■ Microsoft ｜ Microsoft Security

Solutions ˅　Products ˅　Services ˅　Partners　｜　🌐　　All Microsoft ˅　🔍　Light ☀️◯ Dark
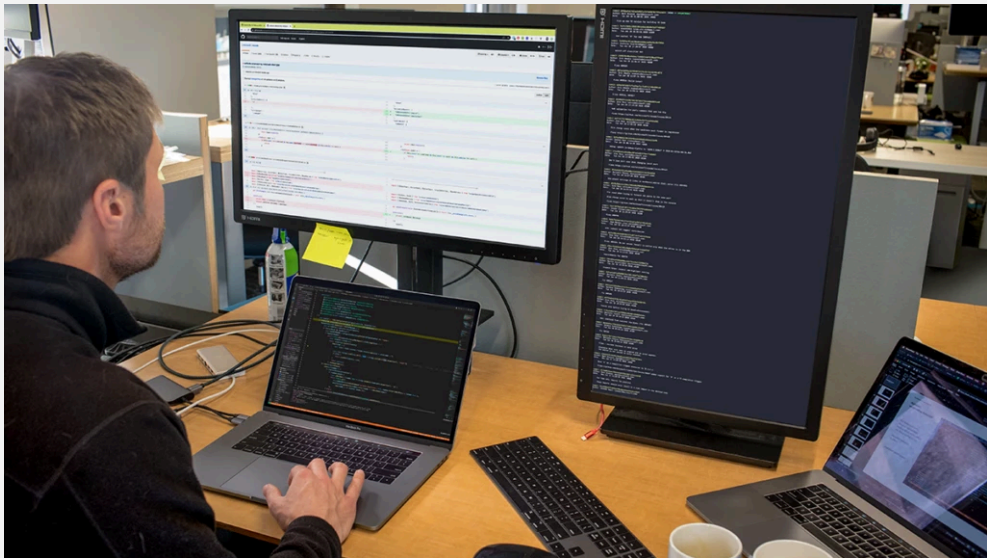
🏠 **Blog home** / Threat intelligence

Search the blog 🔍

Research Threat intelligence Microsoft Defender XDR
Vulnerabilities and exploits
10 min read

Multiple North Korean threat actors exploiting the TeamCity CVE-2023-42793 vulnerability

By Microsoft Threat Intelligence

October 18, 2023

Ⓕ 𝕏 Ⓛ in

Endpoint security

Microsoft Defender

Microsoft Defender for Endpoint

more ˅

Since early October 2023, Microsoft has observed two North Korean nation-state threat actors – Diamond Sleet and Onyx Sleet – exploiting CVE-2023-42793, a remote-code execution vulnerability affecting multiple versions of JetBrains TeamCity server. TeamCity is a continuous integration/continuous deployment (CI/CD) application used by organizations for DevOps and other software development activities.

ONYX SLEET

Read comprehensive report on Onyx Sleet ›

In past operations, Diamond Sleet and other North Korean threat actors have successfully carried out software supply chain attacks by infiltrating build environments. Given this, Microsoft assesses that this activity poses a particularly high risk to organizations who are affected. JetBrains has released an update to address this vulnerability and has developed a mitigation for users who are unable to update to the latest software version.

DIAMOND SLEET

Read about Diamond Sleet campaigns over the years ›

While the two threat actors are exploiting the same vulnerability, Microsoft observed Diamond Sleet and Onyx Sleet utilizing unique sets of tools and techniques following successful exploitation. Based on the profile of victim organizations affected by these intrusions, Microsoft assesses that the threat actors may be opportunistically compromising vulnerable servers. However, both actors have deployed malware and tools and utilized techniques that may enable persistent access to victim environments.

SLEET ACTORS

Read blogs on North Korean threat actors ›

As with any observed nation-state actor activity, Microsoft directly notifies customers that have been targeted or compromised and provides them with the information they need to secure their environments.

Who are Diamond Sleet and Onyx Sleet?

Diamond Sleet (ZINC) is a North Korean nation-state threat actor that prioritizes espionage, data theft, financial gain, and network destruction. The actor typically targets media, IT services, and defense-related entities around the world. Microsoft reported on Diamond Sleet's targeting of security researchers in January 2021 and the actor's weaponizing of open-source software in September 2022. In August 2023, Diamond Sleet conducted a software supply chain compromise of a German software provider.

Onyx Sleet (PLUTONIUM) is a North Korean nation-state threat actor that primarily targets defense and IT services organizations in South Korea, the United States, and India. Onyx Sleet employs a robust set of tools that they have developed to establish persistent access to victim environments and remain undetected. The actor frequently exploits N-day vulnerabilities as a means of gaining initial access to targeted organizations.

Diamond Sleet attack path 1: Deployment of ForestTiger backdoor

Following the successful compromise of TeamCity servers, Diamond Sleet utilizes PowerShell to download two payloads from legitimate infrastructure previously compromised by the threat actor. These two payloads, *Forest64.exe* and *4800-84DC-063A6A41C5C* are stored in the *C:\ProgramData* directory.

When launched, *Forest64.exe* checks for the presence of the file named *4800-84DC-063A6A41C5C*, then reads and decrypts the contents of that file using embedded, statically assigned key of 'uTYNkfKxHiZrx3KJ':

c:\ProgramData\Forest64.exe uTYNkfKxHiZrx3KJ

Interestingly, this same value is specified as a parameter when the malware is invoked, but we did not see it utilized during our analysis. The same value and configuration name was also referenced in historical activity reported by Kaspersky's Securelist on this malware, dubbed *ForestTiger*.

The decrypted content of *4800-84DC-063A6A41C5C* is the configuration file for the malware, which contains additional parameters, such as the infrastructure used by the backdoor for command and control (C2). Microsoft observed Diamond Sleet using infrastructure previously compromised by the actor for C2.

Microsoft observed *Forest64.exe* then creating a scheduled task named *Windows TeamCity Settings User Interface* so it runs every time the system starts with the above referenced command parameter "uTYNkfKxHiZrx3KJ". Microsoft also observed Diamond Sleet leveraging the *ForestTiger* backdoor to dump credentials via the LSASS memory. Microsoft Defender Antivirus detects this malware as *ForestTiger*.
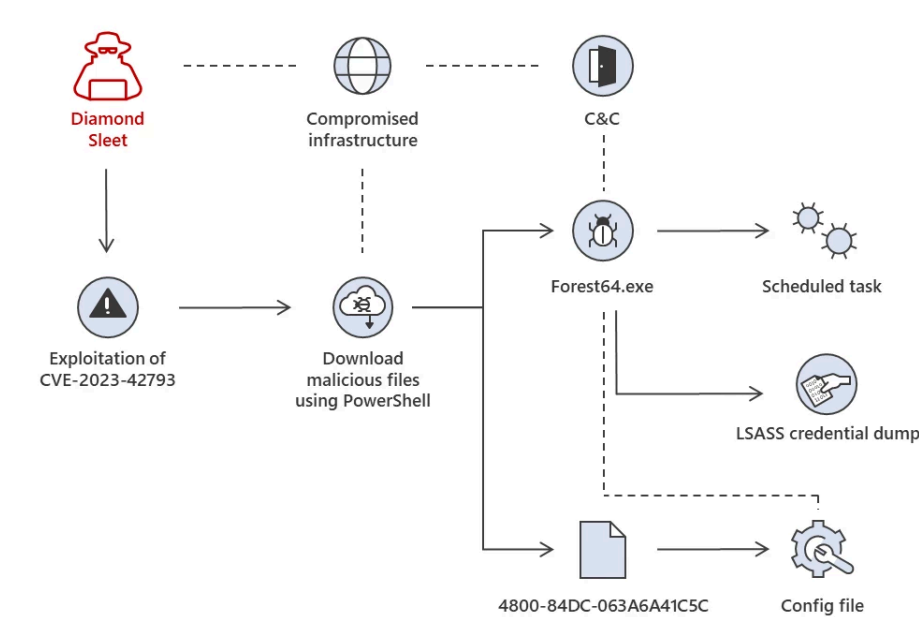

Figure 1. Diamond Sleet attack chain 1 using ForestTiger backdoor

Diamond Sleet attack path 2: Deploying payloads for use in DLL search-order hijacking attacks

Diamond Sleet leverages PowerShell on compromised servers to download a malicious DLL from attacker infrastructure. This malicious DLL is then staged in *C:\ProgramData* alongside a legitimate .exe file to carry out DLL search-order hijacking. Microsoft has observed these malicious DLL and legitimate EXE combinations used by the actor:

Malicious DLL name	Legitimate binary name
DSROLE.dll	*wsmprovhost.exe*
Version.dll	*clip.exe*

DSROLE.dll attack chain

When *DSROLE.dll* is loaded by *wsmprovhost.exe*, the DLL initiates a thread that enumerates and attempts to process files that exist in the same executing directory as the DLL. The first four bytes of candidate files are read and signify the size of the remaining buffer to read. Once the remaining data is read back, the bytes are reversed to reveal an executable payload that is staged in memory. The expected PE file should be a DLL with the specific export named 'StartAction'. The address of this export is resolved and then launched in memory.

While the functionality of *DSROLE.dll* is ultimately decided by whatever payloads it deobfuscates and launches, Microsoft has observed the DLL being used to launch *wksprt*.exe, which communicates with C2 domains. Microsoft Defender Antivirus detects *DSROLE.dll* using the family name *RollSling*.

Version.dll attack chain

When loaded by *clip.exe*, *Version.dll* loads and decrypts the contents of *readme.md*, a file downloaded alongside *Version.dll* from attacker-compromised infrastructure. The file *readme.md* contains data that is used as a multibyte XOR key to decrypt position-independent code (PIC) embedded in *Version.dll*. This PIC loads and launches the final-stage remote access trojan (RAT).
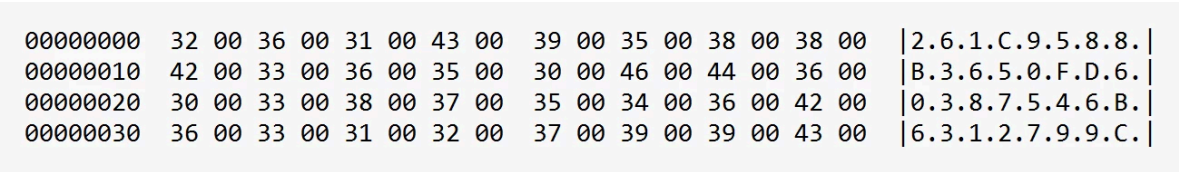
```
00000000  32 00 36 00 31 00 43 00  39 00 35 00 38 00 38 00  |2.6.1.C.9.5.8.8.|
00000010  42 00 33 00 36 00 35 00  30 00 46 00 44 00 36 00  |B.3.6.5.0.F.D.6.|
00000020  30 00 33 00 38 00 37 00  35 00 34 00 36 00 42 00  |0.3.8.7.5.4.6.B.|
00000030  36 00 33 00 31 00 32 00  37 00 39 00 39 00 43 00  |6.3.1.2.7.9.9.C.|
```

Figure 2. Composition of readme.md used as multibyte XOR key by Version.dll

```
malutil-xor Version.dll -o 0x16f604 -s 0x36ed5
0x32003600310043003900350038003800420033003600350030004600440036003000330038003
70035003400360042003600330031003200370039003900430 > dec_blob1.bin
```
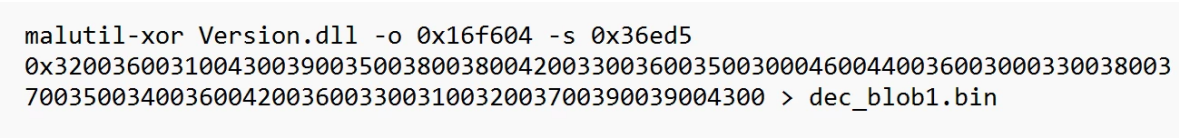
Figure 3. Application of XOR key to expose next-stage code block

```
malutil-pecarver dec_blob1.bin
Found 1 embedded PE file(s) within dec_blob1.bin
Processed dec_blob1.bin and written as pe_0x8d3
_b10c8eb1616fa09ceab3b635959ab1368febb4a9f29dc6f79c6de1dace7eeafe
```
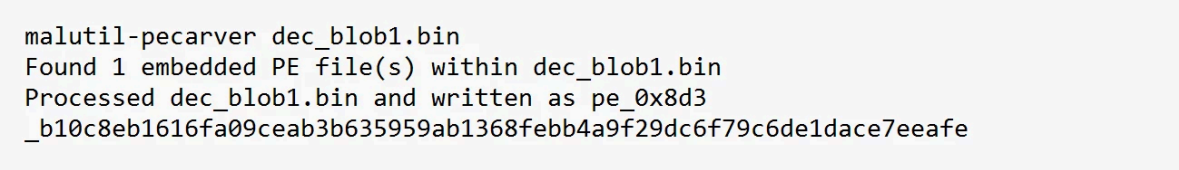
Figure 4. Carving out embedded PE from code block

Once loaded in memory, the second-stage executable decrypts an embedded configuration file containing several URLs used by the malware for command and control. Shortly after the malware beacons to the callback URL, Microsoft has observed a separate process *iexpress.exe* created and communicating with other C2

domains. Microsoft Defender Antivirus detects *Version.dll* using the family name
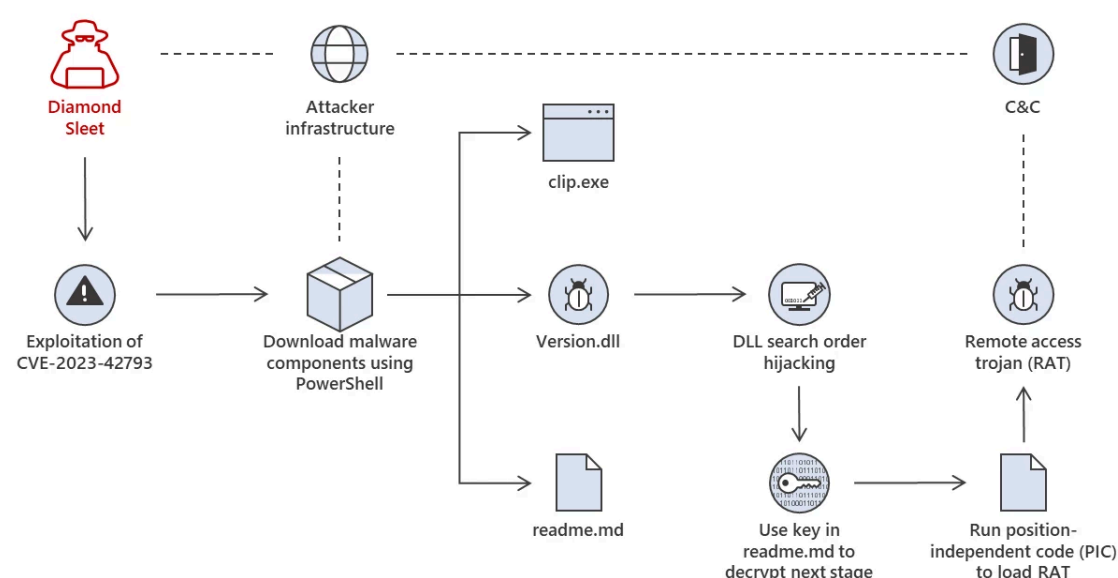*FeedLoad*.

Figure 5. Diamond Sleet attack chain 2 using DLL search order hijacking

After successful compromise, Microsoft observed Diamond Sleet dumping
credentials via the LSASS memory.

In some cases, Microsoft observed Diamond Sleet intrusions that utilized tools and
techniques from both paths 1 and 2.

Onyx Sleet attack path: User account creation, system discovery, and payload deployment

Following successful exploitation using the TeamCity exploit, Onyx Sleet creates a
new user account on compromised systems. This account, named *krtbgt*, is likely
intended to impersonate the legitimate Windows account name KRBTGT, the
Kerberos Ticket Granting Ticket. After creating the account, the threat actor adds it to
the Local Administrators Group through net use:

```
net  localgroup administrators krtbgt /add
```

The threat actor also runs several system discovery commands on compromised
systems, including:

```
net localgroup 'Remote Desktop Users'
net localgroup Administrators
cmd.exe "/c tasklist | findstr Sec"
cmd.exe "/c whoami"
cmd.exe "/c netstat -nabp tcp"
cmd.exe "/c ipconfig /all"
cmd.exe "/c systeminfo"
```

Next, the threat actor deploys a unique payload to compromised systems by
downloading it from attacker-controlled infrastructure via PowerShell. Microsoft
observed these file paths for the unique payload:

- *C:\Windows\Temp\temp.exe*
- *C:\Windows\ADFS\bg\inetmgr.exe*

This payload, when launched, loads and decrypts an embedded PE resource. This
decrypted payload is then loaded into memory and launched directly. The inner
payload is a proxy tool that helps establish a persistent connection between the
compromised host and attacker-controlled infrastructure. Microsoft Defender
Antivirus detects this proxy tool as *HazyLoad*.

Microsoft also observed the following post-compromise tools and techniques
leveraged in this attack path:

- Using the attacker-controlled *krtbgt* account to sign into the compromised
device via remote desktop protocol (RDP)

- Stopping the TeamCity service, likely in an attempt to prevent access by other threat actors
- Dumping credentials via the LSASS memory
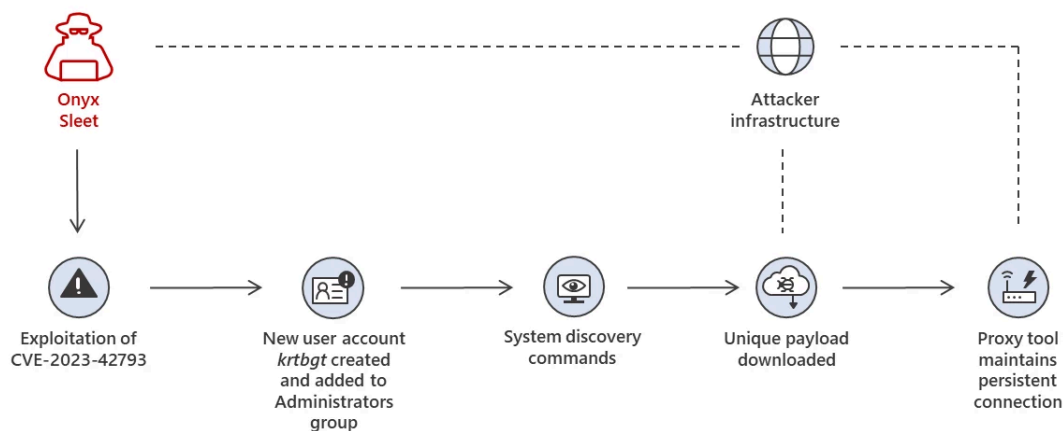- Deploying tools to retrieve credentials and other data stored by browsers

Figure 6. Onyx Sleet attack chain with user account creation

Recommended mitigation actions

Microsoft recommends the following mitigations to reduce the impact of this threat.

- Apply the update or mitigations released by JetBrains to address CVE-2023-42793.
- Use the included indicators of compromise to investigate whether they exist in your environment and assess for potential intrusion.
- Block in-bound traffic from IPs specified in the IOC table.
- Use Microsoft Defender Antivirus to protect from this threat. Turn on cloud-delivered protection and automatic sample submission. These capabilities use artificial intelligence and machine learning to quickly identify and stop new and unknown threats.
- Take immediate action to address malicious activity on the impacted device. If malicious code has been launched, the attacker has likely taken complete control of the device. Immediately isolate the system and perform a reset of credentials and tokens.
- Investigate the device timeline for indications of lateral movement activities using one of the compromised accounts. Check for additional tools that attackers might have dropped to enable credential access, lateral movement, and other attack activities.
- Ensure that "Safe DLL Search Mode" is set.
- Turn on the following attack surface reduction rule:
  - Block executable files from running unless they meet a prevalence, age, or trusted list criterion

Detections

Microsoft 365 Defender

Microsoft 365 Defender is becoming Microsoft Defender XDR. Learn more.

Microsoft Defender Vulnerability Management

Microsoft Defender Vulnerability Management surfaces devices that may be affected by the CVE-2023-42793 vulnerability leveraged in these attacks.

Microsoft Defender Antivirus

Microsoft Defender Antivirus customers should look for the following family names for activity related to these attacks:

- ForestTiger
- RollSling
- FeedLoad
- HazyLoad

Microsoft Defender for Endpoint

The following Microsoft Defender for Endpoint alerts could indicate activity associated with this threat. These alerts, however, can be triggered by unrelated threat activity.

- Diamond Sleet Actor activity detected
- Onyx Sleet Actor activity detected
- Possible exploitation of JetBrains TeamCity vulnerability
- Suspicious behavior by cmd.exe was observed
- Suspicious DLL loaded by an application
- Suspicious PowerShell download or encoded command execution
- Possible lateral movement involving suspicious file
- A script with suspicious content was observed
- Suspicious scheduled task

Hunting queries

Microsoft 365 Defender

Command and control using iexpress.exe or wksprt.exe

```
DeviceNetworkEvents
| where (InitiatingProcessFileName =~ "wksprt.exe" and Initiatin
or (InitiatingProcessFileName =~ "iexpress.exe" and InitiatingPr
```

Search order hijack using Wsmprovhost.exe and DSROLE.dll

```
DeviceImageLoadEvents
| where InitiatingProcessFileName =~ "wsmprovhost.exe"
| where FileName =~ "DSROLE.dll"
| where not(FolderPath has_any("system32", "syswow64"))
```

Search order hijack using clip.exe and Version.dll

```
DeviceImageLoadEvents
| where InitiatingProcessFileName =~ "clip.exe"
| where FileName in~("version.dll")
| where not(FolderPath has_any("system32", "syswow64", "program
"trend micro"))
```

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.

Microsoft Sentinel also has a range of detection and threat hunting content that customers can use to detect the post exploitation activity detailed in this blog in addition to Microsoft 365 Defender detections list above.

- [PowerShell downloads](#)
- [Dumping LSASS Process into a File](#)
- [Anomalous Account Creation](#)
- [RDP Rare Connection](#)
- [Anomalous RDP Activity](#)

Indicators of compromise (IOCs)

The list below provides IOCs observed during our investigation. We encourage our customers to investigate these indicators in their environments and implement detections and protections to identify past related activity and prevent future attacks against their systems.

Diamond Sleet path 1

Indicator	Type	Description
C:\ProgramData\Forest64.exe	File path	File path of ForestTiger binary
e06f29dccfe90ae80812c2357171b5c48fba189ae103d28e972067b107e58795	SHA-256	Hash of Forest64.exe
0be1908566efb9d23a98797884f2827de040e4cedb642b60ed66e208715ed4aa	SHA-256	Hash of Forest64.exe
C:\ProgramData\4800-84DC-063A6A41C5C	File path	ForestTiger configuration file
hxxp://www.bandarpowder[.]com/public/assets/img/cfg.png	URL	Staging URL for 4800-84DC-063A6A41C5C (compromised domain)
hxxps://www.bandarpowder[.]com/public/assets/img/cfg.png	URL	Staging URL for 4800-84DC-063A6A41C5C (compromised domain)
hxxp://www.aeon-petro[.]com/wcms/plugins/addition_contents/cfg.png	URL	Staging URL for 4800-84DC-063A6A41C5C (compromised domain)
hxxp://www.bandarpowder[.]com/public/assets/img/user64.png	URL	Staging URL for Forest64.exe (compromised domain)
hxxps://www.bandarpowder[.]com/public/ass	URL	Staging URL for Forest64.exe

ets/img/user64.png		(compromised domain)
hxxp://www.aeon-petro[.]com/wcms/plugins/addition_contents/user64.png	URL	Staging URL for Forest64.exe (compromised domain)

Diamond Sleet path 2

Indicator	Type	Description
C:\ProgramData\DSROLE.dll	File path	File path of RollSling binary
d9add2bfdfebfa235575687de356f0cefb3e4c55964c4cb8bfdcdc58294eeaca	SHA-256	Hash of DSROLE.dll
C:\ProgramData\Version.dll	File path	File path of FeedLoad binary.
f251144f7ad0be0045034a1fc33fb896e8c32874e0b05869ff5783e14c062486	SHA-256	Hash of Version.dll
C:\ProgramData\readme.md	File path	Used as a multibyte XOR key for FeedLoad Next Stage
fa7f6ac04ec118dd807c1377599f9d369096c6d8fb1ed24ac7a6ec0e817eaab6	SHA-256	Hash of Readme.md
C:\ProgramData\wsmprovhost.exe	File path	Legitimate Windows binary is copied to this directory for DLL search-order hijacking
C:\ProgramData\clip.exe	File path	Legitimate Windows binary is copied to this directory for DLL search-order hijacking
dersmarketim[.]com	Domain	C2 domain (compromised

Indicator	Type	Description
		domain)
olidhealth[.]com	Domain	C2 domain (compromised domain)
galerielamy[.]com	Domain	C2 domain (compromised domain)
3dkit[.]org	Domain	C2 domain (compromised domain)
hxxp://www.mge[.]sn/themes/classic/modules/ps_rssfeed/feed.zip	URL	Staging URL for Version.dll (compromised domain)
hxxp://www.mge[.]sn/themes/classic/modules/ps_rssfeed/feedmd.zip	URL	Staging URL for readme.md (compromised domain)
hxxps://vadtalmandir[.]org/admin/ckeditor/plugins/icontact/about.php	URL	Callback URL from second-stage PE (compromised domain)
hxxps://commune-fraita[.]ma/wp-content/plugins/wp-contact/contact.php	URL	Callback URL from second-stage PE (compromised domain)

Onyx Sleet path

Indicator	Type	Description
C:\Windows\Temp\temp.exe	File path	File path for HazyLoad binary
C:\Windows\ADFS\bg\inetmgr.exe	File path	File path for HazyLoad binary
000752074544950ae9020a35ccd77de277f1cd5026b4b9559279dc3b86965eee	SHA-256	Hash of proxy tool loader

hxxp://147.78.149[.]201:9090/imgr.ico	URL	Staging URL for HazyLoad binary (compromised infrastructure)
hxxp://162.19.71[.]175:7443/bottom.gif	URL	Staging URL for HazyLoad binary (compromised infrastructure)

NOTE: These indicators should not be considered exhaustive for this observed activity.

References

- [Following the Lazarus group by tracking DeathNote campaign | Securelist](#)

Further reading

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: https://aka.ms/threatintelblog.

To get notified about new publications and to join discussions on social media, follow us on Twitter at https://twitter.com/MsftSecIntel.

Related Posts

Research **Threat intelligence** **Threat actors** ·

Sep 29, 2022 · 13 min read

ZINC weaponizing open-source software >

In recent months, Microsoft detected weaponization of legitimate open-source software by an actor the Microsoft Threat Intelligence Center (MSTIC) tracks as ZINC, targeting employees at media, defense and aerospace, and IT service provider organizations in the US, UK, India, and Russia.

Research **Threat intelligence** **Threat actors** ·

Jan 28, 2021 · 18 min read

ZINC attacks against security researchers >

In recent months, Microsoft has detected cyberattacks targeting security researchers by an actor we track as ZINC. Observed targeting includes pen testers, private offensive security researchers, and employees at security and tech companies.

Events **Threat trends** · **Nov 10, 2022** · **5 min read**

Microsoft threat intelligence presented at CyberWarCon 2022 ›

At CyberWarCon 2022, Microsoft and LinkedIn analysts presented several sessions detailing analysis across multiple sets of actors and related activity.

Research **Threat intelligence** **Threat actors** ·

Jul 14, 2022 · **13 min read**

North Korean threat actor targets small and midsize businesses with H0lyGh0st ransomware ›

A group of actors originating from North Korea that MSTIC tracks as DEV-0530 has been developing and using ransomware in attacks since June 2021. This group, which calls itself H0lyGh0st, utilizes a ransomware payload with the same name.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social

What's new

Surface Pro

Surface Laptop

Surface Laptop Studio 2

Surface Laptop Go 3

Microsoft Copilot

AI in Windows

Explore Microsoft products

Windows 11 apps

Business

Microsoft Cloud

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Developer & IT

Azure

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Company

Careers

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Microsoft 365 Copilot

Small Business

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy