North Korean threat actor Citrine Sleet exploiting Chromium zero-day

8/30/2024

On August 19, 2024, Microsoft identified a North Korean threat actor exploiting a zero-day vulnerability in Chromium, now identified as CVE-2024-7971, to gain remote code execution (RCE). We assess with high confidence that the observed exploitation of CVE-2024-7971 can be attributed to a North Korean threat actor targeting the cryptocurrency sector for financial gain. Our ongoing analysis and observed infrastructure lead us to attribute this activity with medium confidence to Citrine Sleet. We note that while the FudModule rootkit deployed has also been attributed to Diamond Sleet, another North Korean threat actor, Microsoft previously identified shared infrastructure and tools between Diamond Sleet and Citrine Sleet, and our analysis indicates this might be shared use of the FudModule malware between these threat actors.

CVE-2024-7971 is a type confusion vulnerability in the V8 JavaScript and WebAssembly engine, impacting versions of Chromium prior to 128.0.6613.84. Exploiting the vulnerability could allow threat actors to gain RCE in the sandboxed Chromium renderer process. Google released a fix for the vulnerability on August 21, 2024, and users should ensure they are using the latest version of Chromium. We would like to thank the Chromium team for their collaboration in addressing this issue. CVE-2024-7971 is the third exploited V8 type confusion vulnerability that has been patched in V8 this year, after CVE-2024-4947 and CVE-2024-5274. As with any observed nation-state actor activity, Microsoft has directly notified targeted or compromised customers, providing them with important information to help secure their environments.

In this blog, we share details on the North Korean threat actor Citrine Sleet and the observed tactics, techniques, and procedures (TTPs) used to exploit CVE-2024-7971, deploy the FudModule rootkit, and compromise systems. We further provide recommended mitigations, detection details, hunting guidance, and indicators of compromise (IOCs) to help defenders identify, respond to, and improve defenses against these attacks.

Who is Citrine Sleet?

The threat actor that Microsoft tracks as Citrine Sleet is based in North Korea and primarily targets financial institutions, particularly organizations and individuals managing cryptocurrency, for financial gain. As part of its social engineering tactics, Citrine Sleet has conducted extensive reconnaissance of the cryptocurrency industry and individuals associated with it. The threat actor creates fake websites masquerading as legitimate cryptocurrency trading platforms and uses them to distribute fake job applications or lure targets into downloading a weaponized cryptocurrency wallet or trading application based on legitimate applications. Citrine Sleet most commonly infects targets with the unique trojan malware it developed, AppleJeus, which collects information necessary to seize control of the targets' cryptocurrency assets. The FudModule rootkit described in this blog has now been tied to Citrine Sleet as shared tooling with Diamond Sleet.

SLEET ACTORS

Read about North Korean threat actors

The United States government has assessed that North Korean actors, like Citrine Sleet, will likely continue targeting vulnerabilities of cryptocurrency technology firms, gaming companies, and exchanges to generate and launder funds to support the North Korean regime. One of the organizations targeted by the CVE-2024-7971 exploitation was also previously targeted by Sapphire Sleet.

Citrine Sleet is tracked by other security companies as AppleJeus, Labyrinth Chollima, UNC4736, and Hidden Cobra, and has been attributed to Bureau 121 of North Korea's Reconnaissance General Bureau.

Exploiting CVE-2024-7971

The observed zero-day exploit attack by Citrine Sleet used the typical stages seen in browser exploit chains. First, the targets were directed to the Citrine Sleet-controlled exploit domain *voyagorclub[.]space*. While we cannot confirm

at this time how the targets were directed, social engineering is a common tactic used by Citrine Sleet. Once a target connected to the domain, the zero-day RCE exploit for CVE-2024-7971 was served.

After the RCE exploit achieved code execution in the sandboxed Chromium renderer process, shellcode containing a Windows sandbox escape exploit and the FudModule rootkit was downloaded, and then loaded into memory. The sandbox escape exploited CVE-2024-38106, a vulnerability in the Windows kernel that Microsoft fixed on August 13, 2024, before Microsoft discovered this North Korean threat actor activity. CVE-2024-38106 was reported to Microsoft Security Response Center (MSRC) as being exploited; however, our investigations so far have not suggested any link between the reported CVE-2024-38106 exploit activity and this Citrine Sleet exploit activity, beyond exploiting the same vulnerability. This may suggest a "bug collision," where the same vulnerability is independently discovered by separate threat actors, or knowledge of the vulnerability was shared by one vulnerability researcher to multiple actors.

Once the sandbox escape exploit was successful, the main FudModule rootkit ran in memory. This rootkit employs direct kernel object manipulation (DKOM) techniques to disrupt kernel security mechanisms, executes exclusively from user mode, and performs kernel tampering through a kernel read/write primitive. We did not observe any additional malware activity on the target devices.

FudModule rootkit

FudModule is a sophisticated rootkit malware that specifically targets kernel access while evading detection. Threat actors have been observed using the FudModule data-only rootkit to establish admin-to-kernel access to Windows-based systems to allow read/write primitive functions and perform DKOM.

Diamond Sleet has been observed using FudModule since October 2021. The earliest variant of FudModule was reported publicly in September 2022 by ESET and AhnLAB researchers, when threat actors exploited known vulnerable drivers to establish admin-to-kernel access in the technique known as bring your own vulnerable driver (BYOVD). In February 2024, Avast researchers published analysis on an updated FudModule variant that is significantly more advanced and difficult to detect, since it exploits a zero-day vulnerability in *appid.sys*, an AppLocker driver that is installed by default into Windows (CVE-2024-21338).

Further research by Avast uncovered a full attack chain deploying the updated variant of FudModule known as "FudModule 2.0," which includes malicious loaders and a late-stage remote access trojan (RAT). This attack chain revealed the previously unknown malware Kaolin RAT was responsible for loading the FudModule rootkit to targeted devices. Kaolin RAT established a secure, AES-encrypted connection with the command and control (C2) server and had capabilities to execute a robust list of commands, such as downloading and uploading files to the C2 server and creating or updating processes. The updated variant of FudModule exhibited an attack chain similar to that seen in Citrine Sleet's zero-day exploit of CVE-2024-7971.

On August 13, Microsoft released a security update to address a zero-day vulnerability in the *AFD.sys* driver in Windows (CVE-2024-38193) identified by Gen Threat Labs. In early June, Gen Threat Labs identified Diamond Sleet exploiting this vulnerability in an attack employing the FudModule rootkit, which establishes full standard user-to-kernel access, advancing from the previously seen admin-to-kernel access. Gen Threat Labs released this information publicly on August 16.

Recommendations

The CVE-2024-7971 exploit chain relies on multiple components to compromise a target, and this attack chain fails if any of these components are blocked, including CVE-2024-38106. Microsoft released a security update on August 13, 2024, for the CVE-2024-38106 vulnerability exploited by Diamond Sleet, thus also blocking attempts to exploit the CVE-2024-7971 exploit chain on updated systems. Customers who have not implemented these fixes yet are urged to do so as soon as possible for their organization's security.

Zero-day exploits necessitate not only keeping systems up to date, but also security solutions that provide unified visibility across the cyberattack chain to detect and block post-compromise attacker tools and malicious activity following exploitation. Microsoft recommends the following mitigations to reduce the impact of this threat.

Strengthen operating environment configuration

- Keep operating systems and applications up to date. Apply security patches as soon as possible. Ensure that Google Chrome web browser is updated at version 128.0.6613.84 or later, and Microsoft Edge web browser is

updated at version 128.0.2739.42 or later to address the CVE-2024-7971 vulnerability.
- Encourage users to use Microsoft Edge and other web browsers that support Microsoft Defender SmartScreen, which identifies and blocks malicious websites, including phishing sites, scam sites, and sites that host malware.

Strengthen Microsoft Defender for Endpoint configuration

- Ensure that tamper protection is turned on in Microsoft Dender for Endpoint.
- Enable network protection in Microsoft Defender for Endpoint.
- 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 let Microsoft Defender for Endpoint take immediate action on alerts to help resolve breaches, significantly reducing alert volume.

Strengthen Microsoft Defender Antivirus configuration

- 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 majority of new and unknown variants.
- Turn on Microsoft Defender Antivirus scanning of downloaded files and attachments.
- Turn on real-time protection in Microsoft Defender Antivirus.

Detection details

Microsoft Defender for Endpoint

The following Microsoft Defender for Endpoint alert might also indicate threat activity related to this threat. Note, however, that this alert can also be triggered by unrelated threat activity.

- Emerging threat activity group Citrine Sleet detected

Microsoft Defender Vulnerability Management

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

- CVE-2024-7971
- CVE-2024-38106

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 intelligence and protection information, and recommend actions to help prevent, mitigate, or respond to associated threats found in customer environments.

Microsoft Defender Threat Intelligence

- Actor profile: Citrine Sleet
- Actor profile: Diamond Sleet
- Tool profile: AppleJeus

Hunting queries

Microsoft Defender XDR

Microsoft Defender XDR customers can run the following query to find related activity in their networks:

Citrine Sleet domain activity

Microsoft Defender XDR customers may query for devices that may have interacted with Citrine Sleet domains related to this activity. Note that Microsoft Defender for Endpoint customers may surface related events with the alert title “Emerging threat activity group Citrine Sleet detected”.

```
let domainList = dynamic(["weinsteinfrog.com", "voyagorclub.space"]);

union

(

DnsEvents

| where QueryType has_any(domainList) or Name has_any(domainList)

| project TimeGenerated, Domain = QueryType, SourceTable = "DnsEvents"

),

(

IdentityQueryEvents

| where QueryTarget has_any(domainList)

| project Timestamp, Domain = QueryTarget, SourceTable = "IdentityQueryEvents"

),

(

DeviceNetworkEvents

| where RemoteUrl has_any(domainList)

| project Timestamp, Domain = RemoteUrl, SourceTable = "DeviceNetworkEvents"

),

(

DeviceNetworkInfo

| extend DnsAddresses = parse_json(DnsAddresses), ConnectedNetworks = parse_json(ConnectedNetworks)

| mv-expand DnsAddresses, ConnectedNetworks

| where DnsAddresses has_any(domainList) or ConnectedNetworks.Name has_any(domainList)

| project Timestamp, Domain = coalesce(DnsAddresses, ConnectedNetworks.Name), SourceTable =
"DeviceNetworkInfo"

),

(

VMConnection

| extend RemoteDnsQuestions = parse_json(RemoteDnsQuestions), RemoteDnsCanonicalNames =
parse_json(RemoteDnsCanonicalNames)

| mv-expand RemoteDnsQuestions, RemoteDnsCanonicalNames

| where RemoteDnsQuestions has_any(domainList) or RemoteDnsCanonicalNames has_any(domainList)

| project TimeGenerated, Domain = coalesce(RemoteDnsQuestions, RemoteDnsCanonicalNames),
SourceTable = "VMConnection"

),

(

W3CIISLog

| where csHost has_any(domainList) or csReferer has_any(domainList)

| project TimeGenerated, Domain = coalesce(csHost, csReferer), SourceTable = "W3CIISLog"

),

(

EmailUrlInfo
```

```
| where UrlDomain has_any(domainList)
| project Timestamp, Domain = UrlDomain, SourceTable = "EmailUrlInfo"
),
(
UrlClickEvents
| where Url has_any(domainList)
| project Timestamp, Domain = Url, SourceTable = "UrlClickEvents"
)
| order by TimeGenerated desc
```

Microsoft Sentinel

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.

Search for domain IOCs

```
let domainList = dynamic(["weinsteinfrog.com", "voyagorclub.space"]);
union
(
DnsEvents
| where QueryType has_any(domainList) or Name has_any(domainList)
| project TimeGenerated, Domain = QueryType, SourceTable = "DnsEvents"
),
(
IdentityQueryEvents
| where QueryTarget has_any(domainList)
| project TimeGenerated, Domain = QueryTarget, SourceTable = "IdentityQueryEvents"
),
(
DeviceNetworkEvents
| where RemoteUrl has_any(domainList)
| project TimeGenerated, Domain = RemoteUrl, SourceTable = "DeviceNetworkEvents"
),
(
DeviceNetworkInfo
| extend DnsAddresses = parse_json(DnsAddresses), ConnectedNetworks = parse_json(ConnectedNetworks)
| mv-expand DnsAddresses, ConnectedNetworks
| where DnsAddresses has_any(domainList) or ConnectedNetworks.Name has_any(domainList)
| project TimeGenerated, Domain = coalesce(DnsAddresses, ConnectedNetworks.Name), SourceTable =
"DeviceNetworkInfo"
),
(
VMConnection
```

```
| extend RemoteDnsQuestions = parse_json(RemoteDnsQuestions), RemoteDnsCanonicalNames =
parse_json(RemoteDnsCanonicalNames)

| mv-expand RemoteDnsQuestions, RemoteDnsCanonicalNames

| where RemoteDnsQuestions has_any(domainList) or RemoteDnsCanonicalNames has_any(domainList)

| project TimeGenerated, Domain = coalesce(RemoteDnsQuestions, RemoteDnsCanonicalNames),
SourceTable = "VMConnection"

),

(

W3CIISLog

| where csHost has_any(domainList) or csReferer has_any(domainList)

| project TimeGenerated, Domain = coalesce(csHost, csReferer), SourceTable = "W3CIISLog"

),

(

EmailUrlInfo

| where UrlDomain has_any(domainList)

| project TimeGenerated, Domain = UrlDomain, SourceTable = "EmailUrlInfo"

),

(

UrlClickEvents

| where Url has_any(domainList)

| project TimeGenerated, Domain = Url, SourceTable = "UrlClickEvents"

),

(

CommonSecurityLog

| where DestinationDnsDomain has_any(domainList)

| project TimeGenerated, Domain = DestinationDnsDomain, SourceTable = "CommonSecurityLog"

),

(

EmailEvents

| where SenderFromDomain has_any (domainList) or SenderMailFromDomain has_any (domainList)

| project TimeGenerated, SenderfromDomain = SenderFromDomain,SenderMailfromDomain =
SenderMailFromDomain, SourceTable = "EmailEvents"

)

| order by TimeGenerated desc
```

Assess presence of vulnerabilities used by Citrine Sleet

```
DeviceTvmSoftwareVulnerabilities

| where CveId has_any ("CVE-2024-7971","CVE-2024-38106","CVE-2024-38193","CVE-2024-21338")

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

CveId,VulnerabilitySeverityLevel

| join kind=inner ( DeviceTvmSoftwareVulnerabilitiesKB | project CveId,
CvssScore,IsExploitAvailable,VulnerabilitySeverityLevel,PublishedDate,VulnerabilityDescription,AffectedSoftwa
CveId

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

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

Indicators of compromise

During the attacks, Microsoft observed the following IOCs:

- voyagorclub[.]space
- weinsteinfrog[.]com

References

- https://nvd.nist.gov/vuln/detail/CVE-2024-7971
- https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html
- https://nvd.nist.gov/vuln/detail/CVE-2024-4947
- https://nvd.nist.gov/vuln/detail/CVE-2024-5274
- https://decoded.avast.io/janvojtesek/lazarus-and-the-fudmodule-rootkit-beyond-byovd-with-an-admin-to-kernel-zero-day/
- https://www.virusbulletin.com/uploads/pdf/conference/vb2022/papers/VB2022-Lazarus-and-BYOVD-evil-to-the-Windows-core.pdf
- https://asec.ahnlab.com/wp-content/uploads/2022/09/Analysis-Report-on-Lazarus-Groups-Rootkit-Attack-Using-BYOVD_Sep-22-2022.pdf
- https://decoded.avast.io/luiginocamastra/from-byovd-to-a-0-day-unveiling-advanced-exploits-in-cyber-recruiting-scams/
- https://www.gendigital.com/blog/news/innovation/protecting-windows-users
- https://www.google.com/chrome/update/
- https://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop_21.html