SECURITY ADVISORY

January, 2024

Iran's Mint Sandstorm Campaign

Context

Mint Sandstorm, who share similarities with the threat actor monitored by other researchers under the names APT35 and Charming Kitten, is an Iranian state-sponsored APT group that primarily focuses on cyber-espionage activities, with a specific interest in targeting individuals and organizations associated with Microsoft's educational and research sectors. Their operations aim to steal sensitive intellectual property, research findings, and other valuable information.

Mint Sandstorm's primary targets are educators and researchers affiliated with Microsoft. The group is known for leveraging social engineering tactics, spear-phishing campaigns, and watering hole attacks to compromise the systems of their victims. The adversaries exploit vulnerabilities in software commonly used by educators and researchers, seeking to gain unauthorized access to sensitive information.

The threat actors utilized compromised legitimate email accounts to send phishing lures, employed the Client for URL (curl) command to establish connections with the Mint Sandstorm command-and-control (C2) server for downloading malicious files, and introduced a new custom backdoor named MediaPl. These sophisticated techniques enhance Mint Sandstorm's ability to evade detection and persistently compromise targeted systems.

Mitigation

Defending against the Mint Sandstorm involves more than simply patching vulnerabilities. It requires a comprehensive strategy that includes implementation of Multi-Factor Authentication (MFA) and protection of session cookies, including detection of suspicious use of valid credentials or session cookies. Additionally, organizations can minimize the risk of compromise by implementing the following controls:

Application Control Policies: Enforce stringent application control or whitelisting policies to prevent unauthorized system modifications, ensuring that only trusted and validated applications can access and alter critical system components.

Blocking Network Traffic: Implement proactive network traffic blocking measures, including the restriction of suspicious IPs, domains, and connections from high-risk Autonomous System Numbers, Top-Level Domains, and countries.

Technical Details

In a recent campaign, Mint Sandstorm proceeded with an email containing a link to a malicious domain. Follow-up messages guided targets to sites like cloud-document-edit[.]onrender[.]com, hosting a RAR archive (.rar) file claiming to contain the draft document for review. Upon opening, the .rar file decompressed into a double extension file (.pdf.lnk) with an identical name. When launched, the .pdf.lnk file executed a curl command, retrieving malicious files from Mint Sandstorm's controlled subdomains at glitch[.]me and supabase[.]co.

Several files, notably various .vbs scripts, were observed downloaded onto targets' devices during this campaign. Additionally, instances were observed where a renamed version of NirCmd, a legitimate command line tool facilitating actions on a device without displaying a user interface, was present on the target's device.

MediaPl, a tailored backdoor, exhibits the capability to send encrypted communications to its Command-and-Control (C2) server. Disguised as Windows Media Player, an application renowned for storing and playing audio and video files, MediaPl is strategically placed in C:\Users\[REDACTED]\AppData\Local\Microsoft\Media Player\MediaPl.dll by Mint Sandstorm.

When executed with the path of an image file as an argument, MediaPl.dll not only launches the image in the Windows Photo application but also parses the image for C2 information. All communications to and from MediaPl's C2 server are secured with AES CBC encryption and Base64 encoding. As of the latest update, MediaPl demonstrates the ability to terminate itself, pause and retry communications with its C2 server, and execute received commands using the _popen function.

In contrast to overt phishing tactics, the group's operations are acknowledged as the craftsmanship of a technically and operationally sophisticated subset within Mint Sandstorm. This specialized faction adeptly concentrates on infiltrating and extracting sensitive information from high-value targets, thereby accentuating a formidable risk to organizations. Of particular significance is their proclivity for orchestrating resource-intensive social engineering campaigns, strategically targeting noteworthy individuals like journalists, researchers, professors, or those endowed with insightful perspectives on security and policy matters of keen interest to Tehran. The nuanced prowess displayed in these endeavors amplifies the overarching jeopardy imposed on organizational security.

Tactics, Techniques and Procedures

The notable TTPs related to the Mint Sandstorm Campaign are:

T1073 - DLL Side-Loading:

Mint Sandstorm employs DLL Side-Loading in spear-phishing campaigns, exploiting vulnerabilities to execute malicious code and evade detection.

T1072 - Software Deployment Tools:

Mint Sandstorm utilizes software deployment tools in watering hole attacks, compromising trusted websites to deploy malware efficiently. Through the injection of malicious code into these websites, Mint Sandstorm delivers malware to visitors, exploiting vulnerabilities in browsers or plugins.

T1068 - Exploitation for Privilege Escalation:

Mint Sandstorm focuses on exploiting software vulnerabilities, particularly in Microsoft Office, for privilege escalation in targeted campaigns.

T1085 - Incorporating Rundll32 in Custom Malware for Persistence:

Mint Sandstorm incorporates Rundll32 in custom malware, ensuring persistent access to compromised systems through the execution of malicious code.

Cyber Threat Intelligence

Mint Sandstorm is an Iranian state-sponsored APT group that has been recently active. The group primarily focuses on cyber-espionage activities, with a specific interest in targeting individuals and organizations associated with Microsoft's educational and research sectors. Their operations aim to steal sensitive intellectual property, research findings, and other valuable information.

References

Related IOC’s & Yara Rules:

- https://otx.alienvault.com/pulse/643f7c31ec6660e495778454
- https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/

Public Intelligence:

- https://www.darkreading.com/vulnerabilities-threats/microsoft-iran-mint-sandstorm-apt-blasts-educators-researchers
- https://www.cybersecurity-review.com/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/
- https://irannewsupdate.com/news/news-digest/unveiling-the-sophistication-of-mint-sandstorm-irans-malign-cyber-operations/