FROM THE SECURONIX THREAT RESEARCH LABS

SECURONIX SHIFT

VOL 1 - May 2017

What is Securonix SHIFT?

Securonix Highlights and Insights From the Trenches (**SHIFT**) is a commentary on cyber threat findings, recent cyber security incidents and autonomous learning from the Securonix Threat Research Lab and Data Sciences Teams.

LAB

LARGEST SWIFT SERVICE BUREAU IN THE MIDDLE EAST IS INFILTRATED BY THE NSA

The Shadow Brokers (TSB), a hacking group that previously released a massive set of hacking tools used by the NSA, has released a new archive that indicates the NSA sought to completely capture the SWIFT financial transaction transfer network.

- According to Shadowbroker's archive, multiple SWIFT boxes were compromised and implanted as part of this massive attack on SWIFT Service Bureau banks in the Middle East - allegedly by NSA.
- Some of the attack TTPs leveraged as part of this massive compromise include initial infiltration using zero-day exploits against the VPN/Cisco infrastructure, SMB/RPC exploits to move laterally, dsquery to compromise hard-coded credentials (1000+ employee credentials were compromised), querying Oracle DB to steal SWIFT data using multi-stage malicious implants for persistence.
- Securonix security analytics were able to ingest the relevant data sources, and use algorithms to detect the infiltration methods. As with all sophisticated cyberattacks, simple rule-based detection tools like signature-based AV or rule-based SIEM can be easily bypassed. However, autonomous machine learning systems like Securonix are able to detect these behaviors/TTPs and surface hidden infiltrations.

Relevant data sources: Cisco ASA, VPN, ETDR (Cylance, CarbonBlack/Bit9, sysmon v6), IIS server, Windows AD/Workstation

LAB

LEGACY SIEM TOOLS AND BLUE TEAMS UNDER ATTACK

The SIEM solutions deployed by a large portion of organizations hoping for a better security posture are actually becoming the weakest security link for exploitation. A severe lack of expertise by the implementers and operators of SIEM tools makes them a prime target. According to John Grigg, a leading cyber security strategist with the Meta Group, "SIEMs are a one-stop shop for attackers. Nobody has these locked down. And once they gain a toehold on the SIEM box, an adversary has a map and keys to do what they want on the network."

- Some of the notable demonstrations showing the targeting of SIEM/blue team tools to accomplish cyberattack objectives include the B-Sides Boston presentation where researchers showed how Splunk can be attacked, as well as the INFILTRATE conference presentation from earlier this month showing more generic attacks against SIEM.

- Based on our discussions with the researchers who presented these findings, one of the most common security issues that makes these attacks possible is SIEM misconfigurations during deployment, so an important first step is to secure and properly configure any security management solution in order to mitigate these attacks.

- Specifically, some of the potential security issues we should be aware of during deployment include; default passwords, leaving SSL off, binding with other vendors over REST insecurely, not auditing the deployed systems or monitoring user and admin access as well as other activities, not hardening the security management infrastructure stack and application.

- Monitoring user access to any security technology and security management solution is also critical to ensure that the environment is appropriately hardened. In particular, the use of dynamic algorithms and machine learning techniques will yield the best results in minimizing risk.

Relevant Data Sources: Proxy, pcaps, SSL proxy

LAB

NEW USER SESSION HIJACKING ATTACK - WINDOWS FEATURE VS. VULNERABILITY

Session hijacking is a well-known technique that can be used to conduct insider attacks. This works by attacking a user who has authenticated to a system or application and is conducting transactions. The attack results in the malicious party taking over an existing user's session and then conducting malicious transactions through that user account. Such attacks are commonly seen in web applications, particularly financial services web portals, but are also seen in other scenarios. Here, a researcher showed how an attacker with a local admin account on a Windows machine could use native command line tools to hijack other Windows users' sessions.

- A security researcher showed that by running one native Windows command, attackers without credentials but with local admin privileges can now hijack user sessions (both active and inactive) locally and remotely; This has been tested on Windows 7, 10, 2008, and 2012.
- From a security professional's perspective, one of the key takeaways is that a feature can also be a security weakness, so baselining normal behavior associated with various legitimate features is critical.
- Another key takeaway is that this technique gives attackers an ability to perform lateral movement and account takeover much quicker than previously with potentially fewer artifacts left on the system for a forensic analyst to find later.
- Simple legacy rules-based detection will not detect such session hijacking, but Securonix security analytics is able to detect the unusual behaviors associated with the tscon-based session hijack provided the end-host log source data is available.

Relevant Data Sources: ETDR (cb/bit9, sysmon v6)

LAZARUS GROUP APTS LINKED TO BANGLADESHI FINANCIAL/SWIFT HEIST

At least part of the Lazarus Group – widely believed to be a North Korean sponsored nation-state hacking group – is now focused on stealing money through cyberattacks. Indications are that a portion of the group has splintered off with its own new set of Tactics, Techniques and Procedures (TTPs) to conduct cyberheists similar to the Bangladeshi SWIFT heist in 2016 which nearly $1 Billion.

- After the Sony attack in 2014 and the 951 million dollar SWIFT attack in Bangladesh in 2016, the Bluenoroff/Lazarus APT attacks continued in 2016 in 2017, most recently compromising banks in Europe and Poland.

- This threat actor has been using a multi-stage approach to compromise financial/SWIFT institutions, starting with spear-phishing/water-holing combined with web-based client-side Adobe Flash .swf exploits chaining command-and-control (C2) through multiple hosts including eye-watch.in & sap.misapor.ch C2 domains, followed by Escalation of Privileges (EP), deploying malicious implants e.g. Backdoor.Fimlis, Downloader. Ratankba, Backdoor.Joanap, Backdoor.Destover (used in Sony attacks as well wiping disk viz. using del /a %1).

- Some of the other interesting TTPs include migrating into running processes using multiple variants of malicious implants/stagers, bypassing security/AV product detections using a custom PE loader.

- Some specific, relevant behaviors associated with the activity of the malicious actor as part of lateral movement include unusual artifacts loaded by rundll32, anomalies associated with malicious implants dropped into C:\Users\%username%\Desktop\win32*, %systemroot%* e.g. msdtc.exe, C:\Windows or C:\MSO10, unusual 4672 w/full SeBackupPrivilege, SeLoadDriverPrivilege, SeDebugPrivilege, SeImpersonatePrivilege access), unusual scheduled task 4648 activity etc.

- Securonix data science and threat research teams have developed and deployed autonomous learning techniques that are able to detect these new TTPs with a very high degree of accuracy.

Relevant Data Sources: ETDR (Cylance, CarboinBlack/Bit9, sysmon v6), HTTP/S Proxy, Windows AD/Workstation.

LAB

For detailed exploration of these, or any other cyber security issues and how big data machine learning can help you defend against these, contact us at **info@securonix.com**.

SECURONIX
Security Analytics. Delivered.