Attch #31 AUSTRAC - Cyberscoop - Ransomware hackers launder bitcoin - 210126

Ransomware hackers launder bitcoin through just a handful of locations, researchers find

(Getty Images)
Written by Jeff Stone
JAN 26, 2021 | CYBERSCOOP

It's starting to look like the ransomware industry is developing its own version of the 1%, where a small number of players enjoy most of the wealth.

Cybercrime investigators have suggested the spiraling trend of increasingly large ransomware cash demands and attack frequency is not the work of a large number of criminals, but instead the result of a specialized black market economy in which hackers will different skill-sets collaborate on a breach, then split the proceeds. A relatively small number of attack groups actually seem to make up most of that black market economy, offering their malicious software on a rental basis and then taking a sizable chunk of the profits and relying on money laundering to cover their tracks.

Researchers now are tracking more of this activity via the blockchain, an accessible ledger through which public bitcoin transactions are recorded. When ransomware victims pay attackers to unlock their systems to decrypt their data, they typically use bitcoin, only for the transaction to be recorded on the blockchain. A new analysis of bitcoin deposit addresses tied to attack groups offers clues about hackers' financial relationships, and the way they move their stolen funds.

Chainalysis, a software company that monitors public cryptocurrency movements and provides tools to law enforcement agencies, tracked $348.6 million in bitcoin that traveled through known ransomware wallets, according to findings provided exclusively to CyberScoop. The trends Chainalysis identified could reap gains for investigators, the company said.

Upon extorting victims, ransomware attackers move the vast majority of their funds, some 82%, to cryptocurrency exchanges and mixers — services that blend cryptocurrency from various sources to hide its place of origin. Attackers invest other funds into specific bitcoin deposit addresses, which function like public bank accounts for virtual currency.

A closer inspection of this ecosystem suggests that just 199 deposit addresses received 80% of all funds sent by ransomware groups in 2020. Of the total 199, 25 accounts collected 46% of the funds. While the identity of the account-holders remains unclear, initial evidence suggests a small number of ransomware operators are doling out regular payments to frequent collaborators, or using the same deposit addresses to launder their funds.

"We're seeing the off-ramps of where this illicit money is going," said Kim Grauer, head of research at Chainalysis. "We can see an address belongs to an affiliate if an account is consistently receiving, say, 60% of a payment."

The Chainalysis findings come as the private sector and international law enforcement agencies are scrambling to keep pace with ransomware gangs. The payouts in attacks has increased by a reported 311% over the past year, with demands now regularly exceeding $10 million from large corporate targets.

Suspected hackers have mostly avoided apprehension, either because of their location outside U.S. jurisdiction or because the number of attacks have overwhelmed American investigators. If most big-time hackers are cashing their funds out of a small number of known bitcoin wallets, though, it could provide investigators with an opportunity to disincentivize the extortion efforts, Grauer said.

"If there's no way to cash out, then [victims] have the potential to recoup their funds," she said.

Researchers at the security firm TrendMicro and the threat intelligence company Intel471, which gathers data on suspected cybercriminals, previously have said a single ransomware attack may involve one group that specializes in malware development, and another in defeating anti-virus software and other niche professionals.

A malware developer, for instance, may leverage their reputation in the cybercriminal underground to contact an illicit data broker with access to hacker networks in a specific company. The partnership might then expand to include specialists capable of exploiting that network access to infect the organization, then a negotiation service that handles direct conversations with a breached company or its lawyers. Each entity takes a cut, driving up the efficiency of the hack and size of the demand.

U.S. investigators, for instance, say they caught accused ransomware operator Maksim Yakubets bragging to an associate that he works with "two teams who worked with his malware and botnets and that each team has their own spammers," according to an indictment.

The FBI's Internet Crime Complaint Center received 2,047 ransomware complaints from U.S. victims in 2019, the most recent bureau figures available, resulting in adjusted losses of roughly $8.9 million. With an apparent shortage of data, the FBI has turned to the insurance industry and security firms to gather more information about hacking groups, their tendencies, demands and perhaps glean insights that might lead to their apprehension.

https://www.cyberscoop.com/ransomware-hack-bitcoin-money-laundering-chainalysis/