LA-SAFE CYBER DIGEST

September 28, 2018

MALWARE | SOCIAL ENGINEERING | CYBERCRIME

Cryptojacking Apps on Google Play Market – **Sophos – 09.24.2018**

Even though the prices of cryptocurrencies have tanked considerably in the past few months, malware authors are still upbeat about the idea of leveraging victims' devices for mining. SophosLabs recently discovered 25 apps on Google Play that disguise themselves as games, utilities and educational apps, but under the hood they turn victim's mobile device into cryptocurrency churning rigs. These apps had been downloaded and installed more than 120,000 times.

Analyst Note:

Cryptojacking apps are a recurring threat in the Google play store. Cryptojacking, harnessing unsuspecting users GPUs or CPUs to mine cryptocurrency, may be less disruptive than a ransomware attack but are still a threat. Cryptojacking causes increased wear and energy consumption on the target device but also could cause unexpected instability in a system due to overstressed systems. The hijacking of resources could also result in a Denial of Service event for the victim's machines or network. Law enforcement and organizations handling sensitive data should be wary of downloading apps on official or personal devices, even those with apparent business or productivity purposes.

CRITICAL INFRASTRUCTURE

DDoS attack on Energy Company – **Deutsche Welle – 09.26.2018**

German company RWE filed a police complaint against unknown attackers who had targeted RWE's public website, a company representative said. The firm's webpage was flooded with distributed denial-of-service (DDoS) attacks and remained virtually inaccessible by Tuesday morning. RWE currently faces harsh criticism from environmental groups over its plans to expand coal mining operations by clearing the ancient Hambach Forest. The mass-circulation daily Bild linked the attack with a Youtube video using the symbols of the hacker group Anonymous. "We will attack your servers and bring down your web pages, causing you economic damage that you will never recover from," says the computer-generated voice in the video. "Together, we will bring RWE to its knees," it adds, calling the viewers to boycott the company.

Analyst Note:

While the Hambach protests and RWE are based in Germany, there have been several high profile clashes between environmentalist and energy companies in the United States. Companies participating in the Dakota Access Pipeline and the Bayou Bridge Pipeline are possible targets of similar DDoS attacks. The DDoS attack on RWE is loosely credited to hacker collective Anonymous after a video surfaced on YouTube using Anonymous' symbols to claim credit for the attack.

While the veracity of these claims are unknown, and largely unverifiable, the use of Anonymous' branding may be an attempt to invoke a sense of larger collective action around the Hambach protests. Anonymous has gained notoriety in the last decade for claiming credit for cyberattacks against a diverse target set, ranging from the Church of Scientology and Westboro Baptist Church, to ISIS and Paypal. Because of its loosely defined membership and anonymous nature, it is also likely that the Anonymous brand is appropriated by criminal organizations and nation state attackers to hide attribution for various actions.

Cyber Attack on Port of San Diego – **San Diego Tribune – 09/27/2018**

The Port of San Diego said Wednesday it is investigating a highly sophisticated cybersecurity threat to its technology systems that is currently affecting the public agency's ability to process park permits and records

requests, and perform other business services. The digital assault is similar, in some ways, to a ransomware attack that was launched against the city of Atlanta in March, security analysts say. The San Diego Harbor Police Department, the law enforcement arm of the Port, is also affected by the attack and is said to be using alternative technology systems

Analyst Note:

The Port of San Diego is an important naval port for shipbuilding, U.S. Navy surface vessels, and submarines. Its significance as a commercial port is dwarfed by the Los Angeles and Long Beach ports 90 miles north. These two ports are vital to global shipping and the staging point of supply lines that effect the entire United States. These supply lines are facilitated by automated logistics platforms that coordinate between multiple fulfillment vendors to create a highly efficient and complex supply chain which facilities Just in Time logistics

Just in Time logistics reduce waste and deliver materials only when needed by forecasting demands and logistic schedules. While efficient, Just in Time logistics are susceptible to disruptions of any link in the supply chain, making ports of particular importance to Just in Time logistics. Port Security officers can prepare for ransomware attacks by implementing redundant storage and cloud systems along with disaster planning exercises to simulate transitioning to backup systems.

DARK WEB

Onion Identity Services – ik3dw5whel25******.onion– 09/27/2018 *(Full .onion URL available by request)***

All passports we sell are directly from the issuing authority, they are 100% originals, just with your photo. ID Cards and Drivers Licenses are professional replicas, but still with all security features (Microprint, UV, Holo). The ID information we use is real data from real persons, so they will be in the country's database. You can use them in any country, but try to avoid to use it in the issuing country, since another person is already living there with that ID. You can open bank accounts, P.O.Boxes, recieve and send Westernunion payments, rent and drive cars and whatever else you can imagine! It takes approximately 14 days to make and ship the IDs and 21 days for passports.

Analyst Note:

This onion site sells what it claims are authentic passports and replica ID's with working security features. The passports sell for around 1700 USD and IDs for 500 USD. Like most services on the dark web, the authenticity of the passports and IDs are not verifiable but the price point makes the barrier to testing them relatively low. Physical security specialists should be aware of the accessibility of fake identification documents and employ mitigating measures such as biometric scanners or secondary identification sources.

ADVANCED PERSISTENT THREATS

Fancy Bear Uses LoJack Based Rootkit - **TechCrunch - 09.27.2018**

Security researchers say that they have found evidence that for the first time Russia-backed hackers are using rootkit malware to target its victims. The malware, dubbed LoJax, uses a portion of LoJack, an anti-theft software that connects to a malicious command and control server operated by the hackers. LoJax, like other rootkits, embeds in the computer's firmware and launches when the operating system boots up. Because it sits in a computer's flash memory, it takes time, effort and extreme care to reflash the memory with new firmware.

Analyst Note:

Rootkits are used to provide persistent privileged access to a computer and are difficult to detect and remove. Rootkit detection is difficult to automate and usually requires manual inspection of the system memory logs or System Call Table for patterns that indicate hidden patterns. Securing analysts attempting to detect root kits should consider using an alternative trusted computer or medium to boot the storage to avoid rootkit deception measures.