Comunicato Stampa 10/03/2022

RAPPORTO YOROI

Yoroi Società del Gruppo Tinexta rilascia il Rapporto 2022 sullo stato delle minacce cibernetiche affrontate dal nostro paese

Roma, 10 marzo 2022 – Yoroi **(Tinexta Group)** Presenta il **Rapporto annuale 2022** che fotografa lo stato delle minacce cibernetiche affrontate dal nostro paese nell'anno precedente e individua le tendenze che a livello globale si riflettono sull'Italia.

Il rapporto evidenzia come le tecniche e procedure usate dai criminali informatici sono simili a quelle osservate negli anni precedenti: **phishing**, malware **zero day**, **attacchi alla supply chain.** Tecniche e strumenti perfezionati dagli aggressori per sfruttare meglio la debolezza del fattore umano con tecniche di ingegneria sociale e indurre le vittime a commettere errori basati sulla fretta, l'urgenza, e la distrazione.

Il volume del codice malevolo intercettato dalla **tecnologia Yoroi-Tinexta** secondo il rapporto è in costante crescita rispetto agli anni precedenti e le modalità operative degli attaccanti suggeriscono una netta suddivisione tra attacchi di tipo opportunistico e attacchi mirati.

Nel 2021 le maggiori problematiche di sicurezza informatica sono però state il fenomeno della **Double Extortion** e quello degli attacchi alla **supply chain**. Ci si attende che accada lo stesso nel corso del 2022.

La telemetria offerta dalla piattaforma Yoroi ha inoltre permesso di estrarre una serie di statistiche riguardo agli attacchi di tipo "**zero-day Malware**", ovvero Malware non noti alle firme dei sistemi antivirus che rappresentano il 76% delle minacce Malware attuali.

Il **phishing** e lo **spear phishing** sono i vettori più adottati nel 2021 come inizio di una catena di attacco. A differenza dell'anno precedente, è stato osservato un aumento repentino del "drop and execute" con la conseguente adozione di attività di "Download" di componenti malevoli.

Attacco e difesa nel contesto italiano

Proprio come evidenziato l'anno scorso, la maggioranza di **malware** presenti nelle organizzazioni osservate sono stati Trojan Bancari. Il **principale vettore** di ingresso è rappresentato da ***Ursnif*** con una presenza del 33.5% sul totale e quella di *Emotet* per il 18.9% dei campioni. Tali trojan sono vettori di ingresso ampiamente utilizzati per installare impianti malevoli di varia natura.

In Italia durante l'anno appena trascorso il **phishing**, con il 41.88% degli attacchi bloccati, è stata la minaccia numero uno da affrontare. Il secondo gruppo per volumi di richieste bloccate è rappresentato dai **malware** con una prevalenza pari al 38.08%; in questa categoria consideriamo tutte le famiglie di codice malevolo, a partire dai Trojan, arrivando ai **ransomware**, e agli **info-stealer**. La terza macro-famiglia di minacce bloccate sono stati i **siti web dannosi** con il 19.95%. In questo caso abbiamo soprattutto due possibili situazioni da considerare: gli attacchi di "Watering hole" e quelli prettamente opportunistici, quali **adware**, malvertising, **click fraud** e altri.

Il territorio d'origine di **Botnet e Attacchi Opportunistici** ripete una distribuzione tipica: al primo posto ci sono **Stati Uniti** con il 38% della quota (con aumento del 34% rispetto all'anno 2020; al secondo posto ci sono i tentativi provenienti dalla **Cina** (CN), costanti rispetto all'anno scorso al 24%; il terzo posto è

conservato dalle **infrastrutture russe**, che dalla nostra telemetria contengono l'8% delle comunicazioni malevole.

La minaccia dalle Email: anche nel 2021 i cybercriminali continuano a preferire le email e la messaggistica come vettore di diffusione del malware: per il quinto anno di fila, le **mail malevole** rappresentano una parte rilevante dei cyber-attacchi. La strategia più utilizzate dagli attaccanti per sfruttare il vettore email sono le campagne di spam malevolo denominate "malspam". Esse sono configurate per **colpire singoli individui e piccole organizzazioni**, ad esempio tramite mail di **finte fatture** con documenti Office malevoli.

Esaminando la **telemetria** raccolta dall'infrastruttura di monitoraggio del **Cyber Security Defence Center**, possiamo confermare che i documenti di **Microsoft Office** sono il vettore di consegna del malware più rilevante, rappresentando il **modo più comune** per diffondere il primo stadio della catena di **infezione** del malware. Infatti, i documenti Microsoft Word (35%) e i fogli di calcolo Excel (33,2%) rappresentano congiuntamente il 68,2% di tutti gli allegati maligni intercettati dai servizi Yoroi di email Protection.

Infatti, una delle ultime tattiche adottate dai cyber criminali è quella di comprimere gli allegati all'interno di un file di archivio (zip, gzip o rar, 7zip) e crittografarli con una password menzionata all'interno del corpo della mail. È un metodo abbastanza semplice, ma rimane una tattica molto efficace e su cui gli avversari fanno sempre più riferimento.

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

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

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

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.

I dati utilizzati in questo rapporto, riguardano incidenti realmente accaduti.

La concretezza di questi dati fornisce quindi un importante spunto di riflessione e un'opportunità di miglioramento per i prossimi anni per quanto riguarda sia la formazione del personale in materia di security awareness che l'impiego di team specializzati come il nostro Defence Center per approntare le difese necessarie.

della cybersecurity in Italia) e vocazione all'innovazione tecnologica, conta più di 40 cyber analisti qualificati, più di 50 sviluppatori e 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.
Dal 2020, Yoroi è parte di **TinextaCyber** (**Tinexta Group**).

Tinexta Cyber SpA

Tinexta Cyber, **Tinexta Group**, è il polo italiano della cybersecurity con forti competenze verticali e soluzioni custom proprietarie per la mitigazione e la governance dei rischi legati alla sicurezza digitale. Con servizi basati in Italia e nel rispetto della compliance EU in ambito di data residency, data protection e GDPR, la società assiste i clienti con attività specializzate di assessment e advisory e si occupa del design, development ed integration delle soluzioni, curandone anche il monitoring e management.
L'azienda agisce, oltre che tramite Yoroi, anche con e attraverso le società controllate Corvallis e Swascan. In particolare, Corvallis ha una lunga esperienza come fornitore di soluzioni ad alto valore e su misura per i grandi progetti di aziende finanziarie e non solo; Swascan, innovativa startup italiana nonché ideatrice e titolare della piattaforma Cloud Security Testing, è un punto di riferimento per le PMI in tema di sicurezza informatica e di compliance normativa. Con 900 dipendenti, Tinexta Cyber opera dalla sede di Roma e da 22 uffici in Italia.

Per maggiori informazioni:

Yoroi
Media Advisor Arturo Di Corinto +393356785259 **@yoroisecurity** **www.linkedin.com/company/yoroi/** **https://www.yoroi.company** **https://blog.yoroi.company/** **https://yomi.yoroi.company**
Tinexta Cyber
Media Advisor BMP Comunicazione per Tinexta Cyber team.tinextacyber@bmpcomunicazione.it Pietro Barrile +393207008732 - Michela Mantegazza +393281225838 – Francesco Petrella +393452731667 https://tinextacyber.com/