Onyx Sleet uses array of malware to gather intelligence for North Korea

7/25/2024

On July 25, 2024, the United States Department of Justice (DOJ) indicted an individual linked to the North Korean threat actor that Microsoft tracks as Onyx Sleet. Microsoft Threat Intelligence collaborated with the Federal Bureau of Investigation (FBI) in tracking activity associated with Onyx Sleet. We will continue to closely monitor Onyx Sleet's activity to assess changes following the indictment.

First observed by Microsoft in 2014, Onyx Sleet has conducted cyber espionage through numerous campaigns aimed at global targets with the goal of intelligence gathering. More recently, it has expanded its goals to include financial gain. This threat actor operates with an extensive set of custom tools and malware, and regularly evolves its toolset to add new functionality and to evade detection, while keeping a fairly uniform attack pattern. Onyx Sleet's ability to develop a spectrum of tools to launch its tried-and-true attack chain makes it a persistent threat, particularly to targets of interest to North Korean intelligence, like organizations in the defense, engineering, and energy sectors.

Microsoft tracks campaigns related to Onyx Sleet and directly notifies customers who have been targeted or compromised, providing them with the necessary information to help secure their environments. In this blog, we will share intelligence about Onyx Sleet and its historical tradecraft and targets, as well as our analysis of recent malware campaigns, with the goal of enabling the broader community to identify and respond to similar campaigns. We also provide protection, detection, and hunting guidance to help improve defenses against these attacks.

Who is Onyx Sleet?

Onyx Sleet conducts cyber espionage primarily targeting military, defense, and technology industries, predominately in India, South Korea, and the United States. This threat actor has historically leveraged spear-phishing as a means of compromising target environments; however, in recent campaigns, they have mostly exploited N-day vulnerabilities, leveraging publicly available and custom exploits to gain initial access. In October 2023, Onyx Sleet exploited the TeamCity CVE-2023-42793 vulnerability as a part of a targeted attack. Exploiting this vulnerability enabled the threat actor to perform a remote code execution attack and gain administrative control of the server.

Onyx Sleet develops and uses a spectrum of tools that range from custom to open source. They have built an extensive set of custom remote access trojans (RATs) that they use in campaigns, and routinely developed new variants of these RATs to add new functionality and implement new ways of evading detection. Onyx Sleet often uses leased virtual private servers (VPS) and compromised cloud infrastructure for command-and-control (C2).

Onyx Sleet is tracked by other security companies as SILENT CHOLLIMA, Andariel, DarkSeoul, Stonefly, and TDrop2.

Affiliations with other threat actors originating from North Korea

SLEET ACTORS

Learn about North Korean threat actors

Onyx Sleet has demonstrated affiliations with other North Korean actors, indicating its integration with a broader network of North Korean cyber operations. Microsoft has observed an overlap between Onyx Sleet and Storm-0530. Both groups were observed operating within the same infrastructure and were involved in the development and use of ransomware in attacks in late 2021 and 2022.

Onyx Sleet targets

In pursuit of its primary goal of intelligence collection, Onyx Sleet has focused on targeting entities in the defense and energy industries, predominately in India, South Korea, and the United States. Recent attacks include the targeting of South Korean educational institutions, construction companies, and manufacturing organizations in May 2024. Onyx Sleet has also shown interest in taking advantage of online gambling websites, possibly for financial gain either on behalf of North Korea or for individual members of the group.

Onyx Sleet tradecraft

Onyx Sleet has used the same tactics, techniques, and procedures (TTPs) over extended periods, suggesting the threat actor views its tradecraft as effective. Onyx Sleet historically leveraged spear-phishing to compromise targets, and in more recent campaigns, they have been observed to primarily use exploits for initial access, alongside a loader, downloader, and backdoor as a part of its well-established attack chain.

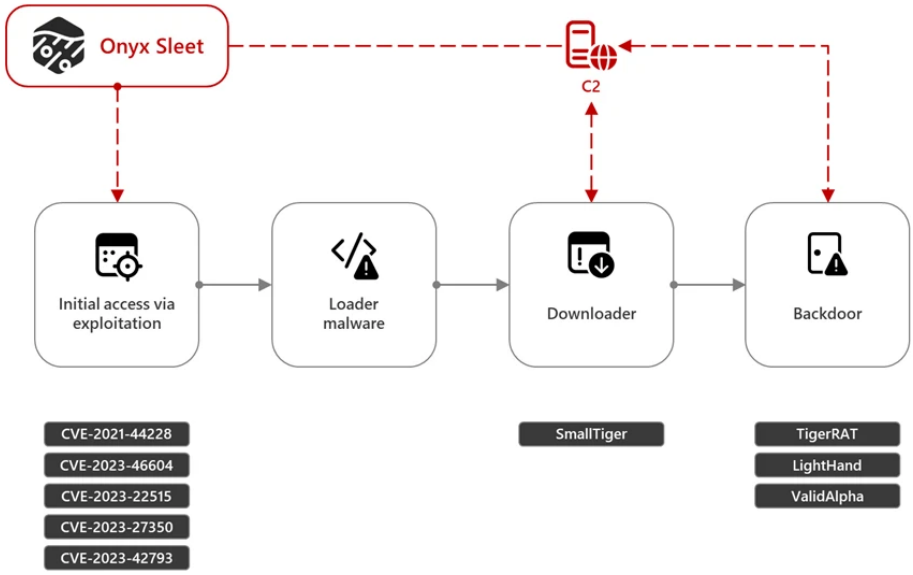

Figure 1. Onyx Sleet attack chain

Onyx Sleet nevertheless made some changes, for example, adding new C2 servers and hosting IPs, creating new malware, and launching multiple campaigns over time. In the past, Onyx Sleet introduced custom ransomware strains as a part of its campaigns. It also created and deployed the RAT identified by Kaspersky as Dtrack, which was observed in global attacks from September 2019 to January 2024. The Dtrack RAT follows the common attack chain used by Onyx Sleet and includes the exploitation of the Log4j 2 CVE-2021-44228 vulnerability for initial access and the use of payloads signed with an invalid certificate masquerading as legitimate software to evade detection.

Another example of Onyx Sleet introducing variations in the implementation of its attack chain is the campaign identified by AhnLab Security Intelligence Center (ASEC) in May 2024. In this campaign, the threat actor employed a previously unseen malware family dubbed as Dora RAT. Developed in the Go programming language, this custom malware strain targeted South Korean educational institutions, construction companies, and manufacturing organizations.

Onyx Sleet avoids common detection techniques across its attack lifecycle by heavily using custom encryption and obfuscation algorithms and launching as much of its code in memory as possible. These tools and techniques have been observed in several reported campaigns, including TDrop2.

Onyx Sleet has also used several off-the shelf tools, including Sliver, remote monitoring and management (RMM) tools SOCKS proxy tools, Ngrok, and masscan. We have also observed Onyx Sleet using commercial packers like Themida and VMProtect to obfuscate their malware. In January 2024, Microsoft Threat Intelligence identified a campaign attributed to Onyx Sleet that deployed a Sliver implant, an open-source C2 framework that supports multiple operators, listener types, and payload generation. Like the Dtrack RAT, this malware was signed with an invalid certificate impersonating Tableau software. Further analysis revealed that this Onyx Sleet campaign compromised multiple aerospace and defense organizations from October 2023 to June 2024.

Figure 2. File signature showing the fake Tableau Software certificate (source: VirusTotal)

Apart from the previously mentioned Log4j 2 vulnerability, Onyx Sleet has exploited other publicly disclosed (N-day) vulnerabilities to gain access to target environments. Some vulnerabilities recently exploited by Onyx Sleet include:

- CVE-2023-46604 (Apache ActiveMQ)
- CVE-2023-22515 (Confluence)
- CVE-2023-27350 (PaperCut)
- CVE-2023-42793 (TeamCity)

In addition to these well-known and disclosed vulnerabilities, Onyx Sleet has used custom exploit capabilities in campaigns targeting users mostly in South Korea. In these campaigns, Onyx Sleet exploited vulnerabilities in a remote desktop/management application, a data loss prevention application, a network access control system, and an endpoint detection and response (EDR) product.

Recent malware campaigns

In December 2023, South Korean authorities attributed attacks that stole over 1.2 TB of data from targeted South Korean defense contractors using custom malware to Andariel. Microsoft has attributed several custom malware families used in the said attacks – TigerRAT, SmallTiger, LightHand, and ValidAlpha – to Onyx Sleet.

TigerRAT

Since 2020, Onyx Sleet has been observed using the custom RAT malware TigerRAT. In some campaigns using TigerRAT, Onyx Sleet exploited vulnerabilities in Log4j 2 to deliver and install the malware. When launched, this malware can steal confidential information and carry out commands, such as keylogging and screen recording, from the C2.

SmallTiger

In February 2024, ASEC identified SmallTiger, a new malware strain targeting South Korean defense and manufacturing organizations. During the process of lateral movement, this malware is delivered as a DLL file (*SmallTiger[.]dll*) and uses a C2 connection to download and launch the payload into memory. Microsoft researchers have determined that SmallTiger is a C++ backdoor with layered obfuscation, encountered in the wild as a Themida or VMProtect packed executable.

The SmallTiger campaign can be tied back to a campaign using a similar attack chain beginning in November 2023 that delivered the DurianBeacon RAT malware. In May 2024, Microsoft observed Onyx Sleet continuing to conduct attacks targeting South Korean defense organizations using SmallTiger.

LightHand

LightHand is a custom, lightweight backdoor used by Onyx Sleet for remote access of target devices. Via LightHand, Onyx Sleet can execute arbitrary commands through command shell (*cmd.exe*), get system storage information, perform directory listing, and create/delete files on the target device.

ValidAlpha (BlackRAT)

ValidAlpha (also known as BlackRAT) is a custom backdoor developed in the Go programming language and used by Onyx Sleet to target organizations globally in the energy, defense, and engineering sectors since at least 2023. ValidAlpha can run an arbitrary file, list contents of a directory, download a file, take screenshots, and launch a shell to execute arbitrary commands.

Samples of ValidAlpha analyzed by Microsoft had a unique PDB string:
I:/01___Tools/02__RAT/Black/Client_Go/Client.go

Recommendations

Microsoft recommends the following mitigations to defend against attacks by Onyx Sleet:

- Keep software up to date. Apply new security patches as soon as possible.
- Turn on cloud-delivered protection in Microsoft Defender Antivirus, or the equivalent for your antivirus product, to help cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block a majority of new and unknown variants.
- Enable network protection to help prevent access to malicious domains.
- Run endpoint detection and response (EDR) in block mode so that Microsoft Defender for Endpoint can help block malicious artifacts, even when your non-Microsoft antivirus does not detect the threat or when Microsoft Defender Antivirus is running in passive mode. EDR in block mode works behind the scenes to help remediate malicious artifacts that are detected post-breach.
- Configure investigation and remediation in full automated mode to allow Microsoft Defender for Endpoint to take immediate action on alerts to help resolve breaches, significantly reducing alert volume

Microsoft Defender customers can turn on attack surface reduction rules to help prevent common attack techniques used by Onyx Sleet:

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

Detection details

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects threat components as the following malware families:

- CertutilPE
- Dora
- LightHand
- SmallTiger
- TigerCrypt
- TigerRAT
- ValidAlpha

Microsoft Defender for Endpoint

The following Microsoft Defender for Endpoint alerts can indicate associated threat activity:

- Onyx Sleet activity group

The following alerts might also indicate threat activity related to this threat. Note, however, that these alerts can be also triggered by unrelated threat activity:

- Document contains macro to download a file

Microsoft Defender Vulnerability Management

Microsoft Defender Vulnerability Management surfaces devices that may be affected by the following vulnerabilities used in this threat:

- CVE-2023-42793 (TeamCity)
- CVE-2023-27350 (Papercut)
- CVE-2021-44228 (Log4j 2)

Microsoft Defender Threat Intelligence

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.

- Tool Profile: Dtrack
- Onyx Sleet targeting defense firm in the Middle East
- Onyx Sleet targets electrical equipment manufacturer in India
- Onyx Sleet exploits vulnerable VMWare Horizon servers
- Onyx Sleet using Sliver remote access trojan in attacks on aerospace and defense

- Same Targets, new playbooks: East Asia threat actors employ unique methods

Microsoft Sentinel queries

Microsoft Sentinel customers can use the TI Mapping analytics (a series of analytics all prefixed with 'TI map') to automatically match the malicious domain indicators mentioned in this blog post with data in their workspace. If the TI Map analytics are not currently deployed, customers can install the Threat Intelligence solution from the Microsoft Sentinel Content Hub to have the analytics rule deployed in their Sentinel workspace.

Use this query to assess the existence of vulnerabilities used by Onyx Sleet:

```
DeviceTvmSoftwareVulnerabilities

| where CveId in ("CVE-2021-44228","CVE-2023-27350","CVE-2023-42793")

| project DeviceId,DeviceName,OSPlatform,OSVersion,SoftwareVendor,SoftwareName,SoftwareVersion,

CveId,VulnerabilitySeverityLevel

| join kind=inner ( DeviceTvmSoftwareVulnerabilitiesKB | project CveId,
CvssScore,IsExploitAvailable,VulnerabilitySeverityLevel,PublishedDate,VulnerabilityDescription,AffectedSoftware ) on
CveId

| project DeviceId,DeviceName,OSPlatform,OSVersion,SoftwareVendor,SoftwareName,SoftwareVersion,

CveId,VulnerabilitySeverityLevel,CvssScore,IsExploitAvailable,PublishedDate,VulnerabilityDescription,AffectedSoftware
```

Use this query to detect associated network IOCs:

```
let remoteip = dynamic(["84.38.134.56","45.155.37.101","213.139.205.151","109.248.150.147","162.19.71.175","147.78.149.

let remoteurl =
dynamic(["americajobmail.site","privatemake.bounceme.net","ww3c.bounceme.net","advice.uphearth.com","http://84.38.134.5

DeviceNetworkEvents

| where RemoteIP == remoteip or RemoteUrl == remoteurl

| project TimeGenerated, DeviceId, DeviceName, Protocol, LocalIP, LocalIPType, LocalPort,RemoteIP, RemoteIPType, Remotel
```

Use this query to detect associated file IOCs:

```
let selectedTimestamp = datetime(2024-07-17T00:00:00.0000000Z);

let fileName = "SmallTiger.dll";

let FileSHA256 = dynamic(["f32f6b229913d68daad937cc72a57aa45291a9d623109ed48938815aa7b6005c","0837dd54268c373069fc5c162
","29c6044d65af0073424ccc01abcb8411cbdc52720cac957a3012773c4380bab3","fed94f461145681dc9347b382497a72542424c64b6ae6fcf9

let SignerName = "INVALID:Tableau Software Inc.";

let Signerhash = "6624c7b8faac176d1c1cb10b03e7ee58a4853f91";

let certificateserialnumber = "76cb5d1e6c2b6895428115705d9ac765";

search in (AlertEvidence,BehaviorEntities,CommonSecurityLog,DeviceBaselineComplianceProfiles,DeviceEvents,DeviceFileEver

DeviceLogonEvents,DeviceNetworkEvents,DeviceProcessEvents,DeviceRegistryEvents,DeviceFileCertificateInfo,DynamicEventCol

TimeGenerated between ((selectedTimestamp - 1m) .. (selectedTimestamp + 90d)) // from July 17th runs the search backwar

and

( FileName == fileName or OldFileName == fileName or ProfileName == fileName or InitiatingProcessFileName == fileName o

or InitiatingProcessVersionInfoInternalFileName == fileName or InitiatingProcessVersionInfoOriginalFileName == fileName

or ProcessVersionInfoInternalFileName == fileName or ProcessVersionInfoOriginalFileName == fileName or DestinationFileNa

or ServiceFileName == fileName or SHA256 in (FileSHA256) or InitiatingProcessSHA256 in (FileSHA256) or Signer == SignerI
```

Indicators of compromise

IP addresses

- 84.38.134[.]56
- 45.155.37[.]101
- 213.139.205[.]151
- 109.248.150[.]147
- 162.19.71[.]175
- 147.78.149[.]201

URL

- hxxp://84.38.134[.]56/procdump.gif

Actor-controlled domain

- americajobmail[.]site
- privatemake.bounceme[.]net
- ww3c.bounceme[.]net
- advice.uphearth[.]com

SHA-256

- TigerRAT
  - f32f6b229913d68daad937cc72a57aa45291a9d623109ed48938815aa7b6005c
  - 0837dd54268c373069fc5c1628c6e3d75eb99c3b3efc94c45b73e2cf9a6f3207
  - 29c6044d65af0073424ccc01abcb8411cbdc52720cac957a3012773c4380bab3
  - fed94f461145681dc9347b382497a72542424c64b6ae6fcf945f4becd2d46c32
  - 868a62feff8b46466e9d63b83135a7987bf6d332c13739aa11b747b3e2ad4bbf
- LightHand
  - f1662bee722a4e25614ed30933b0ced17b752d99fae868fbb326a46afa2282d5
  - 1b88b939e5ec186b2d19aec8f17792d493d74dd6ab3d5a6ddc42bfe78b01aff1
  - 3098e6e7ae23b3b8637677da7bfc0ba720e557e6df71fa54a8ef1579b6746061
  - 8daa6b20caf4bf384cc7912a73f243ce6e2f07a5cb3b3e95303db931c3fe339f
  - 7339cfa5a67f5a4261c18839ef971d7f96eaf60a46190cab590b439c71c4742b
- ValidAlpha
  - c2500a6e12f22b16e221ba01952b69c92278cd05632283d8b84c55c916efe27c
  - c1a09024504a5ec422cbea68e17dffc46472d3c2d73f83aa0741a89528a45cd1

Fake Tableau certificate

- Signer: INVALID:Tableau Software Inc.
- SignerHash: 6624c7b8faac176d1c1cb10b03e7ee58a4853f91
- CertificateSerialNumber: 76cb5d1e6c2b6895428115705d9ac765