COMUNICATO STAMPA

BOOM ATTACCHI INFORMATICI 0-DAYS: 6 SU 10 BLOCCANO AZIENDE PIÙ A LUNGO

*Il Cybersecurity Annual Report 2024 di Yoroi (Gruppo Tinexta) registra nel 2023 un numero in continua crescita di attacchi “0-days” che sfruttano una vulnerabilità o errore di progettazione del software e non danno nessun tempo certo per risolvere il problema. Secondo la ricerca anche la PEC è sotto attacco e il conflitto russo-ucraino ha riacceso l’attivismo informatico degli hacker.*

Il 58% degli attacchi informatici (malware) andati a buon fine nel 2023 è riconducibile ai cosidetti attacchi “0-day” che sfruttano una vulnerabilità o un errore di progettazione in un software, per cui **non esiste ancora una difesa nota e un tempo certo per la risoluzione del problema**. A rilevare l’incremento di questo fenomeno preoccupante è Il “Cybersecurity Annual Report 2024” di Yoroi (Gruppo Tinexta), unico membro italiano della Cyber Threat Alliance (CTA), organizzazione internazionale di cyber security.

“*Questo dato* - commenta **Fabrizio Vacca, Chief Operating Officer di Tinexta Cyber** - *suggerisce che i criminali informatici puntano sull'efficacia dell'elemento sorpresa e sull'uso di nuovi strumenti per superare le difese e portare a termine con successo le loro operazioni dannose*. *Il fenomeno preoccupante e in aumento degli attacchi "0-day" richiede un'attenzione e un impegno continuo nell'adozione di strategie di difesa all'avanguardia e tempestive.* *Nel 2024 ci aspettiamo un aumento degli attacchi informatici mirati a software, hardware e servizi utilizzati dalle aziende per proteggersi. Gli attacchi arriveranno anche dagli hacker meno esperti con la crescita del Ransomware-as-a-service (RaaS), un modello di business con cui le bande esperte vendono il proprio codice ransomware ad altri hacker che lo utilizzano, alimentando sempre di più il mercato del crimine informatico. Di conseguenza le aziende aumenteranno gli investimenti in tecnologie e soluzioni per proteggersi, in accordo con la direttiva europea NIS2, volta a rafforzare il livello generale di cybersicurezza nell'UE. L’Intelligenza Artificiale, poi – conclude* **Fabrizio Vacca** *– giocherà un ruolo fondamentale per automatizzare la risposta agli incidenti informatici e per migliorare la capacità di identificare e prevenire le minacce. Il nostro motto “Defence belongs to humans” colloca sempre la difesa informatica al centro delle responsabilità umane, utilizzando anche l’AI come arma di difesa per tutelare le nostre istituzioni, imprese e i cittadini”.*

**Il 21% dei malware individuati presenta un intervallo di rilevamento tra zero e quindici giorni**, sottolineando l'importanza cruciale di adottare approcci di difesa anticipatoria. Le principali minacce alla sicurezza informatica sono gli attacchi di tipo **Infostealer (26%)** che operano come “ladri digitali” rubando informazioni come nome utente, password e altri dati personali; seguiti dai **Trojan (20%)** virus nascosti che, una volta installati su un computer, permettono agli hacker di prendere il controllo del sistema e di accedere ai dati dell'utente senza che questi se ne accorga.

Il mezzo di diffusione dei malware preferito dai cyber criminali è quello delle e-mail, e i formati dei file allegati giocano un ruolo cruciale nel raggiungere le vittime. Il Rapporto di Yoroi rivela che **il formato più utilizzato è il PDF**, costituendo il **23%** degli allegati infettati. Gli aggressori lo sfruttano per indurre gli utenti ad aprire il malware attraverso link presenti nei documenti PDF, richiedendo una loro **partecipazione attiva**. Seguono i file compressi, soprattutto **ZIP (22%)**, che essendo cifrati con password vengono riconosciuti come sicuri ed eludono i controlli di sicurezza. Gli **oggetti dell’e-mail** infette o ingannevoli più comuni includono i termini “*rimessa c/assegni e fatture*” (21%), “*ricevute e solleciti di pagamento*” (14%), e “*ordini e transazioni*” (5%). Tutte le comunicazioni hanno un carattere economico e di urgenza finalizzato a ingannare gli utenti e diffondere malware.

Anche **le PEC sono sotto attacco**. Yoroi ha rilevato un aumento di attacchi informatici tramite Posta Elettronica Certificata (PEC), un canale di comunicazione vitale per enti pubblici, aziende e cittadini, che garantisce una validità legale equiparabile a quella di una raccomandata con ricevuta di ritorno. Nonostante i suoi protocolli di sicurezza, la PEC è vulnerabile agli attacchi informatici. **Dal monitoraggio di Yoroi su** **oltre 50 milioni di e-mail PEC nel 2023** è stato rilevato che gli attaccanti, attraverso il **phishing**, cercano di ottenere informazioni sensibili fingendosi entità affidabili: questi attacchi utilizzano e-mail PEC ingannevoli e pagine web graficamente simili a quelle legittime, rappresentando una minaccia significativa per la sicurezza informatica degli utenti che sono così portati a rivelare dati critici o a interagire con link dannosi.

**La guerra è anche cyber.** L'hacktivismo, cioè l’attivismo informatico degli hacker, con il Covid è emerso come una forza dinamica e globale, alimenatata dall’impiego di strumenti e tecniche per promuovere cause sociali o politiche, sia a sostegno che in opposizione di autorità e istituzioni. Yoroi sta monitorando il fenomeno da 4 anni rilevando che **il conflitto Russo-Ucraino ha dato un’accelerazione**, mettendo in luce la centralità delle telecomunicazioni e il **potenziale impatto delle azioni hacktiviste sulla sicurezza informatica e geopolitica globale.** Yoroi ha rilevato i gruppi di **hacktivisti nati per sostenere attivamente le politiche della Russia** e dei suoi alleati: ad esempio, Killnet, Noname057(16), From Russia With Love, Anonymous Sudan e Turk Hack Team.

Un altro fenomeno di interesse globale è la formazione delle **"Five Families", un'inedita alleanza di gruppi anarchici nel panorama hacker contemporaneo**. Questo nuovo raggruppamento, composto da BlackForums, Threatsec, GhostSec, Stormous e Sieged, si propone di promuovere l'unità e la collaborazione all'interno della comunità underground di Internet. La loro missione è quella di facilitare la crescita e lo sviluppo delle operazioni hacker, ponendo particolare enfasi sulla condivisione di conoscenze e risorse.

Il Cybersecurity Annual Report di Yoroi 2024 è disponibile sul sito di Yoroi al seguente link: [yoroi.company](https://yoroi.company/)

Yoroi S.r.l.

Yoroi (Tinexta Group) è un’azienda che gestisce Sistemi Integrati Adattivi e Dinamici di Difesa Cibernetica e sviluppata tecnologie proprietarie che hanno ottenuto significativi riconoscimenti anche sul mercato internazionale. Coniugando esperienza 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 Tinexta Cyber (Tinexta Group), 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.

L’azienda agisce con e attraverso le società controllate Corvallis, Swascan, oltre che Yoroi. Con 900 dipendenti complessivi, Tinexta Cyber opera dalla sede di Roma e da 22 uffici in Italia.

**Marketing & Communication**

Francesca Gargaro: [francesca.gargaro@consultant.yoroi.company](mailto:francesca.gargaro@consultant.yoroi.company) - 3482360242

Tinexta Cyber SpA

Tinexta Cyber (Tinexta Group) è il polo italiano della sicurezza informatica, dotato di solide competenze verticali e soluzioni personalizzate proprietarie per la mitigazione e la governance dei rischi legati alla sicurezza digitale. Con servizi con sede in Italia e in conformità con le normative UE sulla residenza dei dati, la protezione dei dati e il GDPR, l'azienda assiste i clienti con attività specializzate di valutazione e consulenza. Essa sovraintende la progettazione, lo sviluppo e l'integrazione delle soluzioni, occupandosi anche del loro monitoraggio e gestione. L'azienda opera tramite le sue controllate Corvallis, Swascan e Yoroi. In particolare, Corvallis vanta una vasta esperienza come fornitore di soluzioni su misura e ad alto valore per progetti di grandi dimensioni, senza limitarsi al settore finanziario. Swascan, un centro di eccellenza nella sicurezza informatica nel panorama italiano, è un punto di riferimento affidabile per la sicurezza informatica, la gestione degli incidenti e la conformità normativa, in particolare per le PMI. Yoroi fornisce sistemi integrati di difesa cibernetica adattabili e dinamici per coloro che cercano di prevenire i rischi o di ridurre i danni potenziali derivanti da attacchi informatici. Attraverso il Cyber Hub, queste tre aziende garantiscono la sicurezza dei clienti con soluzioni per la mitigazione e la governance dei rischi derivanti dagli attacchi informatici, contribuendo a rendere le aziende sempre più competitive. Visita tinextacyber.com.

|  |  |  |
| --- | --- | --- |
| **Communication**  Laura Artesio laura.artesio@tinextacyber.com | **Media Advisor**  SEC Newgate Italia  Irene Fusani  Tel. + 39 340 1280512 [irene.fusani@secnewgate.it](mailto:irene.fusani@secnewgate.it)  Martina Basile  Tel. +39 338 9034914  [martina.basile@secnewgate.it](mailto:martina.basile@secnewgate.it) |  |

TINEXTA SpA

Tinexta è un Gruppo industriale che offre soluzioni innovative per la trasformazione digitale e la crescita di imprese, professionisti e istituzioni. Quotata all’Euronext STAR Milan (MIC: MTAA) è inserita nell’indice europeo Tech Leader come azienda tech ad alto tasso di crescita. Basata in Italia e presente in 12 Paesi tra Europa e America Latina con oltre 2500 dipendenti, Tinexta è attiva nei settori strategici del Digital Trust, Cyber Security e Business Innovation. Al 31 dicembre 2022, il Gruppo ha riportato ricavi consolidati pari a € 357,2 milioni, EBITDA Adjusted pari a € 94,8 milioni e Utile netto pari a € 78,1 milioni.

[**tinexta.com**](http://www.tinexta.com/)|Stock ticker: TNXT, ISIN Code IT0005037210