un capitolo dedicato alle industrie colpite è fornito per mappare il malware alle industrie colpite. Questa sezione potrebbe aiutare i CISO ad essere pronti a fronteggiare gli attacchi più comuni relativi alla sua verticale di business.
Il capitolo sulla propagazione e il movimento laterale descrive come questi artefatti si spostano da un'azienda all'altra. Questa sezione termina descrivendo le minacce in Italia, uno dei paesi più attivi.

Sezione 2: Minacce bloccate. Questa sezione esegue un'immersione profonda nelle minacce informatiche bloccate fornendo dettagli sui domini di primo livello coinvolti e descrivendo gli attacchi botnet/opportunistici influenzati nell'attività informatica quotidiana. Dal momento che le e-mail sono uno dei vettori di attacco preferiti come riportato nel rapporto Yoroi Cybersecurity 2021 e nel rapporto Yoroi Cybersecurity 2019, quest'anno abbiamo deciso di fornire una sezione dedicata, confrontando le tendenze degli ultimi anni.

Sezione 3: La minaccia delle e-mail. Questa sezione è completamente dedicata ai vettori E-Mail. L'analisi dei vettori di malware e gli argomenti comuni sono descritti per evidenziare i modelli comuni sfruttati da una discussione a grappolo. Lo studio dei vettori E-Mail potrebbe permettere ai professionisti della sicurezza di migliorare le loro capacità difensive.

Sezione 4: Tendenze delle tecniche di attacco. Questa sezione è introdotta per visualizzare le nuove tendenze di attacco secondo la matrice MITRE ATT&CK. Comprendere le tendenze di attacco è un passo iniziale per fornire soluzioni di blocco e meccanismi di rilevamento. Il rapporto 2021 si sofferma sulle tematiche Nuove Minacce dalle Supply-Chain e Backdoor di Sanburst.

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 l'esperienza più significativa 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, nell'ottobre del 2020, l'acquisizione della maggioranza del capitale di YOROI da parte di TINEXTA S.p.A.
In questa occasione Yoroi è stata scelta per integrare tutte le componenti esistenti del gruppo Cybaze: YOROI è ora una compagine formata da oltre 140 persone e importanti infrastrutture tra le quali ricordiamo:

- 4 Defense Center (Trieste, Milano, Cesena e Benevento);
- 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).

In YOROI sono presenti:

- Più di 40 cyber analisti qualificati,
- Più di 50 sviluppatori,
- 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.

Tutto questo, unitamente alle acquisizioni della divisione progetti, soluzioni e R&D di Corvallis e di Swascan, permetterà a TINEXTA di creare un hub nazionale specializzato nei servizi di identità digitale e sicurezza digitale. Per maggiori dettagli si veda il comunicato stampa: https://www.tinexta.com/file/1760.

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

Questa frase sintetizza quello che in YOROI esperienza e competenze 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. Occorre uscire da una logica di protezione, con la conseguente moltiplicazione di strumenti e servizi, per andare verso una logica di difesa dinamica, che integri quei prodotti e servizi in un sistema integrato e reattivo, dove la componente umana è inscindibile dalla componente tecnologica.

Un sistema di cyber security è composto da servizi e prodotti che appartengono alle seguenti famiglie principali:

1. Servizi di Difesa Cibernetica: Cyber Security Defense Center (CSDC),
2. Servizi di Analisi della Sicurezza Aziendale,
3. Servizi di Certificazione,
4. Servizi di Formazione,
5. Software proprietari.

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 proprietari 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 stati 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

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

La pratica della doppia estorsione (Double Extortion)

Arrivano gli attacchi di Double Extortion che in poche ore catapultano letteralmente un'azienda in una crisi Cyber

Molti degli attacchi malware di alto profilo emersi nel 2020 sono stati quelli che la comunità della cyber security chiama attacchi **Double Extortion**. Se da un lato l'accelerazione della digitalizzazione è stata fondamentale per la maggior parte delle aziende per garantire la sopravvivenza dell'operatività aziendale durante il lockdown causato dalla pandemia, dall'altro ha consentito l'ampia diffusione di questo tipo di attacchi basati su malware avanzati. Infatti, a causa dell'indebolimento del perimetro di rete e del numero massiccio e improvviso di cambiamenti nell'infrastruttura IT, i reparti IT hanno faticato a tenere il passo con i controlli di sicurezza.
Sentiamo spesso parlare di questi attacchi come attacchi ransomware. Tuttavia, parlare di ransomware è estremamente riduttivo. Il modus operandi di questi attacchi è diverso. Il termine ransomware, infatti, è circolato ancor prima della nascita del fenomeno della Double Extortion: in origine gli attacchi ransomware colpivano per lo più i privati, crittografando i dati all'interno del loro pc. Invece, la dinamica degli attacchi Double Extortion coinvolge intere imprese e persino il tessuto produttivo nazionale.

In effetti, il trend degli attacchi Double Extortion è fortemente cresciuto durante il 2020 e va accuratamente considerata la sua caratteristica di essere fatto su misura. Questi attacchi malware sono gestiti da team organizzati, specialisti della sicurezza che operano come i **Red Team** che le aziende usano per testare le loro difese: specialisti di alto livello degli attacchi cyber, ma senza alcuna etica professionale.

Nel 2019 abbiamo osservato l'aumento di questo trend cyber-criminale, facendo riferimento a questi gruppi come **Dark Team**. Ma all'epoca erano concentrati su un unico obiettivo: installare malware di tipo ransomware in tutta l'azienda. Invece, nel corso del 2020 molti di questi operatori sono passati alla pratica della Double Extortion iniziando a rubare dati preziosi dalla rete della vittima e chiedendo denaro per "garantire" la cancellazione del loro bottino criminale.

Inoltre, le dinamiche degli attacchi di Double Extortion ricordano il modus operandi degli "advanced threat actors", le cosiddette Advanced Persistent Threat (APT). Questo è molto più di un banale dettaglio. Tali intrusioni informatiche avanzate vengono avviate molte volte attraverso host infetti da malware per entrare nella rete aziendale. Quindi, i cyber-specialisti criminali sfruttano il loro set di strumenti e impianti per spostarsi attraverso la rete aziendale, per rubare dati sensibili e infine per assumere completamente il controllo dell'infrastruttura IT, tagliando fuori gli amministratori di sistema e distribuendo massicciamente ransomware su qualsiasi asset aziendale.

Affrontare tali minacce era, fino a pochi anni fa, solo una preoccupazione delle organizzazioni che operavano in settori strategici o in settori verticali fortemente presi di mira come il settore bancario, finanziario, la difesa o le infrastrutture critiche. **Dopo l'accelerazione della pandemia covid19 nel 2020, le stesse metodologie operative dannose stanno ora minacciando settori molto meno cyber-maturi e ancora meno cyber-resilienti**, sbattendo il problema della sicurezza informatica proprio in faccia a molti board aziendali.

Questo punto di svolta è impossibile da ignorare. La convinzione che hanno molte aziende operanti in settori meno cyber-maturi – come ad esempio "le vecchie strategie sono ancora sufficienti" – va in frantumi di fronte alla violenza degli attacchi Double Extortion, che in poche ore catapultano letteralmente l'azienda in una crisi Cyber.

Una situazione caotica che pone di fronte ai vertici aziendali una serie di problematiche di elevata gravità che hanno un impatto immediato sull'operatività del business, sulle responsabilità civili e penali, sulla reputazione del marchio e sulla competitività a lungo termine.

Allora, come è possibile adattare la strategia di sicurezza informatica aziendale per affrontare queste minacce?

Ci sono molti modi per farlo. In ambienti aziendali complessi l'adozione delle migliori pratiche potrebbe tradursi però solo in costosi esercizi estetici; è molto meglio concentrarsi su buone pratiche e principi. Un principio che un CISO potrebbe utilizzare come bussola è l'equilibrio. Ad esempio, bilanciare le risorse e l'investimento tra prevenzione, rilevamento e risposta. Rispondendo a domande del tipo: "Quanto ha investito l'azienda in controlli di sicurezza preventivi?" - oppure - "L'azienda sta investendo in rilevamento e risposta?" o anche "quando è stata l'ultima volta che l'azienda ha rivisto in profondità la sua strategia di sicurezza?" può aiutare molto nel processo decisionale.

Con questo in mente, le strategie di cybersecurity possono essere sviluppate potenziando a livello aziendale la prontezza di risposta alle **Cyber Crisis** e i piani di emergenza. Investire in security operations, in tecnologie di rilevamento e risposta come il **Cyber Security Defense Center di Yoroi** e gli **agenti Kanwa**, sfruttando operazioni e servizi di **Cyber Threat Intelligence** maturi offre nuove opportunità di riduzione del rischio per l'azienda.

I malware zero-day

Il 75,6% di file malevoli utilizzati per attaccare l'organizzazione sono malware zero-day e malware appena conosciuti che hanno una possibilità non trascurabile di aggirare i tradizionali perimetri di sicurezza

Il volume di codice malevole prodotto e diffuso è in costante aumento. I vantaggi tecnici e le tecniche di ingegneria del software non solo consentono alle aziende di trasformare e digitalizzare le proprie attività, ma aiutano anche i criminali informatici nello sviluppo sistematico delle infrastrutture di attacco.

Con oltre un miliardo di sample prodotti nel 2020 [https://www.av-test.org/en/statistics/malware/], il malware può essere visto - senza dubbio - come un vero e proprio settore, caratterizzato da processi di produzione, ingegneria, supply chain e consegna. Anno dopo anno, questo aspetto è in costante crescita e non importa quanti attori e operatori di malware vengano arrestati dalle forze dell'ordine, essi vengono facilmente sostituiti con nuove bande emergenti. Questo è un effetto collaterale del processo di digitalizzazione in corso che sta coinvolgendo la nostra economia e la sua crescita potrebbe potenzialmente durare per molti altri decenni.
In questo ambiente, una tal enorme produzione di malware rappresenta una minaccia per le aziende e le imprese che operano nell'economia digitalizzata. Soprattutto perché molti dei malware là fuori sono nuovi.

Il nuovo malware, o malware zero-day, è incredibilmente pericoloso per le aziende che si affidano ai sistemi di sicurezza tradizionali, perché infrange uno dei presupposti fondamentali dietro l'approccio antivirus tradizionale, che si basa sul blocco delle parti note di codice malevolo. Pertanto, noi teniamo traccia dei malware Zero-Day nella nostra telemetria.

Infatti, la tecnologia di Yoroi cattura e raccoglie campioni diffusi durante gli attacchi informatici e li analizza automaticamente proprio quando si avvicinano al perimetro della rete aziendale. Durante questo processo, come parte della pipeline di analisi automatica, Yomi Sandbox controlla e segnala se i file dannosi vengono potenzialmente rilevati dalle tecnologie Anti-Virus nel momento specifico in cui il malware viene diffuso nell'organizzazione presa di mira.
Questo ci fornisce una preziosa visione di come il malware Zero-Day si evolve nel tempo e di quanto sia critico per le aziende, perché le minacce note sono molto più facili da intercettare, quelle sconosciute decisamente no.
Chiamiamo malware zero-day ogni sample che risulta essere una variante sconosciuta di famiglie di malware arbitrarie.
L'immagine seguente mostra che il 58% dei file malware analizzati **nel 2020 erano sconosciuti alle comuni soluzioni antivirus nel momento in cui hanno attraversato il perimetro aziendale.**

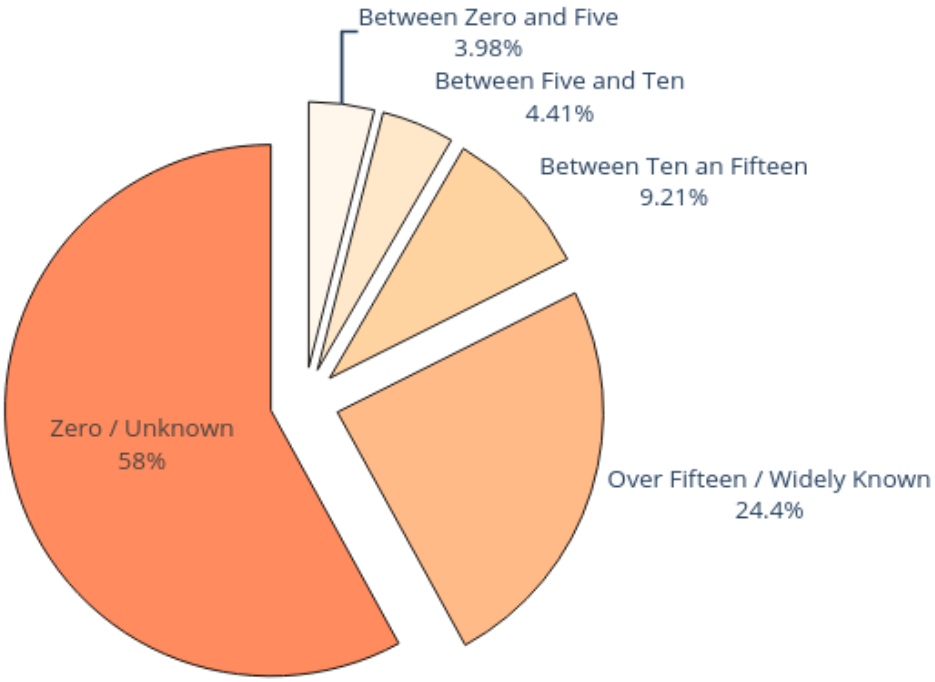


Figura 1. Malware Zero Day distribuito alle organizzazioni

I dati riportati vengono raccolti durante i primi tentativi di propagazione di file malevoli tra le organizzazioni. Ciò significa che le aziende sono fortemente esposte a un rischio rilevante di malware zero-day .
Il rilevamento rapido di questo tipo di malware gioca un ruolo fondamentale nelle strategie di sicurezza informatica consolidate perché ridurrà sensibilmente il rischio di gravi problemi di sicurezza, violazione dei dati o situazioni di crisi cyber. Insieme all'osservazione del malware Zero-Day, anche buona parte dei sample di malware noti non sono così ben rilevati dalle soluzioni antivirus: il 41,8% dei sample conosciuti è stato appena riconosciuto. Infatti, oltre un terzo del malware noto era rilevabile da meno di 15 motori antivirus al momento dell'attacco.

Se riassumiamo queste due categorie, il malware zero-day e quelli appena conosciuti, concludiamo che il **75,6% di file dannosi utilizzati per attaccare l'organizzazione ha una possibilità non trascurabile di aggirare il tradizionale perimetro di sicurezza.**

Un'interpretazione ragionevole di questi dati è conforme alla sofisticatezza dell'industria del malware. Infatti, sezionando la categoria del malware Zero-Day, molti dei malware intercettati appartengono a due classi distinte: il 66% dei campioni sconosciuti mostra comportamenti tipici dei trojan, garantendo agli aggressori un ulteriore accesso persistente alle stazioni di lavoro compromesse e il 28% scaricano ed eseguono altri artefatti dannosi, comportandosi come parte di una catena di infezioni a più fasi più complessa.

Riassumendo i risultati, le organizzazioni aziendali oggi si trovano ad affrontare scenari di rischio estremamente pericolosi a causa dell'attuale panorama delle minacce malware, caratterizzato da tre fatti principali:

1. I volumi estremamente elevati di campioni di malware prodotti e diffusi dagli operatori della criminalità informatica.
2. Oltre due terzi dei file malevoli in arrivo sono sconosciuti, o almeno conosciuti a malapena, al momento dell'attacco.
3. La maggior parte dei file malevoli è progettata per eliminare e installare ulteriori impianti o fornire accesso diretto alle macchine compromesse.

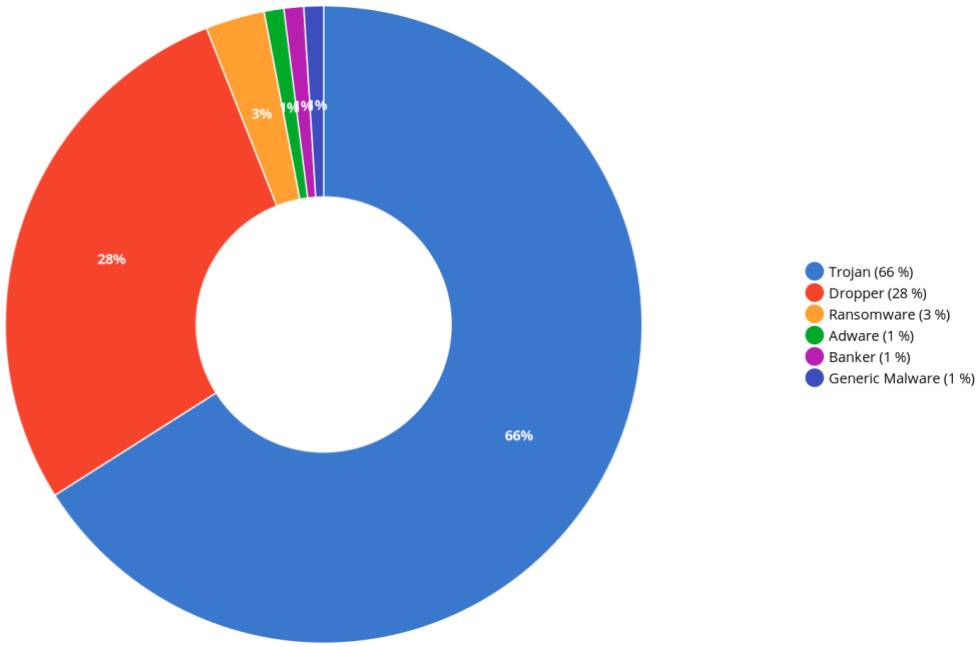


Figura 2. Il malware zero-day intercettato dalle tecnologie CSDC senza corrispondenze AV al momento del rilevamento

I settori interessati

La distribuzione degli attacchi cyber tra i settori non è uniforme.

Capire come i malware colpiscono i settori è una preziosa fonte di conoscenza che aiuta nella valutazione della reale esposizione alla sicurezza per ogni settore e nell'identificazione dei business più preziosi per gli aggressori. In effetti, ci sono business più vulnerabili agli attacchi informatici o a specifici vettori di attacco.

Inoltre, tale analisi, può fungere da driver per l'implementazione di una strategia di Difesa su misura che tenga conto dei vettori di attacco e delle distribuzioni temporali degli attacchi mirati. Per le industrie più vulnerabili agli attacchi informatici, devono essere messi in atto i giusti controlli di sicurezza insieme a un buon programma di gestione delle vulnerabilità e formazione dei dipendenti al fine di ridurre il divario di sicurezza.

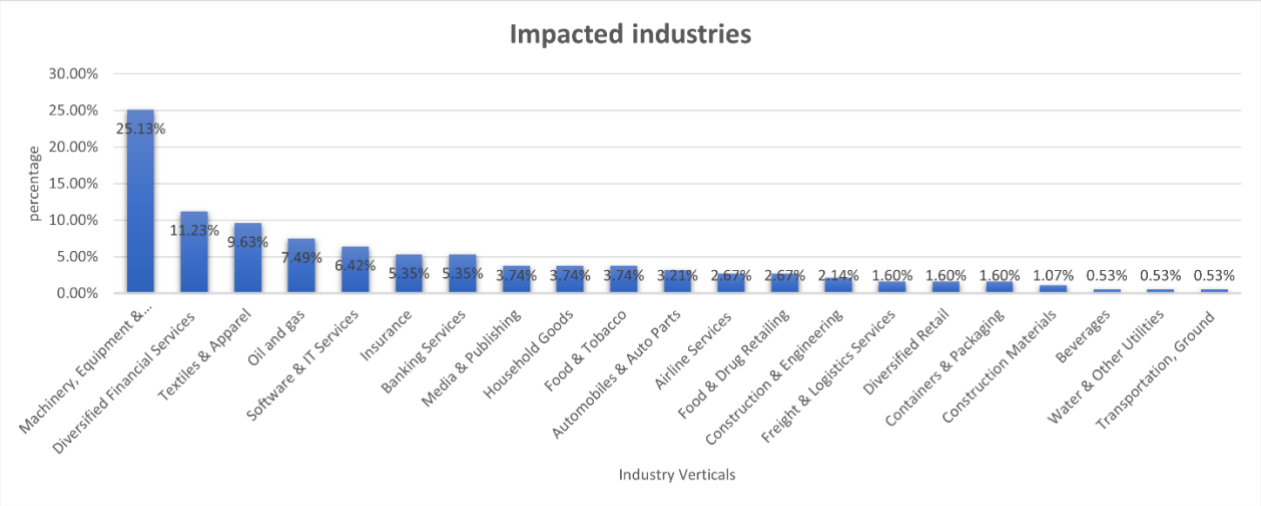


Figura 3. I settori interessati

Come dimostrato dalla distribuzione degli attacchi informatici tra i settori, i settori più colpiti per il 2020 sono *Machinery, Equipment & Components* con una quota del 25,13%, seguiti da *Diversified Financial Services* con l'11,23%, *Textiles & Apparel* con il 9,63%, *Oil and Gas* con il 7,49% seguito da tutti gli altri. Gli ultimi sono *Beverages, Water & Other Utilities* e *Transportation* con lo 0,53%.

Confrontando la distribuzione con l'anno scorso (2019) è possibile notare che i settori più presi di mira rimangono gli stessi (*Machinery, Equipment & Components* e *Diversified Financial Services*). Come mostrato nella figura (Fig. X), la posta elettronica rimane il vettore di attacco principale utilizzato dai criminali informatici. Ciò sottolinea il carattere opportunistico delle minacce. Dal 2019 al 2020 gli attacchi via e-mail sono aumentati dall'89% al 92% e la tendenza è solo in peggioramento.

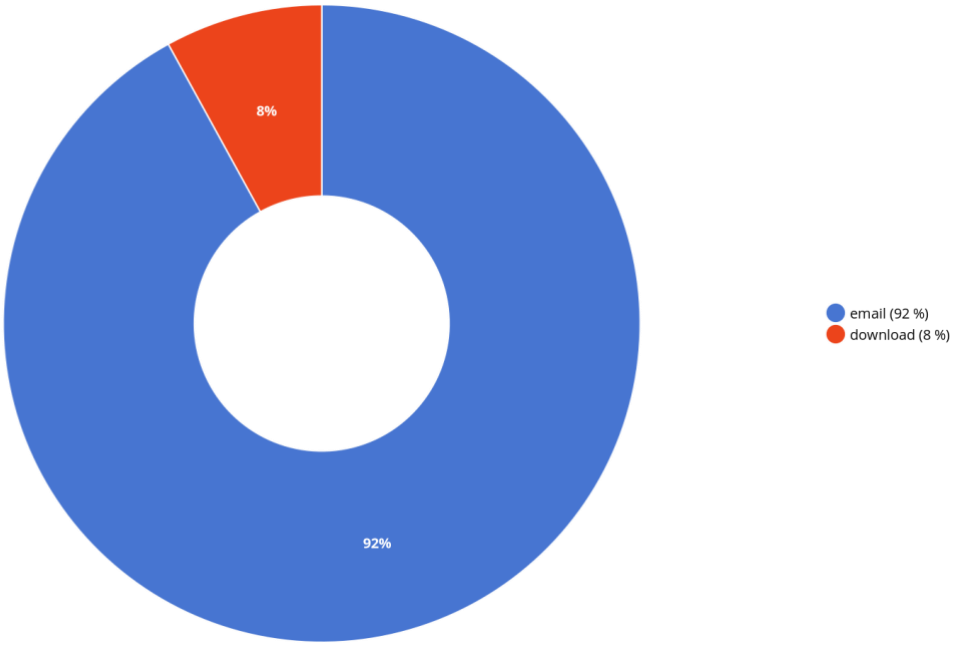


Figura 4. Vettori di attacco

Il phishing e lo spear phishing sono un veicolo così comunemente utilizzato per attacchi successivi e interessano tutti i settori (come mostrato nella Fig. X). Solo una piccola parte (8%) dei vettori dell'attacco è legata al "download di file", ovvero file scaricati da fonti non attendibili. Anche se in percentuale piccola, è preoccupante vedere come, in molte aziende, i dipendenti scarichino ancora file malevoli da fonti non attendibili. Questo avviene per diversi motivi ed è una conseguenza della mancanza o inadeguatezza dei controlli di sicurezza (firewall perimetrali e gateway di sicurezza) che non sono in grado di limitare adeguatamente il download di file malevoli. A ciò si accompagna, inoltre, un programma di sensibilizzazione inefficace o assente per i dipendenti volto a mitigare i rischi derivanti da un uso improprio dei beni aziendali.

Nella figura seguente (Fig. X) è possibile notare la distribuzione dei vettori di attacco in verticale sui settori; tale distribuzione non è uniforme tra i settori. Questa tendenza non indica che un settore sia più virtuoso degli altri, ma rispetto agli attacchi analizzati, le aziende di un settore o l'altro hanno politiche rigorose periodicamente valutate e riviste rispetto ad altre con controlli meno restrittivi.

È interessante notare che "Banking Services", "Retail", "Logistic Services" e "Software and IT" presentano un'alta percentuale di file scaricati malevoli nonostante tali servizi abbiano anche budget specifici da allocare sulla Sicurezza. Questo accade perché tali ambienti sono più eterogenei di altri e i dipendenti sono più inclini a scaricare servizi per il loro lavoro quotidiano.

Ci sono aziende che non presentano affatto casi di "download di file", molto probabilmente perché i dipendenti non hanno bisogno di scaricare software aggiuntivi ma usano semplicemente i loro PC con pochi programmi necessari per il loro lavoro. Cioè "Metals and Mining" o "Food and Drug retailing" o "Textiles and Apparel" sono settori in cui i dipendenti devono utilizzare apparecchiature o PC solo nelle linee di produzione, altrimenti in questo ambiente un attacco potrebbe avere un impatto catastrofico.

In conclusione, la posta elettronica rappresenta il vettore principale per distribuire malware nel business di oggi e la tendenza, rispetto agli anni passati, continua a crescere.

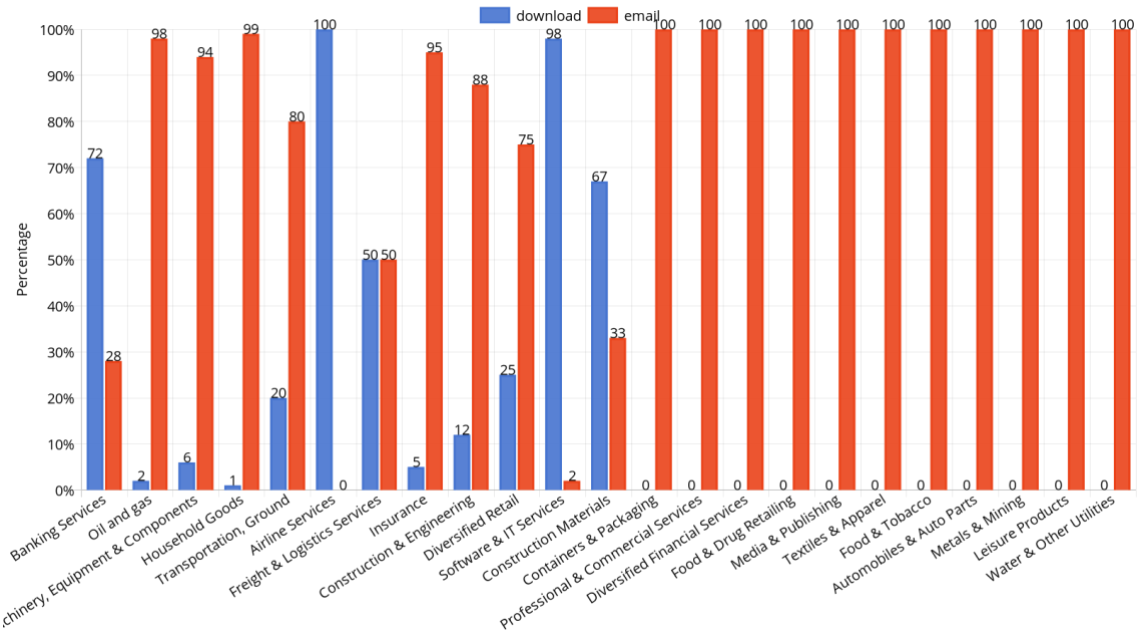


Figura 5. Industrie interessate dal vettore di attacco

La distribuzione temporale degli attacchi malware ci mostra le opportunità dell'aggressore in relazione al tempo e alla quantità:

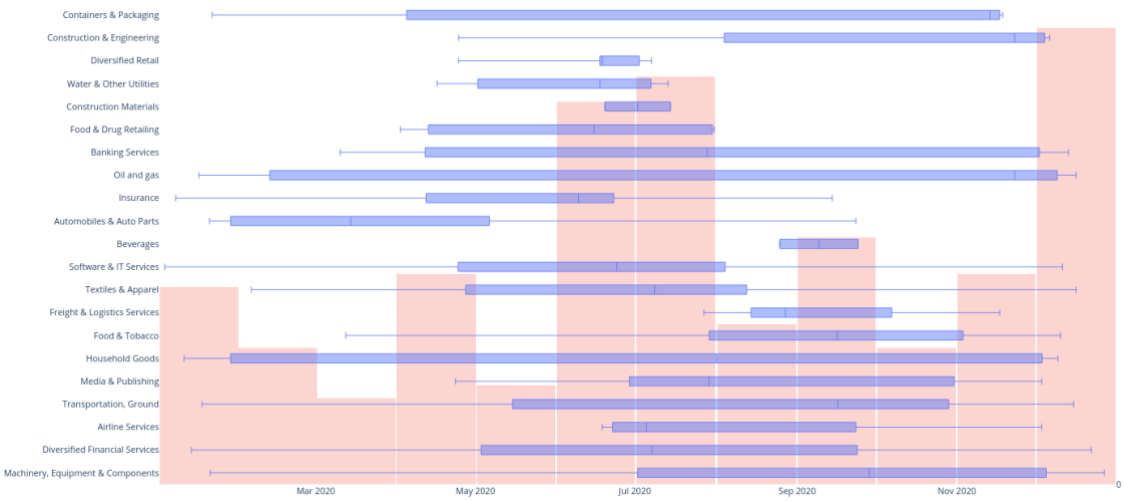


Figura 6. Distribuzione dell'attacco sui settori interessati

La tempistica degli attacchi dipende fortemente dal tipo di business. Dal diagramma sopra si nota che “Household Goods”, “Oil and Gas”, “Banking Services” e “Containers and Packaging” sono stati oggetto di attacchi informatici per lunghi periodi. Ogni settore di attività è stato impattato durante l'anno.

Propagazione e movimento laterale

La capacità di un attacco di propagarsi lateralmente sottolinea l'importanza di una strategia proattiva che permetta di ridurre i tempi di risoluzione di incidenti prima che si attui la propagazione

Spesso gli attacchi informatici vengono duplicati sui target. Gli attacchi odierni sono opportunistici e su larga scala, ciò significa che colpiscono più aziende in un breve lasso di tempo. Conoscere il modello di propagazione è importante per capire quanto velocemente gli attacchi si spostano da un business verticale all'altro. In un'operazione su larga scala, la prima organizzazione colpita si chiama Paziente Zero (PZero). Per condurre tale analisi, abbiamo elaborato i dati provenienti dalle nostre operazioni quotidiane per trovare e isolare PZero.
La figura seguente ci mostra il modello di propagazione di tali attacchi, è possibile notare che la minaccia più evidente è legata alle campagne di posta elettronica malevola (Phishing, Spear Phishing, CEO Fraud ecc.) che si propaga in quasi tutti i settori in un arco di tempo più breve. Una distribuzione più uniforme rispetto al 2019.
Questo comportamento di propagazione fornisce un'indicazione del carattere delle minacce che non sono mirate ma di natura opportunistica.

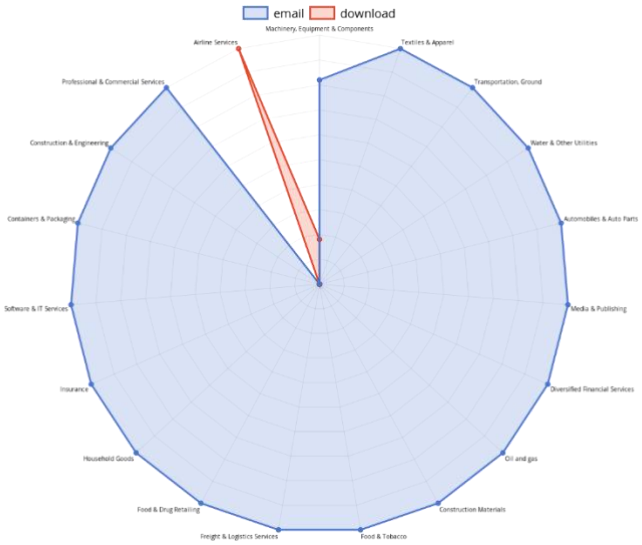


Figura 7. Settori paziente zero per vettore di attacco

I criminali informatici non si preoccupano del settore in cui opera un'azienda o delle dimensioni di un'azienda. Ogni settore industriale potrebbe essere un potenziale PZero e la propagazione verso altri business è solo questione di tempo. L'adozione di un approccio di Sicurezza Proattiva consente di affrontare le minacce informatiche e di offrire un elevato grado di controllo.
Abbiamo raccolto dati da più fonti e registrato i tentativi di propagazione di codice malevolo; l'analisi di tali dati ha mostrato interessanti peculiarità e differenze tra i verticali di settore.

Una volta penetrato all'interno di un confine, il malware può intensificarsi e propagarsi in tutta l'infrastruttura IT. Rispetto allo scorso anno abbiamo riscontrato un aumento importante del tempo complessivo di propagazione

laterale degli attacchi informatici (espresso in ore) principalmente in diversi settori come Banking Services, Textiles & Apparel, Freight & Logistics Services.

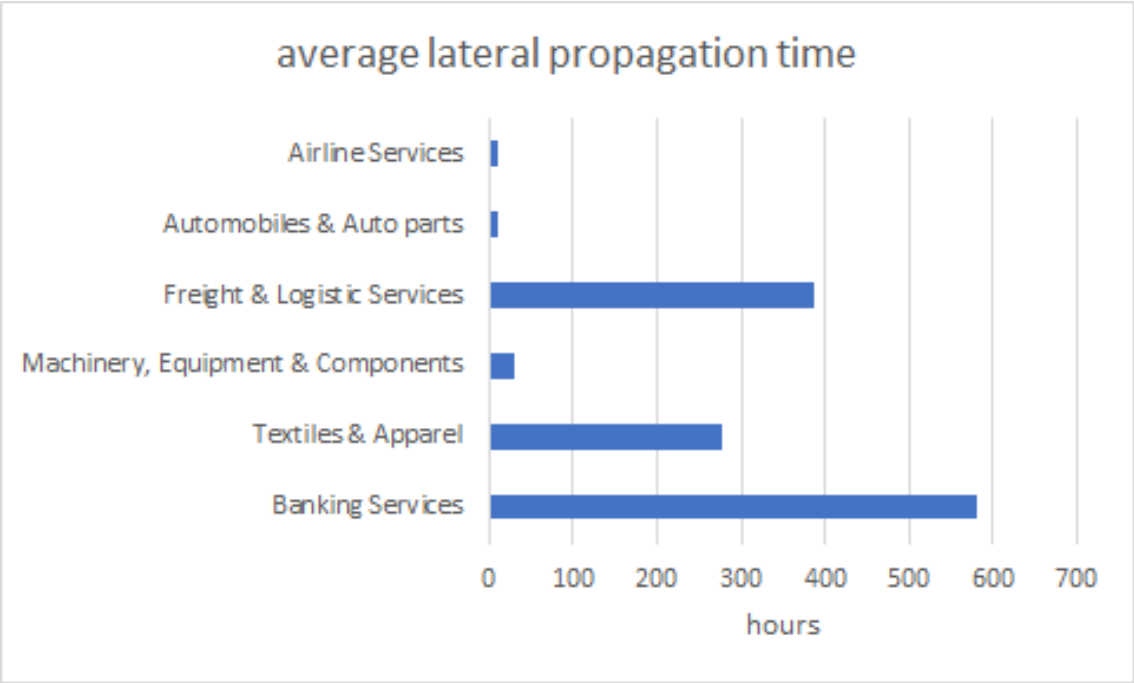


Figura 8. Tempi medi di propagazione del movimento laterale

I rapidi movimenti laterali avvengono nel settore Food&Drug Retailing, Diversified Financial Services and Construct Engineering registrando un tempo che va da pochi minuti a poche ore, e anche Automobiles & Auto parts e Airline Service registrano un tempo di propagazione laterale di poche ore (10/12 ore). Servizi come Banking, Textiles & Apparel e Logistics registrano un tempo di propagazione mediamente lungo, segno di difficoltà nella risoluzione degli incidenti.

Considerando la pervasività delle minacce odierne, la capacità di passare da un business all'altro in poche o decine di ore e la capacità di propagarsi lateralmente una volta all'interno di un perimetro sottolineano l'importanza di una strategia proattiva che permetta di ridurre i tempi relativi alla risoluzione di incidenti congiuntamente al consolidamento delle procedure di contenimento ed eliminazione.

Attacchi malware in Italia

Più della metà degli attacchi malware in Italia sono malware trojan bancario, con il 40% da parte della famiglia Ursnif, che si conferma essere la minaccia più martellante che insiste nel panorama informatico italiano.

Al giorno d'oggi gli attori delle minacce hanno costruito meccanismi coerenti in grado di fornire costantemente codice malevolo attraverso la costruzione delle cosiddette catene di infezione. In questo capitolo, infatti, ci

concentriamo sulla nostra area geografica, l'Italia, e analizziamo i risultati ottenuti grazie alla nostra telemetria raccolta dal nostro Cyber Security Defense Center e dalle nostre operazioni di Cyber Threat Intelligence.

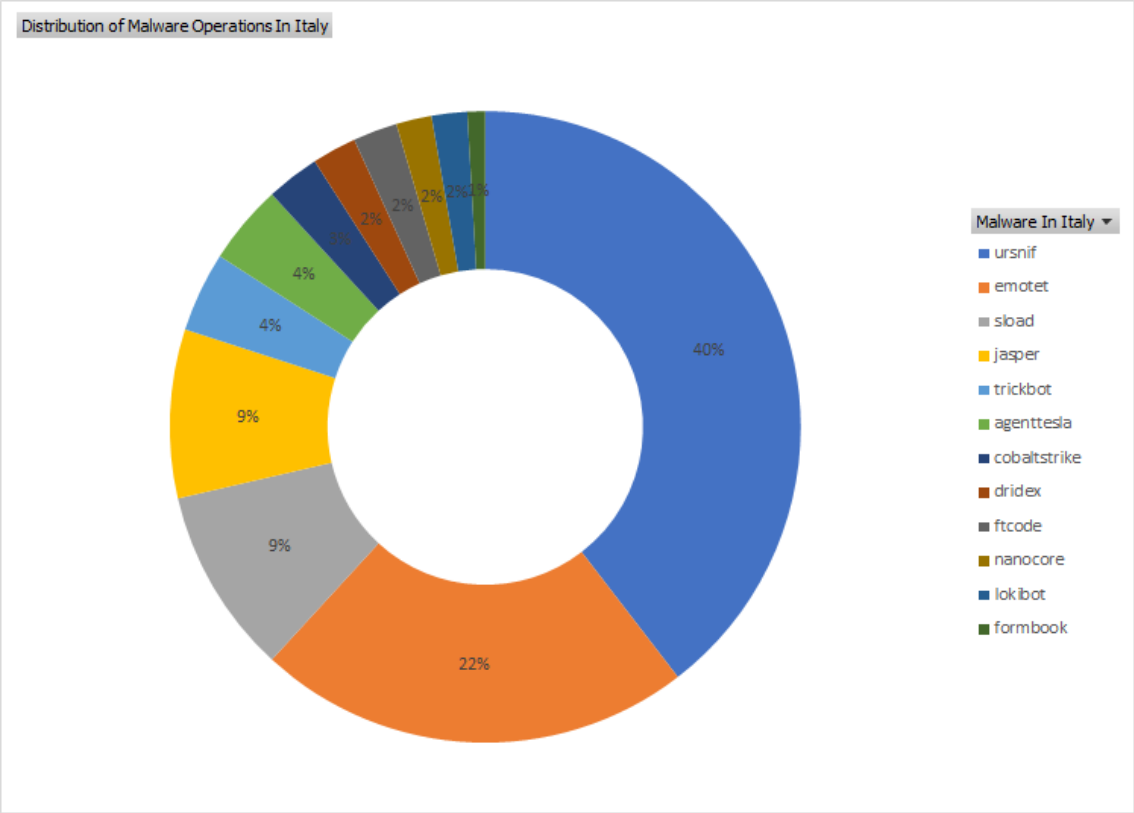


Figura 9. Distribuzione delle principali famiglie di minacce tra le ondate di attacchi di malware nel 2020

La figura mostra che più della metà degli attacchi malware in Italia forniscono malware trojan bancario, con il 40% in più per la famiglia Ursnif e il 22% con campioni Emotet. Questa tendenza non solo sottolinea ciò che abbiamo visto negli anni precedenti, ma mostra anche una maggiore rilevanza di questa classe di malware.

Ursnif conferma di essere la minaccia più martellante che insiste nel panorama informatico italiano. Negli anni ha costantemente aggiornato le tecniche di consegna del payload, grazie ad un'affascinante creatività nelle sue e-mail di phishing, partendo da word o fogli di calcolo e arrivando al payload finale abusando di PowerShell, macro XLM, steganografia e così via.

Emotet è stato ampiamente distribuito nella parte finale dell'anno con campagne massicce. A differenza di Ursnif, Emotet ha adottato uno schema di consegna più uniforme: di solito, l'infezione arriva tramite script dannosi o file di documenti abilitati per le macro. Le e-mail dannose in genere contengono un marchio familiare, con il logo "Microsoft Office 365", progettato per sembrare un'e-mail legittima e cercano di persuadere gli utenti a fare clic sui file dannosi utilizzando un linguaggio allettante su "La tua fattura", "Dettagli sul pagamento" o forse una spedizione imminente dalle società di consegna più comuni.
Dopo aver abilitato le macro, uno script di PowerShell inizia a scaricare il componente dannoso: una DLL da siti Web precedentemente compromessi, con URL personalizzati creati appositamente per l'ondata di attacchi. Tuttavia, a gennaio del 2021, un'azione internazionale coordinata condotta da Europol ed EuroJust ha consentito l'interruzione dell'intera infrastruttura dannosa.

WORLD'S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION

27 January 2021

Press Release

Law enforcement and judicial authorities worldwide have this week disrupted one of most significant botnets of the past decade: EMOTET. Investigators have now taken control of its infrastructure in an international coordinated action.

Figura 10. Interruzione della botnet Emotet gennaio 2021

SLoad e Jasper loader sono responsabili del 18% dei tentativi di distribuzione di malware. Sono caricatori di malware, con capacità di furto di informazioni, che offrono ai loro operatori un punto d'appoggio sulla rete di destinazione e la persistenza sulla macchina vittima, consentendo loro di distribuire i payload di malware arbitrari. La tendenza mostra la loro crescente importanza nella distribuzione del malware. Offrono agli avversari la possibilità di ottenere un punto d'appoggio iniziale su un sistema e vengono in genere utilizzati per fornire vari payload di malware in seguito a una compromissione riuscita.

In dettaglio, abbiamo deciso di approfondire sLoad perché sfrutta la posta PEC, la tecnologia italiana di posta certificata. sLoad è una delle poche famiglie di malware che sfrutta pesantemente le comunicazioni PEC per infettare le workstation sensibili. La vittima ritiene che la posta sia stata convalidata dall'autorità di certificazione PEC, tuttavia la posta spesso contiene un brutto archivio zip contenente un file Visual Basic Script dannoso, che rilascia ulteriori script Powershell. La particolarità di sLoad è la fase di appoggio iniziale, dove lo script Powershell raccoglie le informazioni sulla macchina vittima e solo dopo quella fase di ricognizione, il vero payload dannoso viene scaricato ed eseguito.

Trickbot e Cobalstrike hanno una percentuale inferiore ai due precedenti ma gli autori delle minacce li utilizzano in operazioni più sofisticate come negli attacchi Double Extorsion, descritti nella Sezione 1, l'evoluzione degli attacchi ransomware. In questo caso, gli avversari eseguono le operazioni effettive del Red Team per ottenere il massimo livello di privilegi e rilasciare il malware. Questi due malware sono una sorta di "coltellino svizzero" per molti gruppi che operano sotto questo paradigma di minaccia. In dettaglio, abbiamo osservato che Trickbot è correlato alle attività di ransomware Ryuk / Conti e Cobalt Strike è una sorta di jolly per la maggior parte delle operazioni di intrusione informatica, come abbiamo visto in molti incidenti critici durante lo scorso anno.

Altre minacce costanti nel panorama italiano sono i malware di furto di informazioni, come Lokibot, AgentTesla e Nanocore. Questo tipo di malware può essere utilizzato sia come strumento per attacchi opportunistici, ma anche per attacchi mirati. Nel primo caso, i gruppi criminali informatici sfruttano questi strumenti per creare basi di conoscenza per eseguire frodi o altri tipi di attacchi come il credential stuffing e simili. Queste famiglie di malware sono state utilizzate anche durante operazioni di attacco mirato, dove le funzionalità di info stealer erano utili per effettuare ricognizioni sui sistemi target, dove l'atto di rubare credenziali è fondamentale.

Alla fine, abbiamo notato lo sbiadimento del trojan bancario Gootkit nel panorama italiano. Negli ultimi anni, ha rappresentato una minaccia costante soprattutto grazie alle sue funzionalità Main-in-the-Browser. Ma nell'ultimo anno, la nostra telemetria in Italia non ha osservato alcuna operazione massiccia che sfrutta questo malware, che era ancora attivo in Europa e Germania nel novembre 2020.

Sezione 2:

Minacce bloccate

La maggior parte dei malware utilizza il protocollo DNS per comunicare con il proprio C&C al fine di ricevere comandi o scaricare payload, ma anche per condurre attività dannose come la ricognizione e l'enumerazione della rete. Il DNS, infatti, è un protocollo affidabile che permette di disaccoppiare il malware dalla propria infrastruttura e costruire un canale di comunicazione più flessibile. Ad esempio, il DNS è un abilitatore chiave per l'implementazione del meccanismo DGA, storicamente adottato da varie botnet o anche dalla backdoor Sunburst. DGA consente l'implementazione dinamica di alcuni endpoint Rendez-vous che puntano al C2 reale, questo meccanismo consente di rallentare l'identificazione e il tracciamento da parte di analisti e forze dell'ordine.

Per questi motivi, il DNS rappresenta una preziosa fonte di informazioni per gli operatori di intelligence sulle minacce. Il monitoraggio delle richieste DNS in entrata e in uscita consente di individuare e bloccare tali attività dannose, facendo la differenza nella protezione e difesa del perimetro. La tecnologia di difesa DNS di Yoroi ha bloccato 11.297 domini dannosi relativi a diversi tipi di minacce

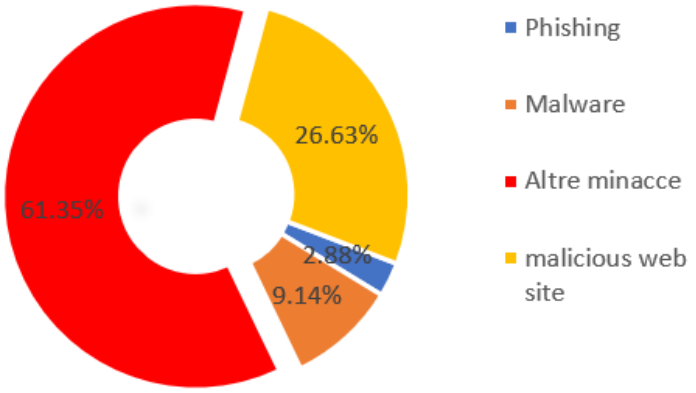


Figura 11. Distribuzione dell'attacco bloccata dalla tecnologia di difesa DNS di Yoroi

Il grafico (Fig XX) mostra la distribuzione delle minacce bloccate nel 2020: il 26,63% appartiene a siti Web dannosi che includono siti Web compromessi, malvertising, adware, frodi sui clic e siti Web illegali impostati con l'unico scopo di iniettare malware. Il 9,14% è correlato a minacce malware e alla loro infrastruttura come comunicazioni con Command and Control, URL utilizzato per la consegna del payload, repository di moduli malware. Il 2,88% dei domini bloccati è correlato al dominio di phishing. In questa categoria rientrano i domini utilizzati in campagne di phishing mirate con lo scopo di rubare credenziali o PII al fine di pianificare ulteriori attacchi sofisticati. Il 61,35% è classificato come "Altre minacce", dove troviamo tutti quei domini che non sono riconducibili a una delle categorie precedenti.

Queste minacce bloccate sono distribuite tra i verticali aziendali e l'analisi di tale distribuzione ci fornisce altre informazioni interessanti. È utile iniziare ad analizzare la distribuzione dei tentativi di phishing bloccati per settore industriale:

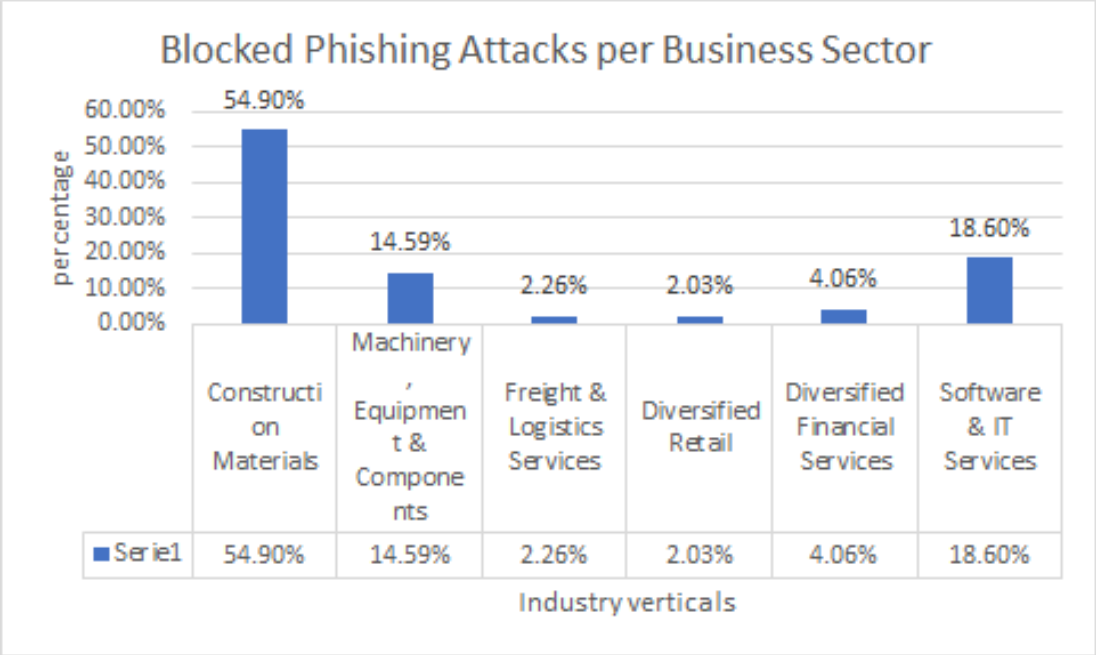


Figura 12. Attacchi di phishing bloccati distribuiti sui primi 6 settori

Quasi ogni tipo di violazione dei dati inizia con un attacco di phishing. L'andamento dell'ultimo anno non si discosta molto dal 2019. Più del 50% dei tentativi di phishing si è registrato nel settore dei Materiali da Costruzione che è composto da industrie produttrici di gesso, cemento, acciaio, legno, vetro e argilla e rappresenta un business importante per l'Italia. Segue Machinery, Equipements and Components Poi abbiamo trovato Software & IT Services (18,60%) che rappresentano un altro importante settore, molto sensibile al furto di proprietà intellettuali, inoltre i servizi finanziari sono un obiettivo prezioso per i cyber criminali.

Il phishing, in tutte le sue forme, rimane oggi una delle minacce più attive e insidiose. Questo perché viene consegnato tramite e-mail e utilizza sofisticate tecniche di ingegneria sociale che sfrutta le debolezze umane, è anche in grado di aggirare i filtri di posta indesiderata e EDR. L'impatto di un attacco riuscito potrebbe essere enorme e va dal furto di proprietà intellettuali, alla perdita di immagine, alla frode e al sabotaggio. Il rischio aumenta in settori critici come Acqua e Altre Utilities in cui il furto delle credenziali dei dipendenti può avere conseguenze dannose.

Per quanto riguarda la distribuzione degli attacchi malware bloccati per settore industriale, è possibile notare che la maggior parte di tali attacchi appartiene a 3 diversi gruppi: Construction Materials con il 73,21% seguito da Textiles & Apparel con il 19,84% e Food & Tobacco con un punteggio del 5,61%.

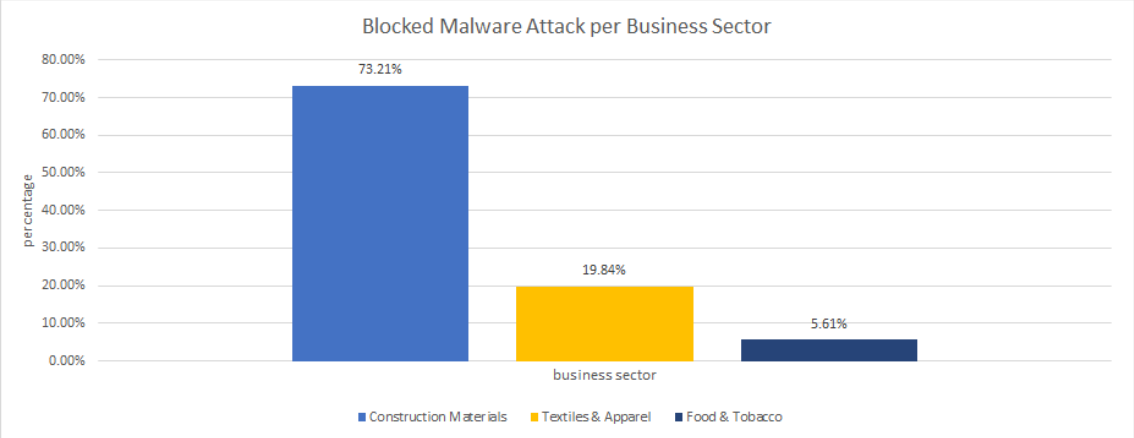


Figura 13. Attacchi malware bloccati distribuiti sui primi 3 settori

Botnet e attività opportunistiche

I dati relativi agli attacchi opportunistici sono utili per comprendere l'importanza di una strategia di reputazione IP basata su geofencing che deve prevedere il blocco di tutte le connessioni in entrata da quei Paesi ad alto rischio.

La firma di rete cambia nel tempo mentre il malware evolve costantemente il proprio comportamento, quindi la reputazione dell'IP e degli indirizzi è un fattore chiave per bloccare in modo proattivo gli attacchi opportunistici.

La tecnologia di Yoroi blocca e registra anche IP dannosi esterni che tentano di infiltrarsi o sfruttare risorse interne o esposte. Da questi IP si stanno conducendo attacchi su larga scala, opportunistici e geograficamente distribuiti.
Nella maggior parte dei casi, l'origine degli IP non riflette la reale origine dell'attacco perpetrato dalla botnet distribuita. Alcune Botnet utilizzano servizi di hosting DNS gratuiti come DynDns.org,

No-IP.com o IP Fluxing per mascherare la sorgente reale utilizzando una rete di host compromessi che funge da proxy. L'osservazione e l'analisi dell'origine di queste attività dannose forniscono spunti utili per la protezione del perimetro.

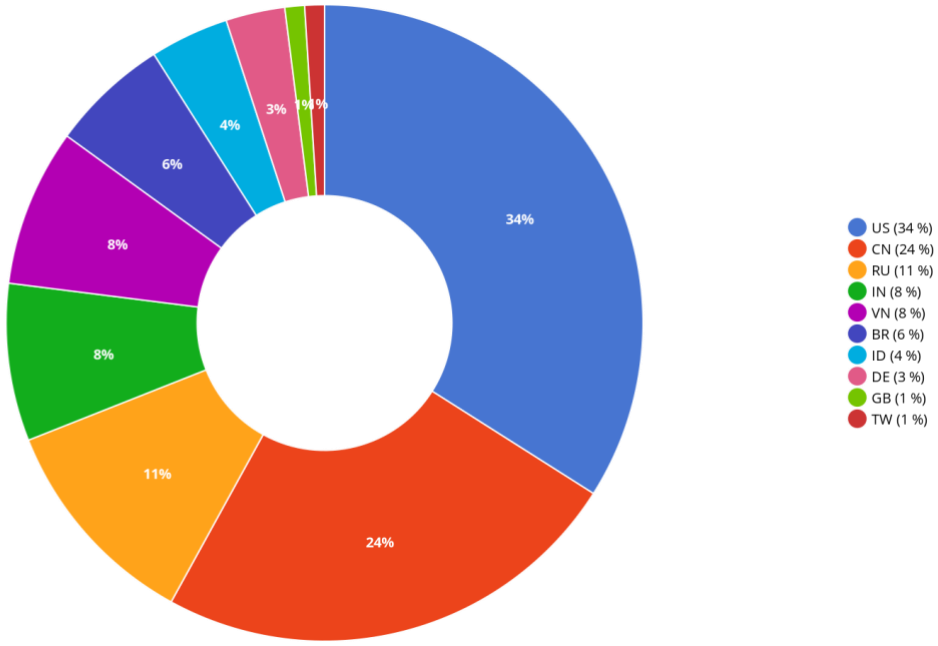


Figura 14. Paesi più attivi in attacchi opportunistici

Osservando la distribuzione (immagine del grafico a torta), gli Stati Uniti occupano i primi posti con il 34% di share che risulta in aumento rispetto all'anno 2019 (12%). Inoltre i tentativi provenienti dalla Cina (CN) sono scesi dal 31% del 2019 al 24%, come è possibile vedere nell'istogramma sottostante (Fig. X). I tentativi provenienti dalla Russia (RU) sono aumentati dal 9% all'11% mentre India (IN), Vietnam (VN), Brasile (BR), Taiwan (TW) e Indonesia (ID) condividono il 26% della distribuzione totale rispetto a un totale del 41% nel 2019. Per il 2020 abbiamo due new entry: Germania (DE) con il 3% e Regno Unito (1%) che diventano apprezzabili in valore assoluto.

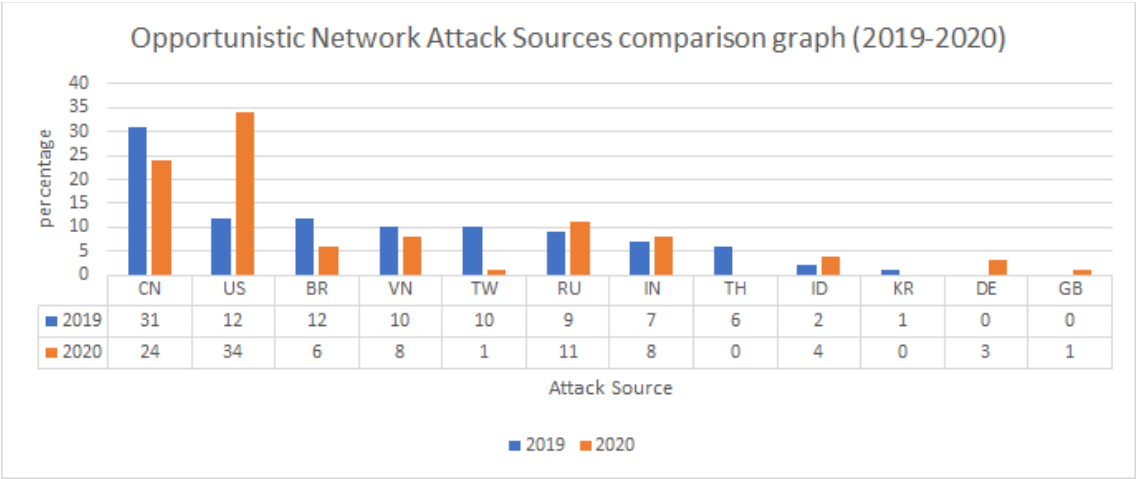


Figura 15. Confronto tra le principali fonti di attacchi opportunistici

I cambiamenti nella distribuzione dell'ultimo anno rispetto al 2019 sono da considerarsi "normali" poiché gli attacchi sono di natura opportunistica quindi, molto spesso le reti coinvolte in tali tentativi sono reti di zombie precedentemente compromesse. USA, CN e RU sono i paesi più grandi e questo è il motivo per cui la maggior parte delle reti Botnet proviene da lì. Inoltre, per quest'anno abbiamo registrato anche alcuni paesi europei.
Questi dati potrebbero essere utili per comprendere l'importanza di una strategia di reputazione IP geofencing che deve considerare i paesi con i quali esistono rapporti commerciali. Infatti, se la società ha una propria attività negli Stati Uniti e non in Cina, ad esempio, si consiglia di 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 entrata potrebbe essere una buona strategia di difesa proattiva insieme ad altre mitigazioni come la reputazione DNS e la soluzione di firma di rete.

Sezione 3:

La minaccia delle e-mail

Gli avversari continuano a preferire le e-mail come principale vettore di diffusione del malware. Per il quarto anno consecutivo, le e-mail dannose rappresentano una parte rilevante degli attacchi informatici. I criminali sono liberi di adottare due diverse strategie per sviluppare una campagna di spam dannoso, ovvero "malspam". Il primo è costruire un kit di exploit resiliente o sfruttare le botnet per diffondere campagne generiche per colpire privati cittadini e piccole imprese.

Un esempio potrebbe essere una mail di fattura con un documento di Office dannoso che richiede l'abilitazione delle macro per visualizzare l'intero contenuto del documento. Quindi, prendendo di mira le vittime di alto valore e preparando la posta elettronica sfruttando temi specifici e l'accesso a caselle di posta affidabili.

Inoltre, l'anno 2020 sarà ricordato dalla storia a causa della pandemia COVID-19, anche dai criminali informatici. In effetti, hanno sfruttato le pandemie per fare in modo che le e-mail dannose sembrassero più impattanti sulla sfera emotiva dei loro bersagli. Inoltre, la situazione pandemica ha costretto le aziende ad adottare cambiamenti immediati, come il lavoro intelligente, a distanza o completamente a distanza. Le conseguenze hanno avuto un impatto negativo sulla sicurezza degli utenti che, in molti casi, operavano fuori dal perimetro di sicurezza.

Esaminando la telemetria raccolta dall'infrastruttura di monitoraggio del Cyber Sceurty Defense Center, possiamo confermare che i documenti di Microsoft Office sono il vettore di distribuzione di malware più rilevante, rappresentando il modo più comune per diffondere la prima fase della catena di infezioni da malware. Infatti, i documenti Microsoft Word (35%) e i fogli di calcolo Excel (33,2%) rappresentano collettivamente il 68,2% di tutti gli allegati dannosi intercettati dai servizi di protezione e-mail di Yoroi.

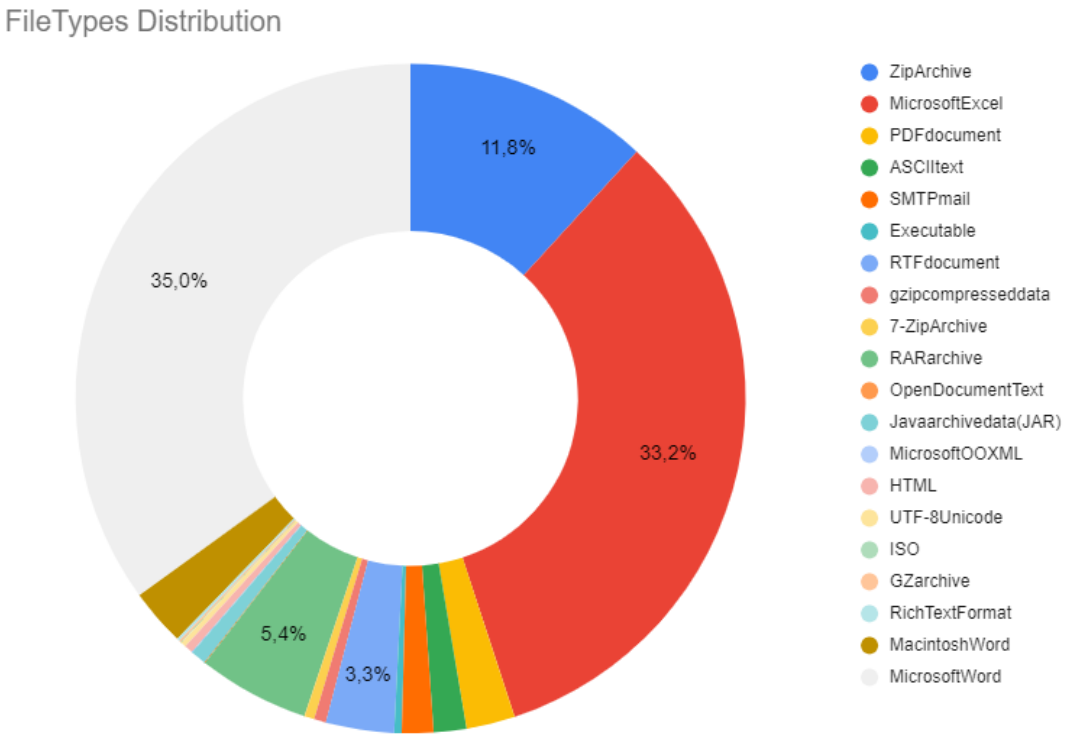


Figura 16. Distribuzione di allegati dannosi

La percentuale di documenti dannosi in generale è ancora più alta. Infatti, una delle ultime tattiche adottate dai criminali informatici è quella di comprimere gli allegati all'interno di un file di archivio (zip, gzip o rar, 7zip) e crittografarli con una password citata all'interno del corpo della mail. È un metodo abbastanza semplice, ma è stato molto efficace durante lo scorso anno.

Un'altra tecnica ampiamente utilizzata nel 2020 è stata l'abuso di XLM Macro 4.0. XLM Macro 4.0 è una tecnologia legacy ancora supportata nelle moderne suite Office, che sono state abusate per eludere il rilevamento antivirus e antispam delle classiche firme antivirus e consentire la seconda fase della catena di infezioni da malware.
Tuttavia, la nostra tecnologia sandbox, Yomi, può analizzare questo tipo di tecniche e rilevare gli allegati di comportamento dannoso e la aggiorniamo costantemente per rilevare i nuovi trucchi anti-rilevamento.

Il gruppo composto da immagini ISO, documenti RTF, così come è eseguibile, archivi JAR ecc. Rappresenta la fetta più piccola della torta. In passato, questi tipi di formati di file ricoprivano un ruolo più importante nel panorama delle minacce. Tuttavia, il miglioramento del rilevamento degli exploit e dell'introspezione del codice implementati all'interno dei confini perimetrali e dei sistemi di protezione degli endpoint rendono più difficile la diffusione diretta di queste minacce. Dall'altro lato, gli attori delle minacce, al fine di aggirare tali contromisure, hanno creato una catena di infezioni più lunga, implementando attacchi multistadio molto più complessi basati su sofisticate infrastrutture DropURL e C2. Stiamo giocando una sorta di gioco "gatto e topo" con gli avversari.

Un altro punto interessante da analizzare sono i trucchi di ingegneria sociale utilizzati dagli aggressori per indurre l'utente a fare clic sul collegamento o allegato dannoso. Anche quest'anno, abbiamo condotto diversi studi sugli algoritmi di clustering di machine learning per rilevare quanti sono i cluster dell'oggetto del messaggio e del nome dell'allegato, riferiti a una diversa campagna di malspam.

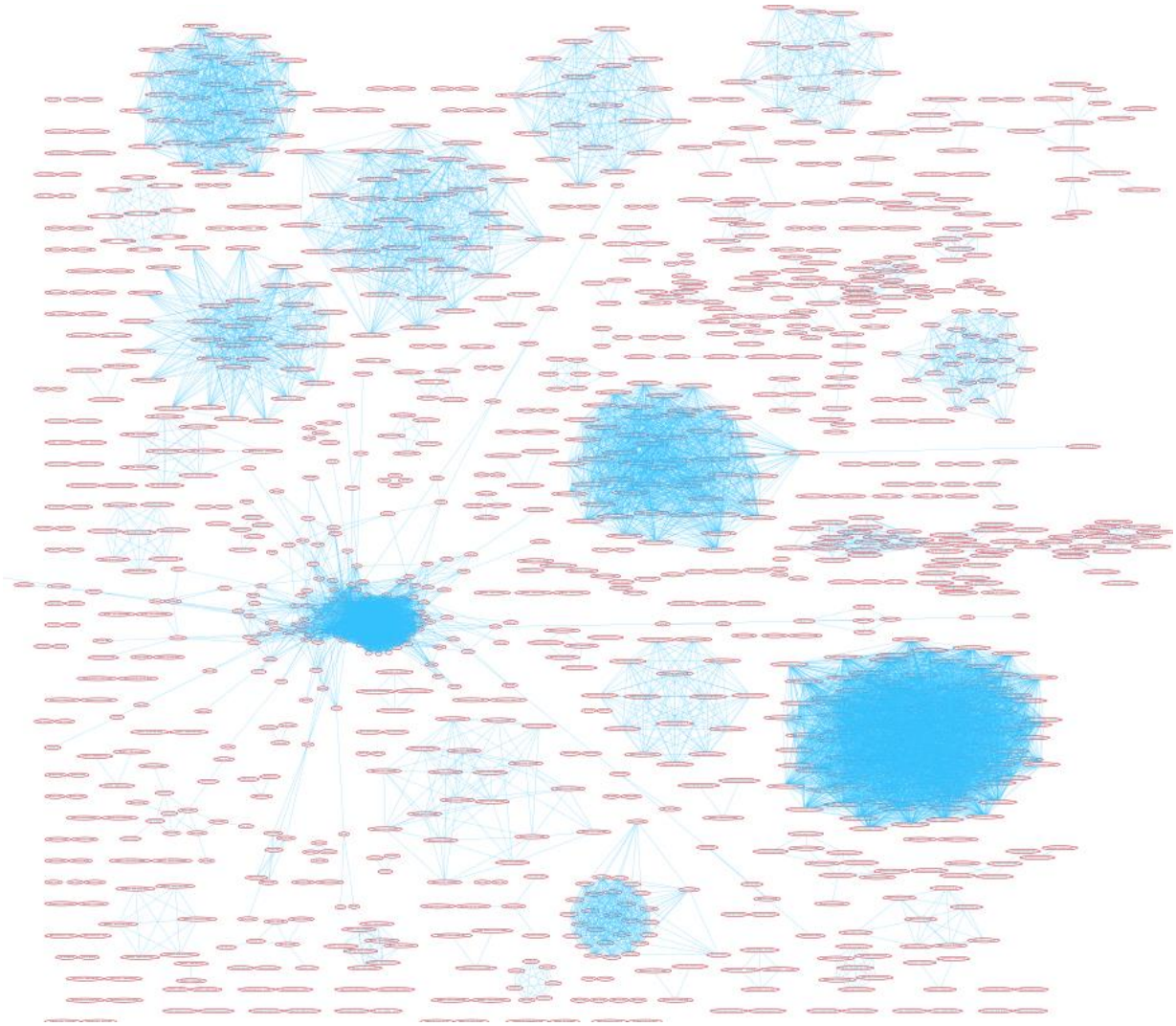


Figura 17. Cluster di temi di spam dannosi

La nostra analisi dell'elaborazione del linguaggio naturale ha rivelato che quest'anno abbiamo almeno dodici diverse campagne principali di malspam: il doppio rispetto all'anno scorso!
Gli argomenti sono praticamente gli stessi dei risultati del Bilancio annuale passato, gli argomenti sono i seguenti:

- Fatture e ordini
- Consegna e monitoraggio dei pacchi
- Moduli fiscali
- Certificati medici
- Curriculum vitae
- Risposte ai thread precedenti
- Messaggi generici come
    - "Ciao, spero che tu stia andando bene"
    - "All'attenzione di"
    - o "Lavoro d'ufficio"
    - o ecc.

Oltre a loro, vogliamo mantenere la vostra attenzione sulla peste emergente del 2020, la pandemia Covid-19. Come accennato in precedenza, questo argomento tocca non solo la sfera professionale dell'utente, ma anche quella emotiva. I criminali informatici lo sanno e usano questo difetto a loro vantaggio.

Hanno creato specifiche campagne di malspam sfruttando questo argomento, siamo stati in grado di intercettarle e identificarle. Abbiamo trovato migliaia di messaggi con quell'argomento e le principali categorie di argomenti della posta sono grossolanamente:

- Fatture e ordini relativi a covid-19
- Informazioni, istruzioni o procedure sulle precauzioni covid 19
- Rinnovare le campagne
- Campagne di cashback
- Ritardi nei pagamenti

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

Sezione 4:

Tendenze delle tecniche di attacco

Nuove minacce dalla Supply-Chain

Gli attacchi alla Supply Chain sono spinti da spionaggio o sabotaggio di specifici target e possono avere un impatto su qualsiasi componente hardware o software in produzione

Gli attacchi alla catena di fornitura (T1195.001) sono considerati la forma di minaccia più sofisticata e rappresentano un rischio significativo per le organizzazioni moderne. Storicamente tali minacce sono perpetrate da APT sfruttando e infiltrandosi nella pipeline di produzione al fine di impiantare malware o per interruzione. Come affermato da MITRE "Gli avversari possono manipolare i prodotti o i meccanismi di consegna dei prodotti prima della ricezione da parte di un consumatore finale allo scopo di compromettere i dati o il sistema".

Gli attacchi alla catena di fornitura possono avere un impatto su qualsiasi componente hardware o software in produzione, mentre le principali motivazioni alla base sono lo spionaggio e il sabotaggio di obiettivi specifici, gli attori delle minacce possono passare a tattiche aggiuntive e prendere di mira un ampio gruppo di consumatori.

Il 2020 è anche l'anno dell'attacco alla supply chain di SolarWinds. SolarWinds produce la suite Orion, un software di monitoraggio e gestione della rete utilizzato da organizzazioni di tutto il mondo. L'attacco consiste nel compromettere la pipeline Orion DevOps e inserire una backdoor DLL dannosa denominata Sunburst, segnalata per la prima volta a dicembre 2020.

L'incidente ha colpito più entità in tutto il mondo, inclusi governi, agenzie di intelligence, grandi aziende tecnologiche, telecomunicazioni ecc. A causa della diffusione e della popolarità del software Orion, il relativo rischio e impatto di questo incidente è considerato catastrofico.

Backdoor di Sunburst

Il componente backdoor è il plugin SolarWinds.Orion.Core.BusinessLayer.dll della suite Orion, firmato digitalmente da SolarWinds che comunica con un server di terze parti (C2) tramite protocollo HTTP.

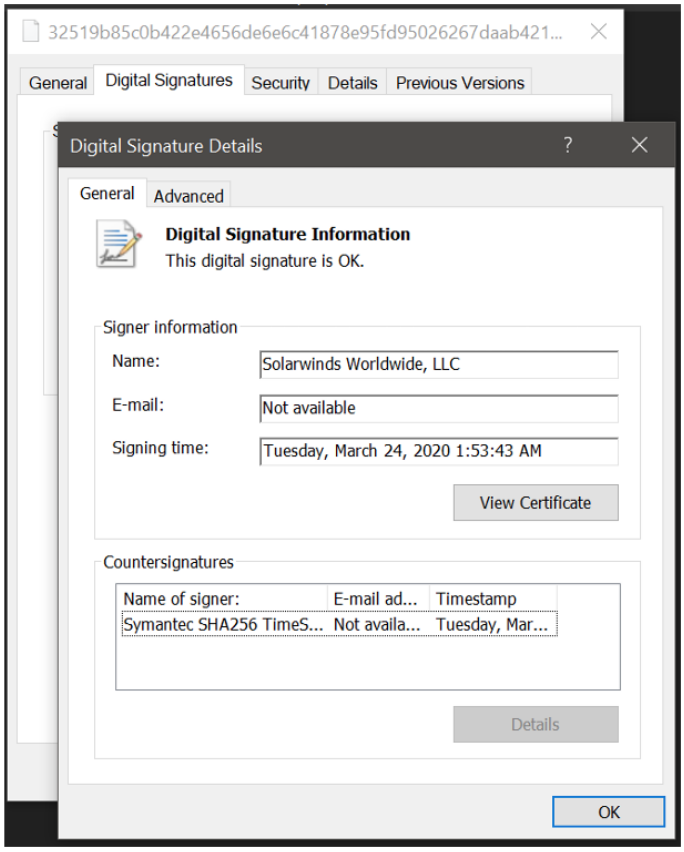


Figura 18. Backdoor Sunburst firmato da SolarWinds

Una volta installato il componente backdoor sul sistema, consente il dispiegamento di diverse attività di post exploitation adottando tecniche con un leggero footprint sul sistema. Infatti, la backdoor sunburst consente la distribuzione di diversi payload dannosi e dropper di sola memoria (TEARDROP) e l'installazione di beacon Cobal Strike. Una volta che la backdoor avvia l'esecuzione, rimane inattiva per due settimane, quindi avvia ed esegue "lavori" responsabili della profilazione del sistema, dell'esecuzione dei file e della disabilitazione degli strumenti forensi e antivirus. Il Threat Actor utilizza diverse tattiche per evitare sospetti ed eludere il rilevamento, di seguito sono riepilogati:

- Spostamento laterale utilizzando credenziali diverse.
- Contagocce di sola memoria e beacon malleabili.
- Indirizzi IP situati in diversi paesi.
- I nomi host dell'attaccante corrispondono all'ambiente della vittima.
- Utilizzare un algoritmo DGA e un intermediario C2.

Inoltre, il comportamento backdoor è mascherato all'interno dell'attività legittima di SolarWinds come Orion Improvement Program (OIP). L'attore della minaccia compartimentalizza le proprie operazioni limitando l'esposizione dell'infrastruttura a ciascuna vittima. Di seguito viene riepilogato il flusso di comunicazione. Il C2 intermedio (coordinatore) istruisce la backdoor e reindirizza SUNBURST al C2 reale tramite record CNAME DNS. Il C2 intermedio funge da server DNS autorevole per il dominio avsvmcloud [.] Com, quindi, per comunicare con il coordinatore C2, SUNBURST utilizza un DGA per costruire sottodomini e risolverli. Questa campagna dannosa è stata condotta con un alto livello di sicurezza operativa e poteva essere rilevata solo con l'implementazione di una strategia di difesa persistente.
Lo sforzo per non farsi rilevare dall'attore della minaccia è impressionante, inoltre scrivono la backdoor con lo stile di codifica SolarWinds ed evitano di infettare la loro rete interna con controlli specifici sui nomi di dominio trovati all'interno della backdoor .NET

```
private static readonly ulong[] patternHashes = new ulong[]
{
    //    HASH                    CRACKED              ASSUMPTIONS
    //  ---------                 ---------           --------------
    1109067043404435916UL,      // 'dev.local' ->  SolarWinds Dev local
    15267980678929160412UL,     // 'swdev.dmz' ->  SolarWinds Development DMZ
    838129226599397726 6UL,     // 'lab.local' ->  Local lab
    379640562369566552 4UL,     // 'lab.na'    ->  SolarWinds North America office
    457848084625562946 2UL,     // 'lab.brno'  ->  SolarWinds Brno office
    872747776954430206 0UL,
    107341270042448797 70UL,    // 'cork.lab'  ->  SolarWinds Cork office
    110732833111045416 90UL,    // 'dev.local' ->  Development
    403023641397519965 4UL,     // 'dmz.local' ->  Demilitarized Zone
    770168327982439777 3UL,
    513225662010499863 7UL,     // 'saas.swi'  ->  maybe: SaaS SolarWinds
    594228205252529491 1UL,     // 'lab.rio'   ->  maybe: SolarWinds Rio Office
    168589559781464066 42UL     // 'apac.lab'  ->  SolarWinds APAC offices
};
```

Figura 19. Controllo preliminare della backdoor Sunburst

Tutti questi elementi ci danno un'idea del livello di sofisticazione di questa campagna, l'obiettivo è chiaro: rubare dati da organizzazioni strategiche ed entità di intelligence in tutto il mondo in modo che la suite Orion sia solo un mezzo e non il vero obiettivo. SolarWinds ha oltre 300.000 clienti tra cui (in base al sito Web dell'azienda):

- Più di 425 delle società Fortune 500 degli Stati Uniti
- Tutte e dieci le prime dieci società di telecomunicazioni statunitensi
- Tutti e cinque i rami delle forze armate statunitensi, il Pentagono degli Stati Uniti, il Dipartimento di Stato, la NASA, la NSA, il servizio postale, il NOAA, il Dipartimento di giustizia e l'Ufficio del Presidente degli Stati Uniti
- Tutte e cinque le prime cinque società di contabilità statunitensi
- Centinaia di università e college in tutto il mondo

Questo elenco non è affatto esaustivo, ma ci dà la percezione e l'ampiezza della campagna. Un altro elemento del suo successo è che SolarWinds Orion opera con i privilegi di accesso più elevati, per questo motivo qualsiasi controllo di sicurezza basato sull'accesso è inefficace.
Sulla base della telemetria condivisa, possiamo confermare che la preminenza dell'organizzazione interessata proviene dagli Stati Uniti, seguiti dal Regno Unito e sparsi tra gli altri paesi. Anche l'Italia purtroppo ne è stata colpita, ea causa della prevalenza di tale operazione, sin dalle prime fasi della scoperta l'Italia ha attivato il Cyber Security Nucleus (Nucleo Tecnico per la sicurezza cibernetica), struttura creata dalla Presidenza del Consiglio dei

Ministri nel 2017 che è responsabile del coordinamento della risposta a qualsiasi attacco informatico che potrebbe avere un potenziale impatto sulla sicurezza nazionale. Il Nucleo, per tutte queste organizzazioni che utilizzano la piattaforma Orion, consiglia di esaminare il problema con la massima e attenzione, avvalendosi a tal fine dell'apposita sezione creata sul sito del CSIRT italiano, contenente consigli, aggiornamenti ed eventuali misure di mitigazione degli incidenti.
In una dichiarazione congiunta FBI, CISA e NSA attribuiscono la responsabilità delle intrusioni a un APT, molto probabilmente russo. Il 17 dicembre, la Cybersecurity and Infrastructure Security Agency (CISA) del DHS ha rilasciato un avviso che fa riflettere sull'attacco SolarWinds, osservando che CISA aveva prove di vettori di accesso aggiuntivi diversi dalla piattaforma SolarWinds Orion. L'avviso della CISA ha specificamente rilevato che "uno dei modi principali con cui l'avversario raggiunge questo obiettivo è compromettere la firma SAML (Security Assertion Markup Language)";
L'autenticazione basata su SAML viene utilizzata anche da SolarWinds e si basa sui servizi federati Active Directory di Microsoft.
Come indicato nell'avviso, CISA ha le prove che esistono altri vettori di accesso iniziale [TA0001] oltre alla piattaforma Orion di SolarWinds. Infatti, CISA ha individuato alcuni compromessi in cui le vittime non utilizzano la piattaforma Orion o dove è stato osservato uno sfruttamento non attivo di Orion.
Gli altri vettori di accesso iniziale sono costituiti da abuso di password [T1101.001], irrorazione di password [T1101.003], servizi di accesso remoto esterni [T1133] e compromissione del certificato di firma SAML utilizzando i privilegi di Active Directory intensificati: TTP coerenti con quelli utilizzati nel compromesso della catena di approvvigionamento di SolarWinds Orion.

Deep Web e violazioni della sicurezza

L'impatto della fuga di dati sui gateway VPN Fortinet è enorme, poiché i dati erano legati a una vulnerabilità di 2 anni e ci sono IP relativi a importanti aziende, banche e organizzazioni governative in tutto il mondo, comprese quelle italiane

Un altro incidente importante ha caratterizzato il 2020: la pubblicazione di una fuga di dati relativa al CVE 2018-13379 sui gateway VPN Fortinet. Il 19 novembre 2020 infatti, la fuga di circa 49.000 IP di gateway VPN Fortinet vulnerabili è stata rilasciata su un popolare forum di hacking.

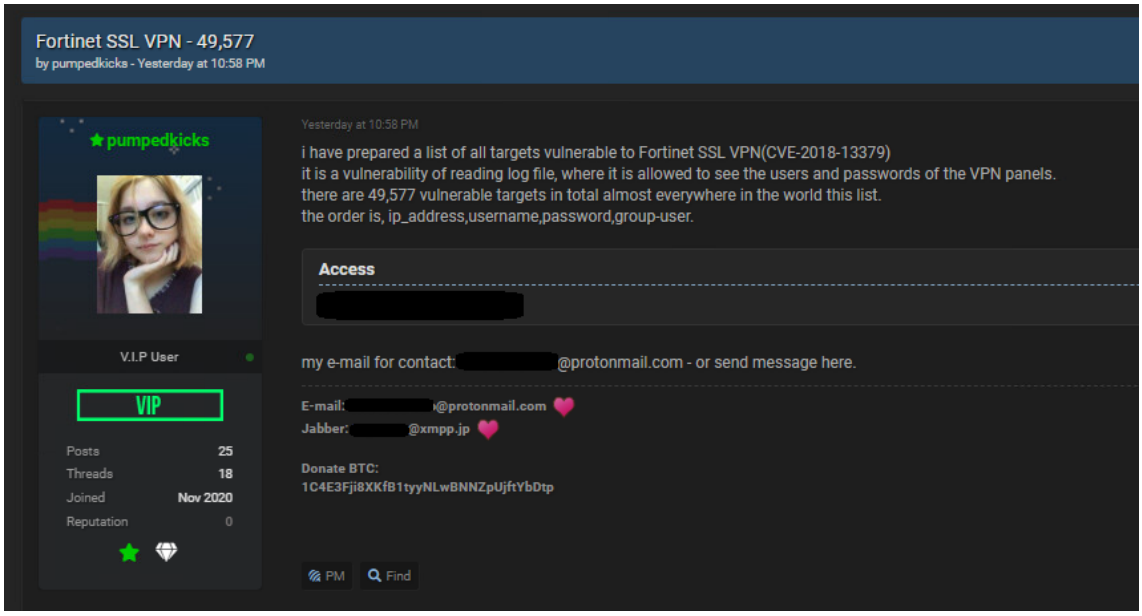


Figura 20. Annuncio dell'elenco delle vulnerabilità VPN di Fortinet

Circa 6 giorni dopo, sullo stesso forum, un altro attore ha anche pubblicato un elenco di credenziali in chiaro relative allo stesso elenco di IP di Fortinet. L'entità dell'impatto è enorme, poiché i dati erano legati a una vulnerabilità di 2 anni, in tale fuga di notizie ci sono IP relativi a importanti aziende, banche e organizzazioni governative in tutto il mondo, comprese quelle italiane e ancora non patchate.

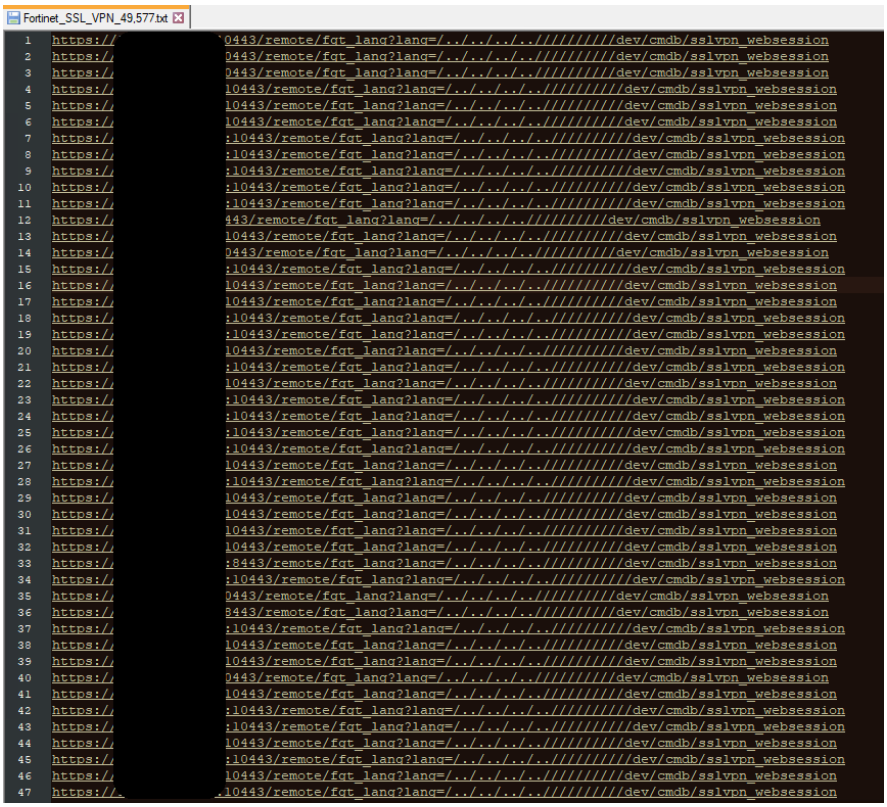


Figura 21. Elenco delle vulnerabilità VPN Fortinet

Il CVE 2018-13379 è una vulnerabilità di attraversamento del percorso in alcune versioni di FortiOS (da 6.0.0 a 6.0.4, da 5.6.3 a 5.6.7) a causa di una convalida impropria di un nome di percorso in una directory limitata, consente un utente malintenzionato non autenticato per scaricare il file sslvpn_websession (che contiene le credenziali) tramite richieste HTTP speciali nel portale web SSL VPN. Il punteggio di base CVSSv3 del CVE 2018-13379 è 9,8 con gravità definita come critica. In un joint advisory pubblicato lo scorso ottobre, CISA e FBI hanno riferito che anche l'APT Russian Energetic Bear sta usando questo e altri exploit per portare attacchi contro vari obiettivi critici degli Stati Uniti.
Queste credenziali stanno ancora circolando sul Web, quindi potrebbero essere semplicemente consultate e utilizzate in modo improprio da un attore malintenzionato per infiltrarsi in modo non autorizzato all'interno delle infrastrutture e rubare dati o impiantare malware per diversi scopi dannosi. Una quota di questi IP esposti appartenenti ad organizzazioni italiane: 1639 numero di protocollo internet appartenente ad organizzazioni italiane perché relativo a provider italiani, corrispondente a circa il 3,3% degli IP esposti. La quota italiana è composta da IP relativi ai seguenti settori:

- ISP: 91%
- Istruzione: 0,25%
- Affari: 3,7%
- Hosting: 4,93%

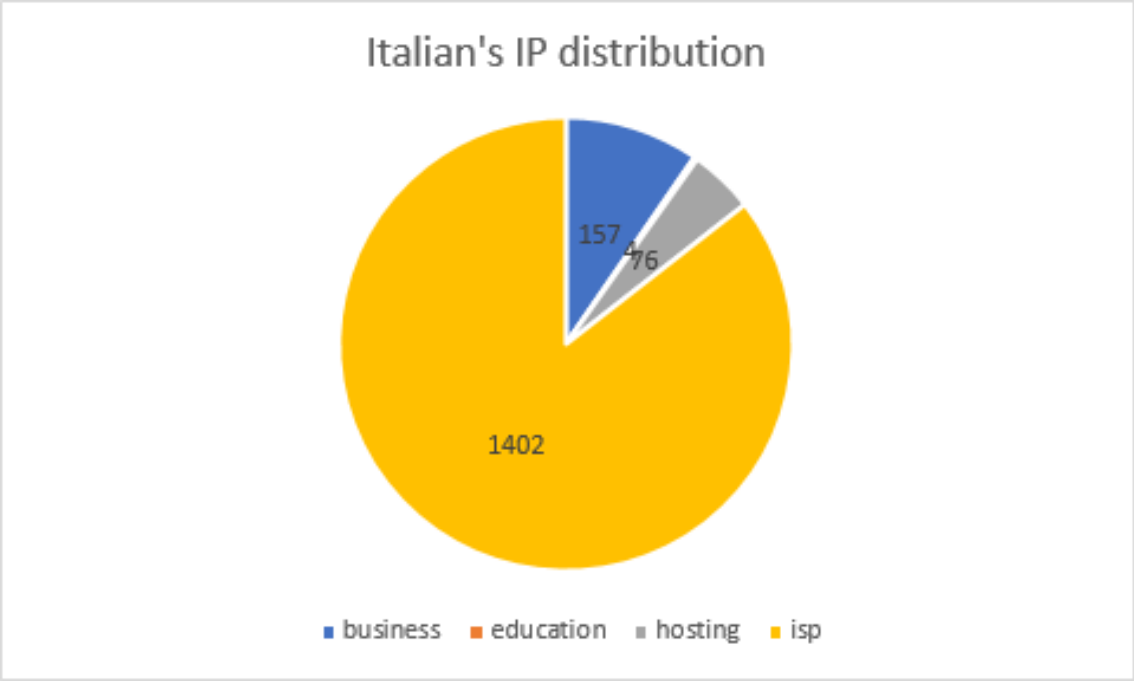


Figura 22. Distribuzione della vulnerabilità VPN Fortinet in Italia

È possibile notare che la maggior parte di questi IP appartiene a reti ISP (91%), seguita da Hosting (4,93%), Business (3,7%) e Education con appena lo 0,25% della quota totale. Tuttavia, questi numeri non danno la dimensione reale della superficie di attacco, che è molto più grande, perché, molto probabilmente, c'è un numero enorme di sistemi ancora pubblicamente esposti e non già patchati.

Per un malintenzionato non è difficile cercare endpoint vulnerabili, considerando che Fortinet Fabric è abbastanza diffuso in alcuni ambienti.

Oggi la maggior parte delle organizzazioni rimane ancora vulnerabile e non ha ancora patchato questa vulnerabilità, questo perché non tutte predispongono e implementano un adeguato programma di gestione delle vulnerabilità che è fondamentale per un'efficace strategia di mitigazione del rischio informatico.

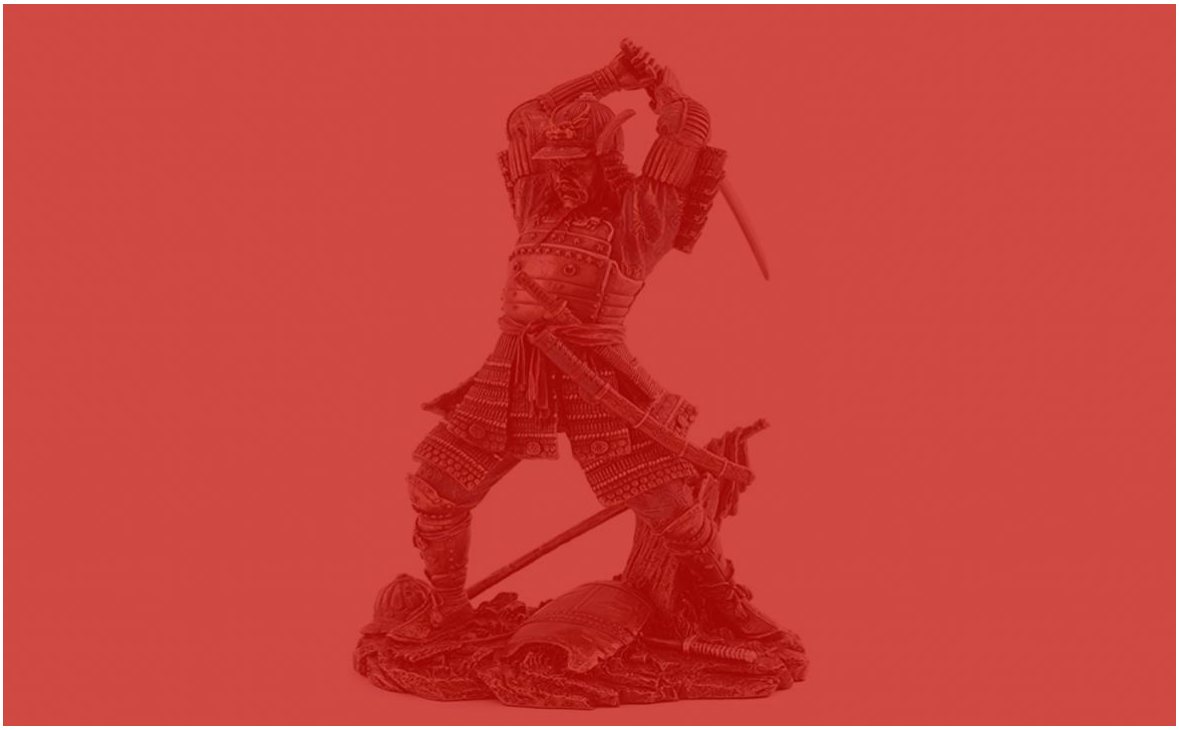
Conclusioni

Negli ultimi 12 mesi l'intera società è cambiata radicalmente. Il Covid-19 è stato in grado di rallentare le economie, di cambiare il modo in cui molti di noi lavorano, di spostare quote di mercato e di forzare drasticamente il modo in cui le aziende gestiscono il loro spazio digitale. La tecnologia digitale ha aiutato l'intera società durante i frequenti e diffusi lockdown fornendoci un modo per comunicare, condividere esperienze e continuare a lavorare da casa. Il lavoro a distanza ha consentito ai router domestici o ai personal computer di connettersi direttamente agli asset aziendali. Di solito aprendo tunnel VPN in grado di aggirare i confini perimetrali, consentendo le connessioni dei guerrieri digitali direttamente sulla LAN interna. Molte aziende si sono trovate ad avere connessioni esterne provenienti da macchine non attendibili direttamente alle loro reti di gestione o a quelle aziendali, dal momento che gli amministratori IT dovevano operare tramite VPN o i lavoratori dovevano interagire con il CRM interno per muovere il business da case private. Questo è stato uno dei percorsi di attacco più abusati negli ultimi mesi. Fondamentalmente, gli aggressori che sfruttano i dispositivi domestici non protetti hanno atteso di connettersi al VPN e quindi hanno iniziato un passaggio laterale da tale dispositivo agli asset interni. Questi asset non erano progettati per distinguere attacchi interni poiché prima del lockdown erano protetti da proxy, IDS, firewall, soluzioni DNS e così via. Molto spesso i servizi aziendali non sono stati progettati per avere accesso diretto a dispositivi esterni e non protetti. Come visto nei capitoli precedenti, le e-mail sono ancora uno dei principali vettori di attacco preferiti tanto quanto lo è la messaggistica istantanea, ma gli aggressori si stanno rapidamente muovendo per utilizzare esche di phishing, quindi scommettiamo che nel prossimo futuro i kit di phishing giocheranno un ruolo interessante nelle minacce a venire.

Ma il 2020 e l'inizio del 2021 sono anche un anno straordinario perché abbiamo assistito all'abbattimento di Emotet. Una delle più grandi operazioni informatiche di sempre, che ha coinvolto settore pubblico e privato, forze di polizia internazionali e aziende private internazionali. Abbiamo visto tutti questi gruppi lavorare insieme per rendere lo spazio digitale un posto migliore in cui stare. Operazioni gigantesche molto ben sincronizzate hanno distrutto i sistemi di comando e controllo Emotet e disattivato gli impianti viventi distribuendo un Emotet payload autodistruttivo su ogni dispositivo infetto.

Purtroppo, se da un lato abbiamo avuto questo grande successo, abbiamo anche vissuto uno dei più importanti attacchi alla supply-chain della storia. SolarWinds è stato un impressionante attacco informatico eseguito da gruppi sofisticati che ha colpito centinaia di migliaia di aziende in tutto il mondo. Questo attacco ha evidenziato un argomento noto sugli attacchi alla catena di approvvigionamento e ha avvertito l'intera comunità informatica che i fornitori dell'azienda sarebbero stati la prossima cosa a cui prestare attenzione.

Al giorno d'oggi come mai prima d'ora ogni azienda ha bisogno di rinforzare le proprie protezioni informatiche poiché il suo successo aziendale passa attraverso il suo spazio digitale che è costantemente minacciato dagli attacchi informatici.
Le aziende come Yoroi devono diventare più attrattive per le piccole e medie imprese aiutandole ad avere successo nella loro attività proteggendo le loro risorse digitali come mai prima d'ora. Siamo qui per aumentare la sicurezza informatica dell'era digitale.



Yoroi S.r.l.
www.yoroi.company - info@yoroi.company
Piazza Sallustio, 9
00187 – Roma (RM)
+39 (051) 0301005