Ransomware e finanza, i principali trend secondo l’Intelligence Finanziaria



Il FinCEN (Financial Crimes Enforcement Network) evidenzia un **forte aumento di attacchi ransomware** nei primi mesi del 2021, valutando in **590 milioni di dollari** l’importo dei pagamenti estorti tramite ransomware tra il 1 gennaio e il 30 giugno 2021. Il dato è preoccupante: in soli sei mesi è stato superato il valore totale guadagnato dagli autori degli attacchi nell’anno precedente, che ammontava a **416 milioni di dollari,** evidenziando così un **aumento dei pagamenti dei riscatti del 42%** rispetto al 2020**,** il trend sembra mantiene una crescita esponenziale. Gli analisti avvertono che di questo passo si arriverà nel prossimo anno ad un numero di attacchi ransomware pari alla somma di tutti quelli avvenuti nei 10 anni precedenti.

Il Financial Crimes Enforcement Network è l’ufficio governativo per la lotta contro i reati finanziari amministrato dal Dipartimento del tesoro degli Stati Uniti d’America. Si occupa quindi di riciclaggio di denaro, traccia le persone che operano in maniera sospetta, monitora transazioni elettroniche complesse tramite ricerche e divulgazioni su beni ed attività, e riferisce al Sottosegretario al Tesoro per il Terrorismo e l’Intelligence Finanziaria.

L’analisi si basa sulle segnalazioni di attività sospette (Suspicious Activity Reports, SAR) presentate dalle istituzioni finanziarie al FinCEN, un totale di **635 report e 458 transazioni confermate,** che forniscono un’utile panoramica sulla crescente minaccia provocata da questo tipo di malware. Nel 2021 gli Stati Uniti sono stati i più colpiti, con

34.816.097 attacchi, seguiti da Giappone, Australia e Italia (6.097.979) che si posiziona così al quarto posto annoverando tra i settori più colpiti la Sanità, la Pubblica Amministrazione, il Manufacturing, il Tech e il Banking.

I trend del cyber crime individuati dall'Intelligence Finanziaria

Lo scopo dei ricercatori era quello di individuare le tendenze di comportamento degli autori degli attacchi ransomware, per comprendere meglio come individuarli e come difendersi.

Gli esperti di FinCEN hanno identificato, all'interno del periodo di riferimento, **68 cosiddette "varianti"**, ovvero **versioni del ransomware appartenenti a differenti autori**. Di queste 68 varianti hanno analizzato le 10 più comuni per ottenere i trend nei pagamenti dei riscatti.

Il report conferma la predilezione degli hacker verso l'**utilizzo di criptovalute**, soprattutto **Bitcoin**, con un incremento nell'utilizzo di **Monero**, criptovaluta anonima.

In media, i riscatti si aggirano sui 100mila dollari, ma le cifre variano significativamente, con una maggioranza che si attesta comunque **sotto i 250mila**.

Il canale di comunicazione preferenziale per contattare le vittime rimane **The Onion Router (TOR)**, software che permette l'anonimato sul web, oppure email criptate o meno.

I trucchi degli hacker per riciclare gli introiti e aggirare la legge

Gli analisti di FinCEN hanno poi individuato 6 modalità relative alle 10 varianti analizzate con cui gli hacker riciclano gli introiti derivanti da attacchi ransomware.

Nello specifico:

- Pagamenti in **criptovalute anonime (AEC)**
- **Evitare di usare più volte gli stessi indirizzi Wallet**.
- Utilizzo di **exchange centralizzati di criptovalute convertibili (CVC) per i prelievi**
- Ricorso alla pratica del "**chain hopping**" per nascondere le proprie tracce sulle blockchain, convertendo CVC in diverse CVC prima di trasferire i fondi su un'altra
- Aumento nell'uso di **servizi di mixing**, quindi siti o software creati per nascondere l'identità del proprietario delle CVC.
- Preferenza di **exchange decentralizzati** o altre applicazioni legate alla finanza decentralizzata per convertire i proventi illeciti

Consigli e indicazioni su come proteggersi dai ransomware

Gli analisti raccomandano innanzitutto di utilizzare **indicatori di compromissione (IOC) e sistemi di allarme** che possano fermare o almeno individuare e segnalare eventuali attività malevole. Si invita inoltre a **contattare tempestivamente le forze dell'ordine**.

È comunque importante considerare che la crescita delle minacce legate ai ransomware è dovuta anche all'**aumento delle segnalazioni alle autorità**, quindi ad una maggiore attenzione, capacità e volontà da parte delle vittime di rendere noti questo tipo di cyber attacchi.

I ransomware restano attualmente una delle minacce più pericolose per i settori pubblici e privati, ed è sempre bene che le aziende adottino **programmi di cyber security** sia per evitare di incorrere in **sanzioni**, sia per ridurre drasticamente la possibilità di essere vittima dei cyber attacchi.

A cura della Redazione

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/ransomware-e-finanza-i-principali-trend-secondo-lintelligence-finanziaria/