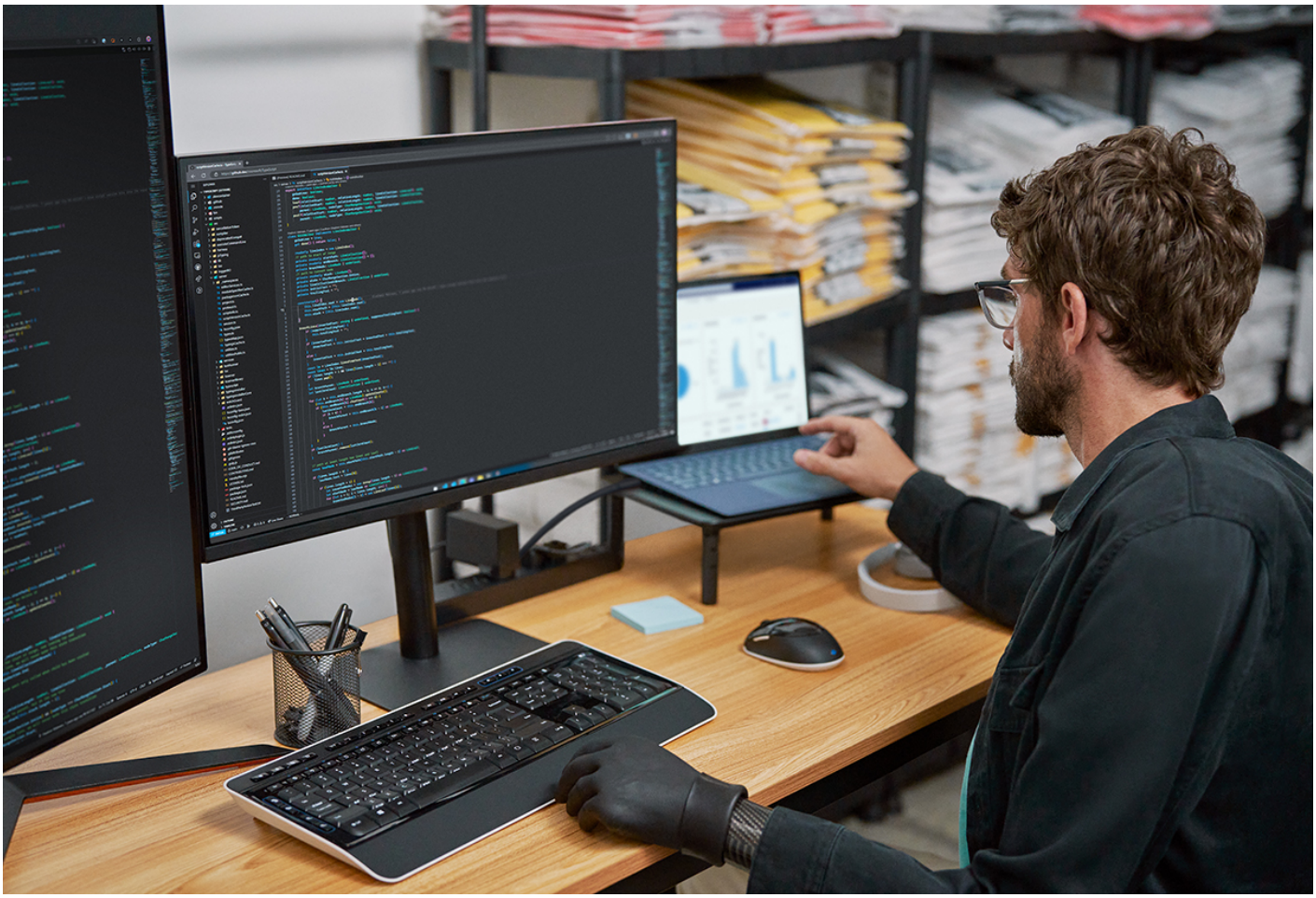
Diamond Sleet supply chain compromise distributes a modified CyberLink installer

⋮ 11/22/2023



- By Microsoft Threat Intelligence

Microsoft Threat Intelligence has uncovered a supply chain attack by the North Korea-based threat actor Diamond Sleet (ZINC) involving a malicious variant of an application developed by CyberLink Corp., a software company that develops multimedia software products. This malicious file is a legitimate CyberLink application installer that has been modified to include malicious code that downloads, decrypts, and loads a second-stage payload. The file, which was signed using a valid certificate issued to CyberLink Corp., is hosted on legitimate update infrastructure owned by CyberLink and includes checks to limit the time window for execution and evade detection by security products. Thus far, the malicious activity has impacted over 100 devices in multiple countries, including Japan, Taiwan, Canada, and the United States.

Microsoft attributes this activity with high confidence to Diamond Sleet, a North Korean threat actor. The second-stage payload observed in this campaign communicates with infrastructure that has been previously compromised by Diamond Sleet. More recently, Microsoft has observed Diamond Sleet utilizing trojanized open-source and proprietary software to target organizations in information technology, defense, and media.

To address the potential risk of further attacks against our customers, Microsoft has taken the following steps to protect customers in response to this malicious activity:

- Microsoft has communicated this supply chain compromise to CyberLink
- Microsoft is notifying Microsoft Defender for Endpoint customers that have been targeted or compromised in this campaign
- Microsoft reported the attack to GitHub, which removed the second-stage payload in accordance with its Acceptable Use Policies
- Microsoft has added the CyberLink Corp. certificate used to sign the malicious file to its disallowed certificate list
- Microsoft Defender for Endpoint detects this activity as Diamond Sleet activity group.
- Microsoft Defender Antivirus detects the malware as Trojan:Win32/LambLoad.

Microsoft may update this blog as additional insight is gained into the tactics, techniques, and procedures (TTPs) used by the threat actor in this active and ongoing campaign.

Who is Diamond Sleet?

The actor that Microsoft tracks as Diamond Sleet (formerly ZINC) is a North Korea-based activity group known to target media, defense, and information technology (IT) industries globally. Diamond Sleet focuses on espionage, theft of personal and corporate data, financial gain, and corporate network destruction. Diamond Sleet is known to use a variety of custom malware that is exclusive to the group. Recent Diamond Sleet malware is described in Microsoft's reporting of the group's weaponization of open source software and exploitation of N-day vulnerabilities. Diamond Sleet overlaps with activity tracked by other security companies as Temp.Hermit and Labyrinth Chollima.

DIAMOND SLEET (ZINC)

Learn about other recent activity

Activity overview

Microsoft has observed suspicious activity associated with the modified CyberLink installer file as early as October 20, 2023. The malicious file has been seen on over 100 devices in multiple countries, including Japan, Taiwan, Canada, and the United States. While Microsoft has not yet identified hands-on-keyboard activity carried out after compromise via this malware, the group has historically:

- Exfiltrated sensitive data from victim environments
- Compromised software build environments
- Moved downstream to additional victims for further exploitation
- Used techniques to establish persistent access to victim environments

Diamond Sleet utilized a legitimate code signing certificate issued to CyberLink Corp. to sign the malicious executable. This certificate has been added to Microsoft's disallowed certificate list to protect customers from future malicious use of the certificate:

Signer: CyberLink Corp.
Issuer: DigiCert SHA2 Assured ID Code Signing CA
SignerHash: 8aa3877ab68ba56dabc2f2802e813dc36678aef4
CertificateSerialNumber: 0a08d3601636378f0a7d64fd09e4a13b

Microsoft currently tracks the malicious application and associated payloads as LambLoad.

LambLoad

LambLoad is a weaponized downloader and loader containing malicious code added to a legitimate CyberLink application. The primary LambLoad loader/downloader sample Microsoft identified has the SHA-256 hash 166d1a6ddcde4e859a89c2c825cd3c8c953a86bfa92b343de7e5bfbfb5afb8be.

Before launching any malicious code, the LambLoad executable ensures that the date and time of the local host align with a preconfigured execution period.

```
Time = _time64(0);
tm0 = _localtime64(&Time);
time64_t0 = unknown_libname_5(tm0);
tm1 = _gmtime64(&Time);
if ( time64_t0 - (unsigned int)unknown_libname_5(tm1) == 19800 )
{
  tm2 = _localtime64(&Time);
  if ( tm2->tm_wday == 2 && tm2->tm_hour == 11 )
  {
    tm_min = tm2->tm_min;
    if ( tm_min >= 30 && tm_min < 60 )
    {
```

Figure 1. Code for checking date and time of local host

The loader then targets environments that are not using security software affiliated with FireEye, CrowdStrike, or Tanium by checking for the following process names:

- *csfalconservice.exe* (CrowdStrike Falcon)
- *xagt.exe* (FireEye agent)
- *taniumclient.exe* (Tanium EDR solution)

If these criteria are not met, the executable continues running the CyberLink software and abandons further execution of malicious code. Otherwise, the software attempts to contact one of three URLs to download the second-stage payload embedded inside a file masquerading as a PNG file using the static User-Agent ‘Microsoft Internet Explorer’:

- *hxxps[:]//i.stack.imgur[.]com/NDTUM.png*
- *hxxps[:]//www.webville[.]net/images/CL202966126.png*
- *hxxps[:]//cldownloader.github[.]io/logo.png*

The PNG file contains an embedded payload inside a fake outer PNG header that is, carved, decrypted, and launched in memory.

```
while ( numTries < 3 );
cryptSize = nBuffSize - 0x3937F;
decPayload1 = operator new[](nBuffSize - 0x3937F);
cryptData1 = cryptData0;
decPayload0 = decPayload1;
memmove(decPayload1, (char *)cryptData0 + 0x39373, cryptSize);
if ( cryptData1 )
  j__free(cryptData1);
for ( i = cryptSize - 1; i >= 0; --i )
{
  if ( (i & 3) == 0 )
    --decPayload0[i];
  if ( i )
    decPayload0[i] -= decPayload0[i - 1];
  decPayload0[i] ^= 0x59u;
}
if ( *decPayload0 == 'M' && decPayload0[1] == 'Z' )
  f_bootstrap_payload(decPayload0, cryptSize, 0);
j__free(decPayload0);
return 0;
```

Figure 2. Payload embedded in PNG file

When invoked, the in-memory executable attempts to contact the following callbacks for further instruction. Both domains are legitimate but have been compromised by Diamond Sleet:

- *hxxps[:]//mantis.jancom[.]pl/bluemantis/image/addon/addin.php*
- *hxxps[:]//zeduzeventos.busqueabuse[.]com/wp-admin/js/widgets/sub/wids.php*

The crypted contents of the PNG file (SHA-256: 089573b3a1167f387dcdad5e014a5132e998b2c89bff29bcf8b06dd497d4e63d) may be manually carved using the following command:

```
dd if=logo.png bs=1 skip=$[0x39373] of=crypt.bin count=$[0x79a00]
```

To restore the in-memory payload statically for independent analysis, the following Python script can be used to decrypt the carved contents.

```
#!/usr/bin/python
import sys

buff = bytearray(sys.stdin.buffer.read())

for i in range(len(buff) - 1, -1, -1):
    if (i & 3) == 0:
        buff[i] = buff[i] - 1 & 0xff
    if i:
        buff[i] = (buff[i] - buff[i - 1]) & 0xff
    buff[i] ^= 0x59

sys.stdout.buffer.write(buff)
```

To crypt and verify:

```
cat crypt.bin | python poc.py > dec.bin

file dec.bin
dec.bin: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

sha256sum dec.bin
915c2495e03ff7408f11a2a197f23344004c533ff87db4b807cc937f80c217a1  dec.bin
```

Both the fake PNG and decrypted PE payload have been made available on VirusTotal.

Recommendations

Microsoft recommends the following mitigations to reduce the impact of this threat. Check the recommendations card for the deployment status of monitored mitigations.

- Use Microsoft Defender Antivirus to protect from this threat. Turn on cloud-delivered protection and automatic sample submission on Microsoft Defender Antivirus. These capabilities use artificial intelligence and machine learning to quickly identify and stop new and unknown threats.
- Enable network protection to prevent applications or users from accessing malicious domains and other malicious content on the internet.
- Enable investigation and remediation in full automated mode to allow Microsoft Defender for Endpoint to take immediate action on alerts to resolve breaches, significantly reducing alert volume.
- 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 data integrity with hash codes.
- Turn on the following attack surface reduction rule: Block executable files from running unless they meet a prevalence, age, or trusted list criterion.

Detection details

Microsoft Defender Antivirus

Microsoft Defender Antivirus detects threat components as the following malware:

- Trojan:Win32/LambLoad.A!dha
- Trojan:Win32/LambLoad.B!dha
- Trojan:Win32/LambLoad.C!dha
- Trojan:Win64/LambLoad.D!dha
- Trojan:Win64/LambLoad.E!dha

Microsoft Defender for Endpoint

Alerts with the following title in the security center can indicate threat activity on your network:

- Diamond Sleet activity group

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

- An executable loaded an unexpected dll

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

Microsoft Defender XDR Threat analytics

Hunting queries

Microsoft Defender XDR

Microsoft Defender XDR (formerly Microsoft 365 Defender) customers can run the following query to find related activity in their networks:

```
let iocs = dynamic(["166d1a6ddcde4e859a89c2c825cd3c8c953a86bfa92b343de7e5bfbfb5afb8be",
"089573b3a1167f387dcdad5e014a5132e998b2c89bff29bcf8b06dd497d4e63d",
"915c2495e03ff7408f11a2a197f23344004c533ff87db4b807cc937f80c217a1"]);
DeviceFileEvents
| where ActionType == "FileCreated"
| where SHA256 in (iocs)
| project Timestamp, DeviceName, FileName, FolderPath, SHA256
```

Microsoft Defender XDR and Microsoft Sentinel

This query can be used in both Microsoft Defender XDR advanced hunting and Microsoft Sentinel Log Analytics. It surfaces devices where the modified CyberLink installer can be found.

```
DeviceFileCertificateInfo
| where Signer contains "CyberLink Corp"
```

```
| where CertificateSerialNumber == "0a08d3601636378f0a7d64fd09e4a13b"

| where SignerHash == "8aa3877ab68ba56dabc2f2802e813dc36678aef4"

| join DeviceFileEvents on SHA1

| distinct DeviceName, FileName, FolderPath, SHA1, SHA256, IsTrusted, IsRootSignerMicrosoft, SignerHash
```

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.

The following YAMLs contain queries that surface activities related to this attack:

Indicators of compromise

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.

Indicator	Type	Description
166d1a6ddcde4e859a89c2c825cd3c8c953a86bfa92b343de7e5bfbfb5afb8be	SHA-256	Trojanized CyberLink installer (LambLoad)
089573b3a1167f387dcdad5e014a5132e998b2c89bff29bcf8b06dd497d4e63d	SHA-256	Second-stage PNG payload
915c2495e03ff7408f11a2a197f23344004c533ff87db4b807cc937f80c217a1	SHA-256	Decrypted PE from second-stage PNG
hxxps[:]//update.cyberlink[.]com/Retail/Promeo/RDZCMSFY1ELY/CyberLink_Promeo_Downloader.exe	URL	CyberLink update URL used to deliver malicious installer
hxxps[:]//update.cyberlink[.]com/Retail/Patch/Promeo/DL/RDZCMSFY1ELY/CyberLink_Promeo_Downloader.exe	URL	CyberLink update URL used to deliver malicious installer
hxxps[:]//cldownloader.github[.]io/logo.png	URL	Stage 2 staging URL
hxxps[:]//i.stack.imgur[.]com/NDTUM.png	URL	Stage 2 staging URL
hxxps[:]//www.webville[.]net/images/CL202966126.png	URL	Stage 2 staging URL

Indicator	Type	Description
hxxps[:]//mantis.jancom[.]pl/bluemantis/image/addon/addin.php	URL	Stage 2 callback URL
hxxps[:]//zeduzeventos.busqueabuse[.]com/wpadmin/js/widgets/sub/wids.php	URL	Stage 2 callback url