BatLoader Continues Signed MSIX App Package Abuse

esentire.com/blog/batloader-continues-signed-msix-app-package-abuse

What We Do

eSentire MDR for Microsoft

Visibility and response across your entire Microsoft security ecosystem.

Learn More →

Resources

TRU Intelligence Center

Our Threat Response Unit (TRU) publishes security advisories, blogs, reports, industry publications and webinars based on its original research and the insights driven through proactive threat hunts.

EXPLORE RESOURCES →

Company

ABOUT ESENTIRE

eSentire is The Authority in Managed Detection and Response Services, protecting the critical data and applications of 2000+ organizations in 80+ countries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events.

About Us →

Leadership →

Careers →

EVENT CALENDAR

Sep

13

Cyber Security Summit Philadelphia

Sep

13

AppDirect Chicago Academy

Sep

17

Midsize Enterprise Fall Summit Houston

View Calendar →

Partners

PARTNER PROGRAM

LEARN MORE →

Apply to become an e3 ecosystem partner with eSentire, the Authority in Managed Detection and Response.

APPLY NOW →

Login to the Partner Portal for resources and content for current partners.

LOGIN NOW →

Get Started

Want to learn more on how to achieve Cyber Resilience?

TALK TO AN EXPERT

Adversaries don't work 9-5 and neither do we. At eSentire, our 24/7 SOCs are staffed with Elite Threat Hunters and Cyber Analysts who hunt, investigate, contain and respond to threats within minutes.

We have discovered some of the most dangerous threats and nation state attacks in our space – including the Kaseya MSP breach and the more_eggs malware.

Our Security Operations Centers are supported with Threat Intelligence, Tactical Threat Response and Advanced Threat Analytics driven by our Threat Response Unit – the TRU team.

In TRU Positives, eSentire's Threat Response Unit (TRU) provides a summary of a recent threat investigation. We outline how we responded to the confirmed threat and what recommendations we have going forward.

Here's the latest from our TRU Team…

What did we find?

In July, the eSentire Threat Response Unit (TRU) identified multiple BatLoader cases investigated by our SOC team. In these cases, the victims fell for suspected malicious advertisements impersonating Zoom and TradingView after performing web searches for

these products.

The victims had then downloaded malicious MSIX installer files (such as Zoom-x64.msix) which attempted to infect their systems with Redline Stealer and SectopRAT. These were the first such observations in our telemetry since May 2023. Our analysis here will focus on discovering imposter websites and MSIX samples currently being used in BatLoader campaigns.

BatLoader Imposter Sites Registered on June - July 2023

TRU identified several suspected BatLoader payload sites hosted on IP 80.68.159.10 registered in June and July 2023:

- tradling-view[.]com
- get-adobe[.]net
- zooml-us[.]com
- open-aii[.]com
- mldiourney[.]com
- store-steampowered[.]net
- mlcrosoft-online[.]net
- qul-cken[.]com

The domain names suggest an array of brands are impersonated in these attacks, including Microsoft, Zoom, Adobe, Steam, OpenAI, etc. (a more complete list can be found at the end of this blog). These brands have been used historically in previous BatLoader attacks, and landing pages comprise of an imposter download page for these products.

When visited manually, these sites present empty content or 403 HTTP errors, and successful recreation of infection chains has been minimal thus far. This may suggest operators may have improved the cloaking of these sites to evade discovery by researchers and scanners.

We did identify one successfully rendered page for Steam (store-steampowered[.]net) submitted to Urlscan.io on June 6, which shows an imposter page for the gaming service. The website was registered the same day and served a legitimate Steam binary at the time.

Figure 1 Imposter page for Steam, retrieved from Urlscan.io.

We assess this site likely served Steam-x64.msix (md5: c37aee1ebad9b0f7bd2e7755a3133d0e) in mid-July 2023 shown in Figure 2 below.

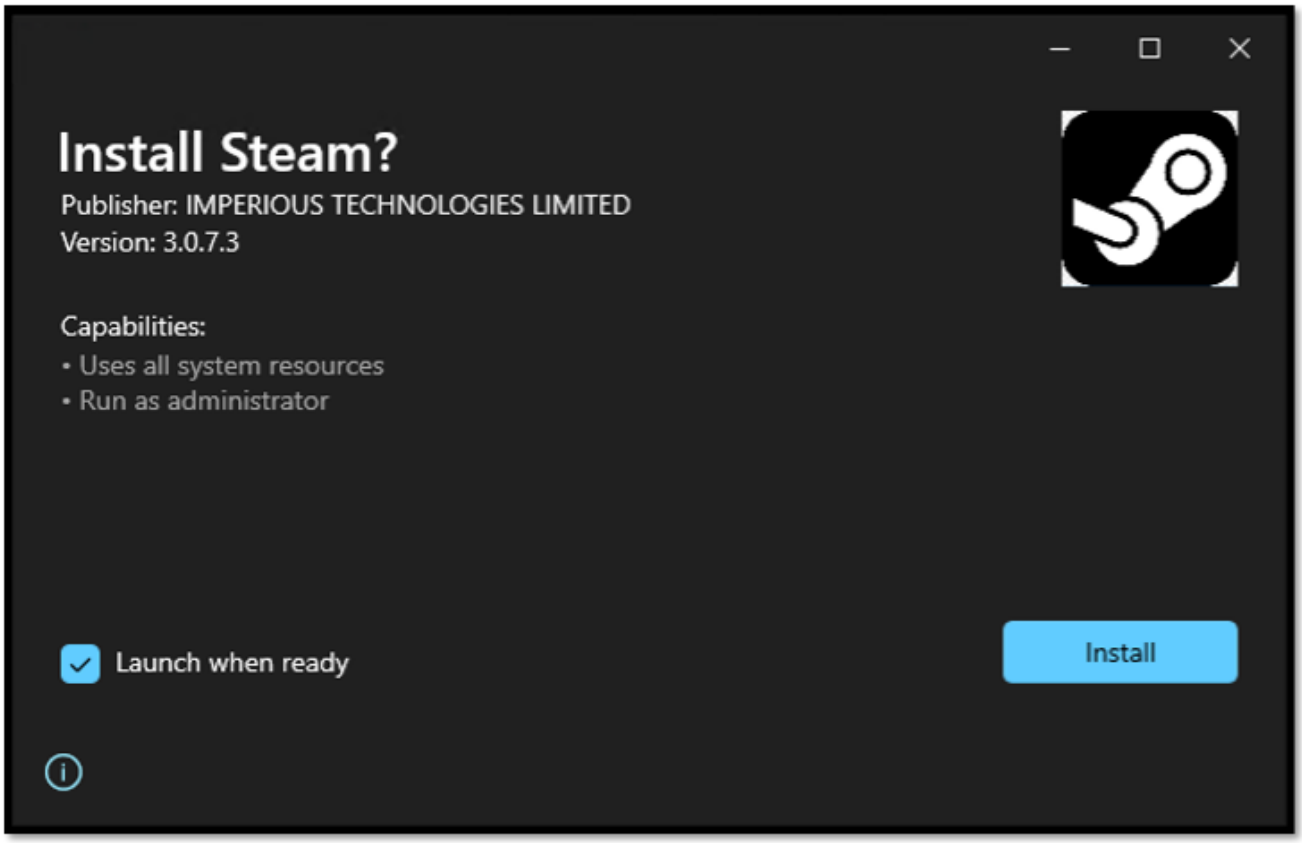

Figure 2 MSIX app launch. File is signed and asks for elevated privileges.

BatLoader Continues to Abuse Signed MSIX Packages

As we covered in our May blog, MSIX files are a relatively new installer format designed for Windows 10 and above. It requires the package contents to be signed; a barrier intended to limit abuse by threat actors. Unfortunately, these code signing certificates do find their way into threat actor hands and can be acquired on underground forums for a fee.

In a February post on XSS forums, a suspected BatLoader operator vouched for a code signing service offered by another forum member by providing a screenshot of their previous transaction with this member:

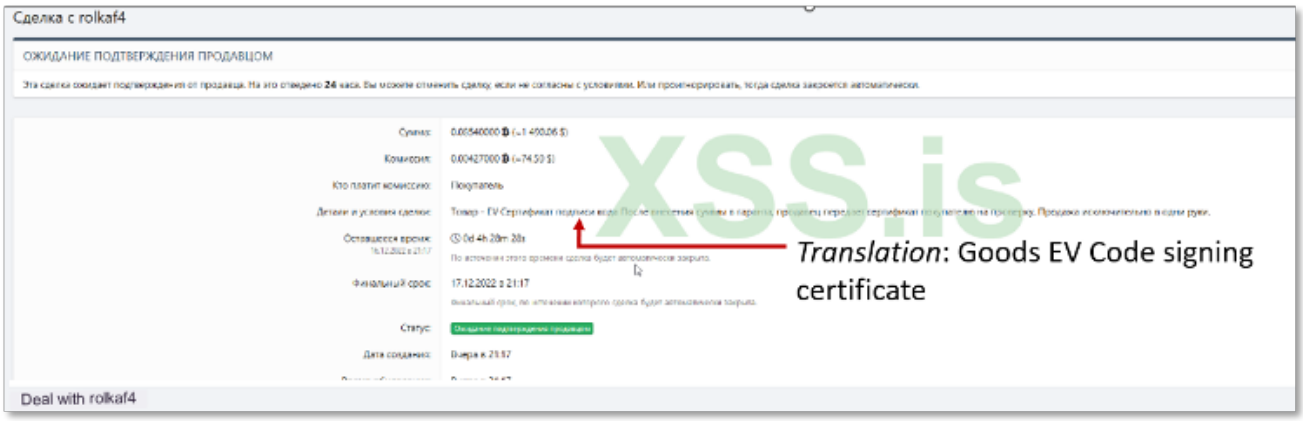

Figure 3 Suspected BatLoader operator's image posted to XSS in February 2023. The image

purports to be the purchase of a code signing certificate from another forum member.

It's highly probable that BatLoader operators are purchasing the required code signing certificates used in their campaigns from other threat actors.

The latest MSIX app packages reviewed by TRU contained content signed by IMPERIOUS TECHNOLOGIES LIMITED, a private limited company based out of the UK.

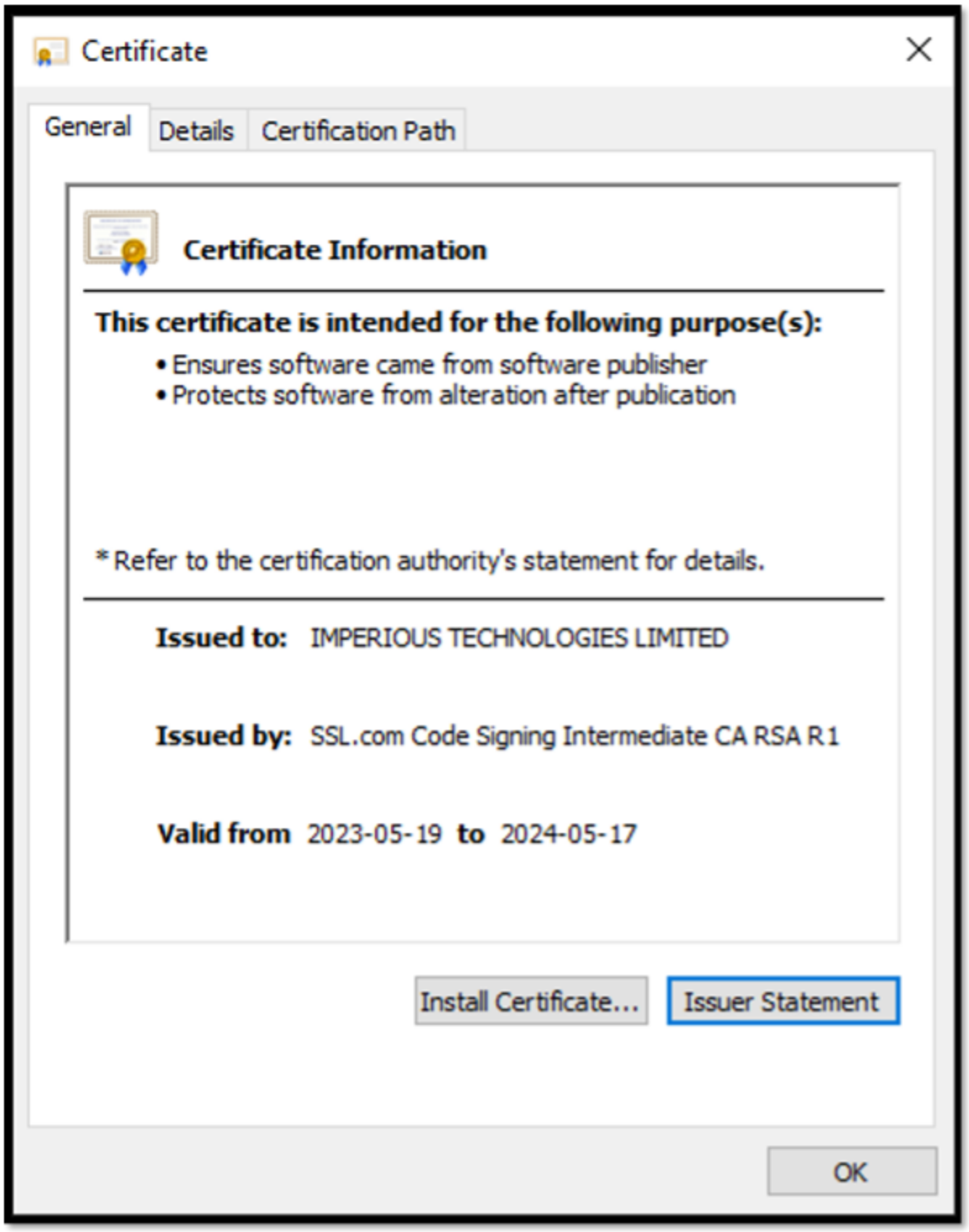

Figure 4 Steam-x64.msix digital signature.

The AppManifest shows the package was created with Advanced Installer version 20.2 configured with Russian-language settings.

When launched, the package executes with elevated privileges then executes an embedded PowerShell script then drops and executes a legitimate copy of the Steam installer as a decoy. The PowerShell script (“NEW_mormons_v1.ps1”, MD5: d87bc0bcfa1976ffa6a165545fb7ca62) contains a similar structure to prior samples, with some minor updates. It downloads Redline Stealer binary disguised as a jpg file (“czx.jpg”, MD5: d5a1d54158e110a8d9b0eea06d37e26f) from hxxps://tatmacerasi[.]com and SectopRAT/ArechClient (“zhelp.exe”, MD5: 3AC860860707BAAF32469FA7CC7C0192) from hxxps://fullpower682[.]store.

Additional details on the PowerShell script can be seen in the annotated image below.

Figure 5 PowerShell script "NEW_mormons_v1.ps1" with annotations.

Similarities with prior BatLoader samples include:

- MSIX created with Advanced Installer v. 20.2 with Russian language option

- Decoy executable
- PowerShell execution via signed MSIX
- PowerShell behavior:
    - One or more execution delays via sleep command
    - Connect to C2 to signal “start”
    - Download payload from URL ending in .jpg
    - Connect to C2 to signal “install”
    - Load payload assembly using PowerShell

A May PowerShell sample for comparison:

Figure 6 May 2023 PowerShell sample. See https://www.esentire.com/blog/batloader-impersonates-midjourney-chatgpt-in-drive-by-cyberattacks

Payloads

SectopRAT is downloaded as an encrypted RAR archive and decrypted using 7zip (also downloaded). The SectopRAT payload (MD5: DD50DE3ACC26293986F40EB04F0F1A99) is written to AppData\Local\Temp\ and injected into MsBuild.exe. It retrieves its C2 configuration from Pastebin and connects to 194.26.135[.]180 for command and control.

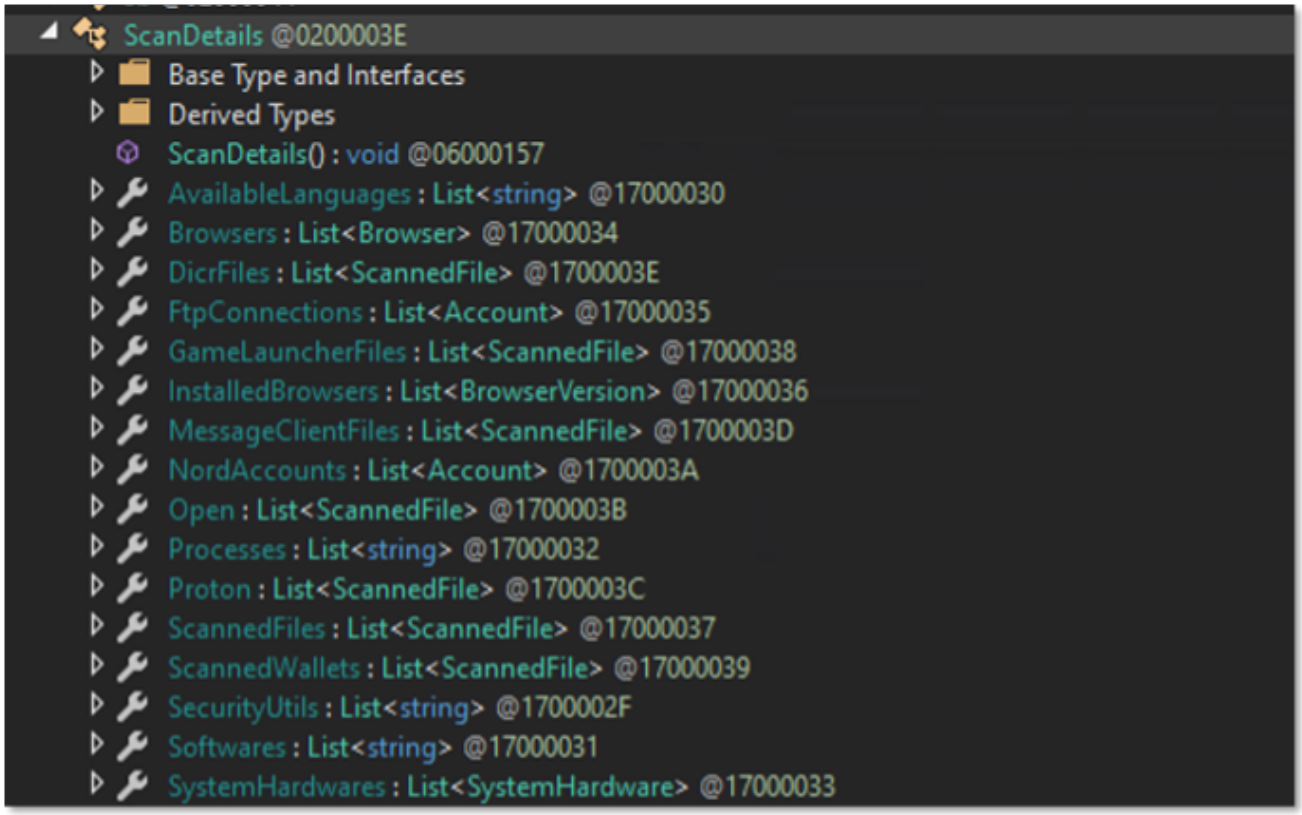

Figure 7 SectopRAT seen in debugging tool showing the ScanDetails class and various properties related to information collected from the target system.

Redline Stealer is loaded as assembly by PowerShell, with the resulting payload (MD5: D5A1D54158E110A8D9B0EEA06D37E26F) connecting to 194.26.135[.]119 port 12432 for command-and-control.

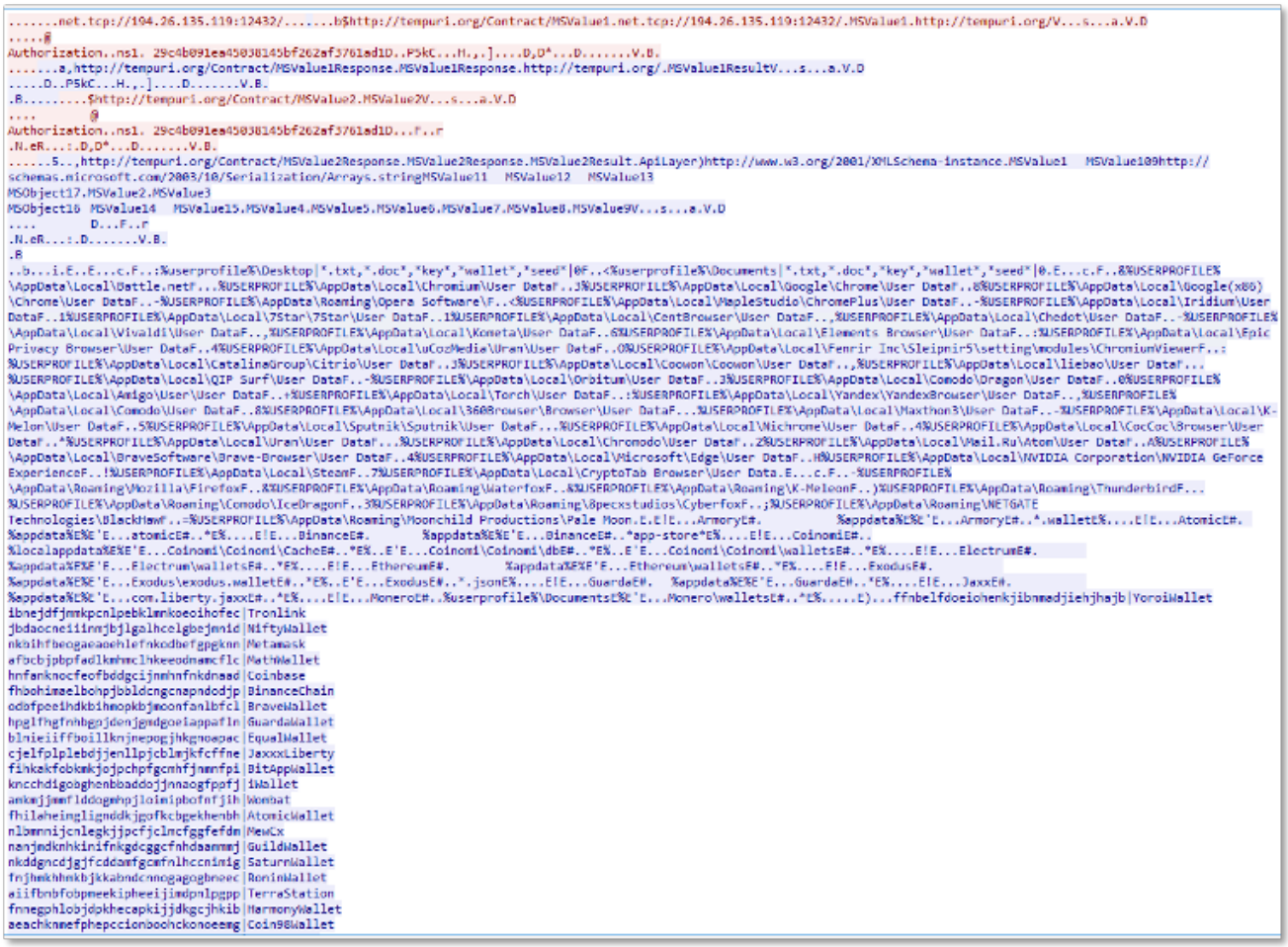

Figure 8 Snippet of Redline Stealer network traffic.

For a complete analysis of another Redline sample, read our Redline Stealer malware analysis.

How did we find it?

MDR for Endpoint identified MSIX activity and blocked subsequent behavior.

What did we do?

Our team of 24/7 SOC Cyber Analysts isolated the host and alerted the customer while an investigation took place before remediating the threat.

What can you learn from this TRU positive?

- Imposter sites distributed via ad platforms (such as Google Ads) have diminished since the start of 2023 but remain a concern. It's probable these ad services have improved their processes to tamp down on abuse, but it's also apparent that threats like BatLoader have improved their tradecraft to circumvent these controls.

- Targeted brands include products and services commonly found in business environments. Infected, domain-joined systems offer more value for data theft and follow-on intrusion attacks (e.g. ransomware).
    Both Redline and SectopRAT provide a foundation to monetize infected assets and exploit them for further intrusion actions.
- Signed code is a barrier that can be circumvented. Code signing certificate services can be acquired from criminal forums for a fee; BatLoader has likely used these services to sign MSIX packages.
- Suspicious MSIX execution can be identified by monitoring for PowerShell (or other script formats) execution under aistubx64.exe.
    For example: svchost.exe -> aistubx64.exe -> PowerShell.exe

Recommendations from our Threat Response Unit (TRU):

- Protect endpoints against malware by:
    - Ensuring antivirus signatures are up-to-date.
    - Using a Next-Gen AV (NGAV) or Endpoint Detection and Response (EDR) tool to detect and contain threats.
- Raise awareness of malware masquerading as legitimate applications, and include in your Phishing and Security Awareness Training (PSAT) program. An effective PSAT program emphasizes building cyber resilience by increasing risk awareness, rather than trying to turn everyone into security experts.
- Windows Defender Application Control provides options for managing packaged apps (MSIX).

Indicators of Compromise

Indicator	Note
tradling-view[.]com	Suspected BatLoader Imposter Sites
www[.]adlobe[.]net	
www[.]get-adobe[.]net	
adlobe[.]net	
get-adobe[.]net	
www[.]drlve-googie[.]com	
www[.]zooml-us[.]com	
drlve-googie[.]com	

usblank[.]net	
zooml-us[.]com	
open-aii[.]com	
so-lfi[.]com	
virtuaibox[.]net	
mldiourney[.]com	
blt-warden[.]com	
store-steampowered[.]net	
mlcrosoft-online[.]net	
qul-cken[.]com	
fileziila-project[.]com	
www.whcts-app[.]com	
www.notcpad-pius-pius[.]org	
623start[.]site	BatLoader C2 (confirmed)
cdn-prok[.]site	BatLoader C2 (suspected)
cdn-dwnld[.]ru	
start-up-plus[.]site	
newvision623[.]site	
cdn-dwnld[.]site	
cdn-dwnld[.]store	
tatmacerasi[.]com	Secondary Payload Host
fullpower682[.]store	Secondary Payload Host
194.26.135[.]180	SectopRAT C2
194.26.135[.]119	Redline C2
C37AEE1EBAD9B0F7BD2E7755A3133D0E	Steam-x64.msix
D87BC0BCFA1976FFA6A165545FB7CA62	NEW_mormons_v1.ps1

D5A1D54158E110A8D9B0EEA06D37E26F	czx.jpg
3AC860860707BAAF32469FA7CC7C0192	zhelp.exe
DD50DE3ACC26293986F40EB04F0F1A99	SectopRAT
D5A1D54158E110A8D9B0EEA06D37E26F	Redline

eSentire Threat Response Unit (TRU)

Our industry-renowned Threat Response Unit (TRU) is an elite team of threat hunters and researchers, that supports our 24/7 Security Operations Centers (SOCs), builds detection models across our Atlas XDR Cloud Platform, and works as an extension of your security team to continuously improve our Managed Detection and Response service. TRU has been

recognized for its threat hunting, original research and content development capabilities. TRU is strategically organized into cross-functional groups to protect you against advanced and emerging threats, allowing your organization to gain leading threat intelligence and incredible cybersecurity acumen.