New TTPs observed in Mint Sandstorm campaign targeting high-profile individuals at universities and research orgs

⋮ 1/17/2024

- By Microsoft Threat Intelligence

Since November 2023, Microsoft has observed a distinct subset of Mint Sandstorm (PHOSPHORUS) targeting high-profile individuals working on Middle Eastern affairs at universities and research organizations in Belgium, France, Gaza, Israel, the United Kingdom, and the United States. In this campaign, Mint Sandstorm used bespoke phishing lures in an attempt to socially engineer targets into downloading malicious files. In a handful of cases, Microsoft observed new post-intrusion tradecraft including the use of a new, custom backdoor called MediaPl.

Operators associated with this subgroup of Mint Sandstorm are patient and highly skilled social engineers whose tradecraft lacks many of the hallmarks that allow users to quickly identify phishing emails. In some instances of this campaign, this subgroup also used legitimate but compromised accounts to send phishing lures. Additionally, Mint Sandstorm continues to improve and modify the tooling used in targets' environments, activity that might help the group persist in a compromised environment and better evade detection.

Mint Sandstorm (which overlaps with the threat actor tracked by other researchers as APT35 and Charming Kitten) is a composite name used to describe several subgroups of activity with ties to the Islamic Revolutionary Guard Corps (IRGC), an intelligence arm of Iran's military. Microsoft attributes the activity detailed in this blog to a technically and operationally mature subgroup of Mint Sandstorm that specializes in gaining access to and stealing sensitive information from high-value targets. This group is known to conduct resource-intensive social

engineering campaigns that target journalists, researchers, professors, or other individuals with insights or perspective on security and policy issues of interest to Tehran.

These individuals, who work with or who have the potential to influence the intelligence and policy communities, are attractive targets for adversaries seeking to collect intelligence for the states that sponsor their activity, such as the Islamic Republic of Iran. Based on the identities of the targets observed in this campaign and the use of lures related to the Israel-Hamas war, it's possible this campaign is an attempt to gather perspectives on events related to the war from individuals across the ideological spectrum.

In this blog, we share our analysis of the new Mint Sandstorm tradecraft and provide detection, hunting, and protection information. Organizations can also use the mitigations included in this blog to harden their attack surfaces against the tradecraft observed in this and other Mint Sandstorm campaigns. These mitigations are high-value measures that are effective ways to defend organizations from multiple threats, including Mint Sandstorm, and are useful to any organization regardless of their threat model.

New Mint Sandstorm tradecraft

Microsoft observed new tactics, techniques, and procedures (TTPs) in this Mint Sandstorm campaign, notably the use of legitimate but compromised email accounts to send phishing lures, use of the Client for URL (curl) command to connect to Mint Sandstorm's command-and-control (C2) server and download malicious files, and delivery of a new custom backdoor, MediaPI.

Social engineering

In this campaign, Mint Sandstorm masqueraded as high-profile individuals including as a journalist at a reputable news outlet. In some cases, the threat actor used an email address spoofed to resemble a personal email account belonging to the journalist they sought to impersonate and sent benign emails to targets requesting their input on an article about the Israel-Hamas war. In other cases, Mint Sandstorm used legitimate but compromised email accounts belonging to the individuals they sought to impersonate. Initial email messages did not contain any malicious content.

This tradecraft, namely the impersonation of a known individual, the use of highly bespoke phishing lures, and the use of wholly benign messages in the initial stages of the campaign, is likely an attempt to build rapport with targets and establish a level of trust before attempting to deliver malicious content to targets. Additionally, it's likely that the use of legitimate but compromised email accounts, observed in a subset of this campaign, further bolstered Mint Sandstorm's credibility, and might have played a role in the success of this campaign.

Delivery

If targets agreed to review the article or document referenced in the initial email, Mint Sandstorm followed up with an email containing a link to a malicious domain. In this campaign, follow up messages directed targets to sites such as *cloud-document-edit[.]onrender[.]com,* a domain hosting a RAR archive (*.rar*) file that purported to contain the draft document targets were asked to review. If opened, this *.rar* file decompressed into a double extension file (*.pdf.lnk*) with the same name. When launched, the *.pdf.lnk* file ran a curl command to retrieve a series of malicious files from attacker-controlled subdomains of *glitch[.]me* and *supabase[.]co*.

Microsoft observed multiple files downloaded to targets' devices in this campaign, notably several *.vbs* scripts. In several instances, Microsoft observed a renamed version of NirCmd, a legitimate command line tool that allows a user to carry out a number of actions on a device without displaying a user interface, on a target's device.

Persistence

In some cases, the threat actor used a malicious file, *Persistence.vbs*, to persist in targets' environments. When run, *Persistence.vbs* added a file, typically named *a.vbs*, to the *CurrentVersion\Run* registry key. In other cases, Mint Sandstorm created a scheduled task to reach out to an attacker-controlled *supabase[.]co* domain and download a *.txt* file.

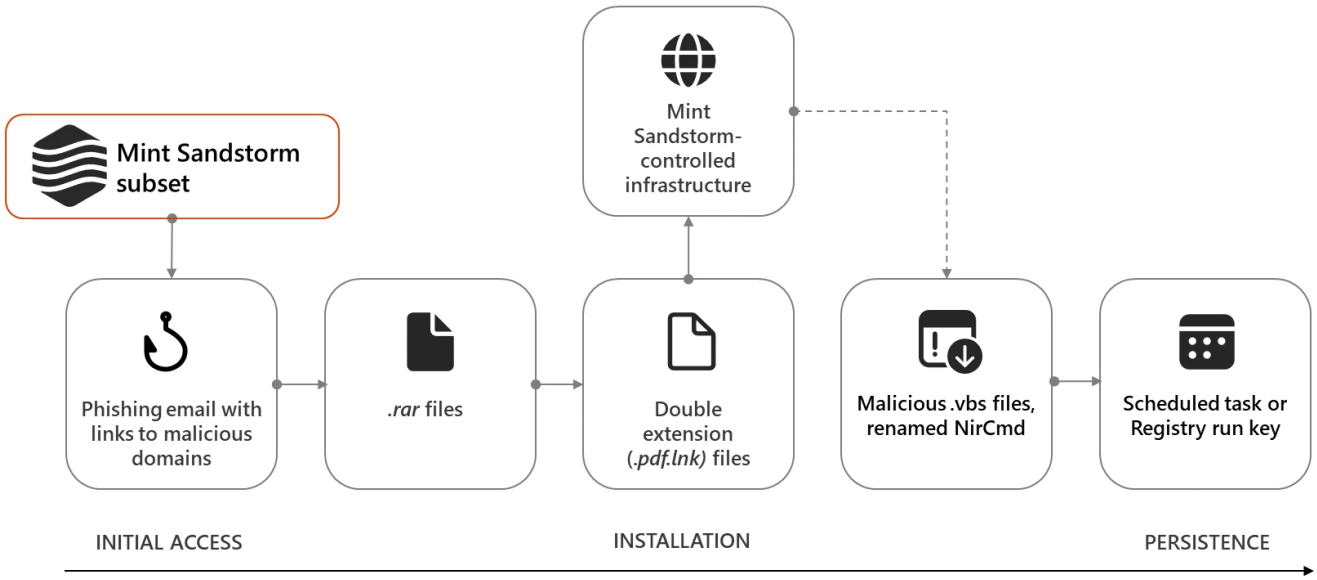

Figure 1. Intrusion chain leading to backdoors observed in the ongoing Mint Sandstorm campaign

Collection

Activity observed in this campaign suggests that Mint Sandstorm wrote activity from targets' devices to a series of text files, notably one named *documentLoger.txt.*

In addition to the activity detailed above, in some cases, Mint Sandstorm dropped MischiefTut or MediaPI, custom backdoors.

MediaPI backdoor

MediaPI is a custom backdoor capable of sending encrypted communications to its C2 server. MediaPI is configured to masquerade as Windows Media Player, an application used to store and play audio and video files. To this end, Mint Sandstorm typically drops this file in *C:\\Users\\[REDACTED] \\AppData\\Local\\Microsoft\\Media Player\\MediaPI.dll*. When MediaPI.dll is run with the path of an image file provided as an argument, it launches the image in Windows Photo application and also parses the image for C2 information. Communications to and from MediaPI's C2 server are AES CBC encrypted and Base64 encoded. As of this writing, MediaPI can terminate itself, can pause and retry communications with its C2 server, and launch command(s) it has received from the C2 using the _popen function.

MischiefTut

MischiefTut is a custom backdoor implemented in PowerShell with a set of basic capabilities. MischiefTut can run reconnaissance commands, write outputs to a text file and, ostensibly, send outputs back to adversary-controlled infrastructure. MischiefTut can also be used to download additional tools on a compromised system.

Implications

The ability to obtain and maintain remote access to a target's system can enable Mint Sandstorm to conduct a range of activities that can adversely impact the confidentiality of a system. Compromise of a targeted system can

also create legal and reputational risks for organizations affected by this campaign. In light of the patience, resources, and skills observed in campaigns attributed to this subgroup of Mint Sandstorm, Microsoft continues to update and augment our detection capabilities to help customers defend against this threat.

Recommendations

Microsoft recommends the following mitigations to reduce the impact of activity associated with recent Mint Sandstorm campaigns.

- Use the Attack Simulator in Microsoft Defender for Office 365 to organize realistic, yet safe, simulated phishing and password attack campaigns in your organization by training end-users against clicking URLs in unsolicited messages and disclosing their credentials. Training should include checking for poor spelling and grammar in phishing emails or the application's consent screen as well as spoofed app names, logos and domain URLs appearing to originate from legitimate applications or companies. Note that Attack Simulator testing only supports phishing emails containing links at this time.
- Encourage users to use Microsoft Edge and other web browsers that support SmartScreen, which identifies and blocks malicious websites, including phishing sites, scam sites, and sites that contain exploits and host malware. Turn on network protection to block connections to malicious domains and IP addresses.
- Turn on cloud-delivered protection in Microsoft Defender Antivirus or the equivalent for your antivirus product to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block a majority of new and unknown variants.

Microsoft Defender XDR customers can also turn on attack surface reduction rules to harden their environments against techniques used by this Mint Sandstorm subgroup. These rules, which can be configured by all Microsoft Defender Antivirus customers and not just those using the EDR solution, offer significant protection against the tradecraft discussed in this report.

- Block executable files from running unless they meet a prevalence, age, or trusted list criterion.
- Block JavaScript or VBScript from launching downloaded executable content.
- Block execution of potentially obfuscated scripts.

Detection details

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects activity associated with the MediaPl backdoor as the following malware:

- Backdoor:Win64/Eyeglass.A

Microsoft Defender Antivirus detects activity associated with the MischiefTut backdoor as the following *malware*:

- Behavior:Win32/MischiefTut

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint provides customers with detections and alerts. Alerts with the following titles in the Security Center can indicate threat activity related to Mint Sandstorm.

- Possible Mint Sandstorm activity
- Anomaly detected in ASEP registry

Threat intelligence reports

Microsoft customers can use the following reports in Microsoft products to get the most up-to-date information about the threat actor, malicious activity, and techniques discussed in this blog. These reports provide the intelligence, protection information, and recommended actions to prevent, mitigate, or respond to associated threats found in customer environments.

Microsoft Defender Threat Intelligence

- Nation-state threat actor Mint Sandstorm refines tradecraft to attack high-value targets
- Mint Sandstorm delivers MischiefTut to researchers in tailored phishing campaigns

Microsoft Defender XDR Threat analytics

- Nation-state threat actor Mint Sandstorm refines tradecraft to attack high-value targets

Indicators of compromise

Organizations who fit the targeting model discussed in this report can hunt for the following indicators of compromise in their environments.

Domains

- *east-healthy-dress[.]glitch[.]me*
- *coral-polydactyl-dragonfruit[.]glitch[.]me*
- *kwhfibejjyxregxmnpcs[.]supabase[.]co*
- *epibvgvoszemkwjnplyc[.]supabase[.]co*
- *ndrrftqrlblfecpupppp[.]supabase[.]co*
- *cloud-document-edit[.]onrender[.]com*

Files

- *MediaPl.dll* (SHA-256: *f2dec56acef275a0e987844e98afcc44bf8b83b4661e83f89c6a2a72c5811d5f*)

Advanced hunting

Microsoft Defender XDR

Curl command used to retrieve malicious files

Use this query to locate the curl command Mint Sandstorm used to pull down malicious files in this campaign.

```
DeviceProcessEvents

| where InitiatingProcessCommandLine has_all('id=',

'&Prog') and InitiatingProcessCommandLine has_any('vbs', '--ssl')
```

Creation of log files

Use this query to identify files created by Mint Sandstorm, ostensibly for exfiltration.

```
DeviceProcessEvents
```

```
| where InitiatingProcessCommandLine has_all('powershell', '$pnt', 'Get-Content', 'gcm') and
InitiatingProcessCommandLine has_any('documentLog', 'documentLoger', 'Logdocument')
```

Files with double file name extensions

Use this query to find files with double extension, e.g., .pdf.lnk.

```
DeviceFileEvents

| where FileName endswith ".pdf.lnk"
```

Registry keys with VBScript

Use this query to find registry run keys entry with VBScript in value

```
DeviceRegistryEvents

| where ActionType == "RegistryValueSet" or ActionType == "RegistryKeyCreated"

| where RegistryKey endswith @"\Software\Microsoft\Windows\CurrentVersion\Run" or

RegistryKey endswith @"\Software\Microsoft\Windows\CurrentVersion\RunOnce" or

RegistryKey endswith @"\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run"

| where RegistryValueData has_any ("vbscript",".vbs")
```