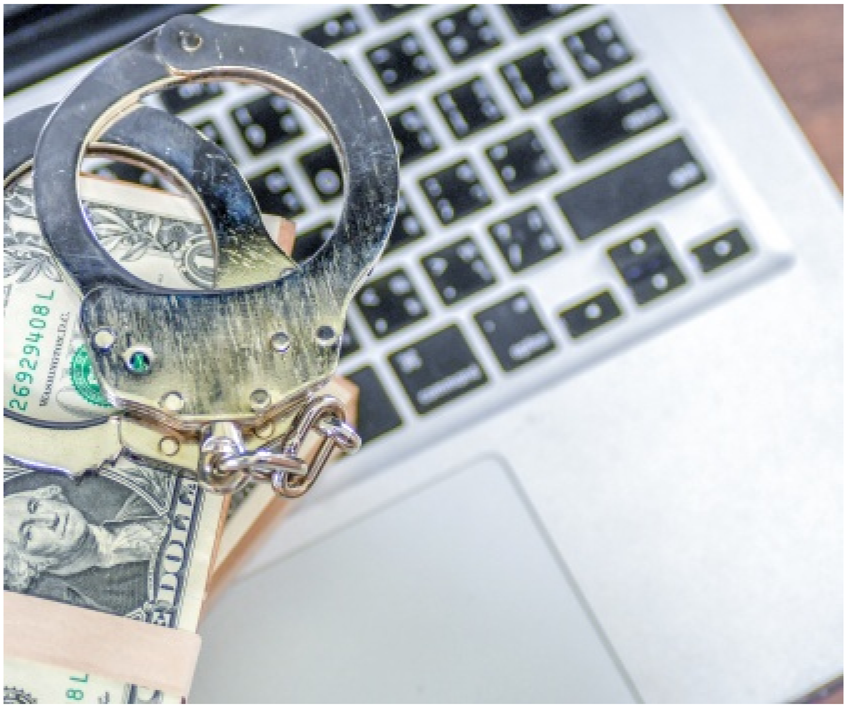
Lazarus: Three North Koreans Charged for Financially Motivated Attacks

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lazarus-north-korea-indictment



The U.S. government has charged three men in relation to a string of financially motivated cyber attacks linked to the North Korean Lazarus (aka Appleworm) group. The attackers stole approximately $1.3 billion from a range of financial institutions and cryptocurrency exchanges.

In a second case, a Canadian-American citizen has pleaded guilty to involvement in a money laundering scheme linked to heists organized by the Lazarus group.

The charges relate to a number of financially motivated attacks, including several investigated by Symantec, a division of Broadcom (NASDAQ: AVGO).

Banking attacks

Lazarus was linked to a 2016 attack that stole US$81 million from the Bangladesh Central Bank and a number of other attacks against banks in Asia and South America. The attacks prompted an alert by payments network SWIFT, after it was found that the attackers had used malware to cover up evidence of fraudulent transfers.

In order to steal such massive sums, the attackers deployed relatively sophisticated malware, most notably Trojan.Banswift, which was used to wipe evidence of fraudulent transactions. Banswift shared code with an older Lazarus tool called Backdoor.Contopee. Contopee, along with two other pieces of Lazarus malware, Backdoor.Fimlis and Backdoor.Fimlis.B, were already being used in limited targeted attacks against the financial sector in South-East Asia.

Financially motivated attacks continued into 2017, when dozens of organizations were targeted through watering-hole attacks involving a previously unseen piece of malware. The attackers compromised websites likely to be visited by staff at targeted organizations and used a custom exploit kit to deliver malware to selected targets. The exploit kit was configured to only infect visitors from approximately 150 different IP addresses. These IP addresses belonged to 104 different organizations located in 31 different countries, most of which were banks. While the malware used in these attacks (Downloader.Ratankba) had been previously unseen, further analysis by Symantec uncovered strong links between this tool and known Lazarus tools.

WannaCry

Lazarus was subsequently implicated in the WannaCry ransomware attacks. The ransomware incorporated the leaked EternalBlue exploit that used two known vulnerabilities in Windows (CVE-2017-0144 and CVE-2017-0145) to turn the ransomware into a worm, capable of spreading itself to any unpatched computers on the victim's network and also to other vulnerable computers connected to the internet.

Within a matter of hours, the malware had infected hundreds of thousands of computers worldwide. The attack had the potential to be highly profitable but it was poorly executed. WannaCry was supposed to generate a unique Bitcoin wallet address for each infected computer but, due to a bug, it failed to do so and instead defaulted to three hardcoded Bitcoin addresses for payment. This meant the attackers had no way of knowing which victims had paid using the hardcoded addresses. The attackers also included a "killswitch" in the malware. This was the address of a non-existent domain. WannaCry was designed to check if the domain was live and, if it was, it would cease installing. However, it was quickly found by a security researcher who registered the domain themselves, thus limiting the damage.

FASTCash ATM attacks

The group's interest in financially motivated attacks persisted and, in 2018, evidence appeared of its involvement in attacks on ATM networks in Africa and Asia. The operation, known as FASTCash, allowed the group to effectively empty ATMs of cash. The attacks began with breaches of the targeted bank's network in order to gain access to the switch application server that handled ATM transactions. Malware (Trojan.Fastcash) was installed on the server and used to intercept fraudulent cash withdrawal requests and send falsified approval responses, allowing cash to be withdrawn.

Cryptocurrency attacks

In a related announcement, the FBI, the Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Treasury released details on AppleJeus, malware that was used in a series of attacks on cryptocurrency exchanges. The malware is designed to masquerade as legitimate cryptocurrency trading applications.

At least seven different versions of AppleJeus have been discovered, each of which is designed to target a different cryptocurrency trading application. The following trading platforms were targeted by the malware:

- Celas Trade Pro
- JMT Trading
- Union Crypto
- Kupay Wallet
- CoinGoTrade
- Dorusio
- Ants2Whale

Initially the malware was spread using fake versions of the legitimate trading platform websites. However, later the attackers switched vectors, relying on phishing, social networking, and social engineering techniques to fool victims into downloading the malware.

Far-reaching investigations

The indictment is the latest in a series of charges laid out against state-sponsored espionage actors by authorities in the U.S. and comes on the back of a 2018 indictment against one of the men named in this week’s announcement. The charges are a timely reminder of the ability of law enforcement to investigate attacks that originate far beyond national borders.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise