

Scenario:

You are part of the Threat Intelligence team in the SOC (Security Operations Center). An executable file has been discovered on a colleague's computer, and it's suspected to be linked to a Command and Control (C2) server, indicating a potential malware infection. Your task is to investigate this executable by analyzing its hash. The goal is to gather and analyze data beneficial to other SOC members, including the Incident Response team, to respond to this suspicious behavior efficiently.

Question asks what category of malware belongs to the provided hash. There are several ways to determine this, but the most straightforward is to input the hash into **VirusTotal** or a similar website. After doing so you will find the answer.

The screenshot shows the VirusTotal analysis page for the file hash 248fc901aff4e4b4c48c91e4d78a939bf681c9a1bc24addc3551b32768f907b. The main summary indicates a community score of 61/75, with 61 out of 75 security vendors flagging the file as malicious. The file is identified as WEXTRACT.EXE.MUI. Below the summary, there are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (16). The DETAILS tab is selected, showing threat categories like trojan and trojan/criffi/stealer, and family labels like criffi and stealer. A table titled "Security vendors' analysis" lists various vendors and their findings. The table includes columns for vendor name, threat type, and vendor-specific names. For example, AhnLab-V3 found a Dropper/Win.Generic.X!2198, while BitDefender found a Gen:Heur.Criffi.1. Alibaba, Antiy-AVL, Avast, Avira (no cloud), and Bkav Pro also analyzed the file. The table shows a total of 16 detections across different vendors.

Question 1 Answer: Trojan

Question 2: Next, we need to find the name of the file. I stayed on **VirusTotal** and navigated to the **Details** section, where I located the file name.

Names

Wextract

WEXTRACT.EXE .MUI
248ffcc901aff4e4b4c48c91e4d78a939bf681c9a1bc24addc3551b32768f907b.exe
red.exe
18cbe5c5c3b28754916f1cbf4dfc95cf9.exe
NEAS.248ffcc901aff4e4b4c48c91e4d78a939bf681c9a1bc24addc3551b32768f907b.exe

Question 2 Answer: Wextract

Question 3: The third question requires finding when this malware was first seen. Again, I remained on **VirusTotal**, and under the **Details** tab, I found the answer in the **History** section.

History	
Creation Time	2022-05-24 22:49:06 UTC
First Submission	2023-10-06 04:41:50 UTC
Last Submission	2024-07-18 23:57:38 UTC
Last Analysis	2024-08-10 15:49:02 UTC

Question 3 Answer: 2023-10-06 04:41:50 UTC

Question 4: This question involved identifying the MITRE ATT&CK technique ID for the malware's data collection before exfiltration. To find this, I moved to the **Behavior** tab on **VirusTotal** and located the relevant information under the **MITRE ATT&CK Tactics and Techniques** section.

MITRE ATT&CK Tactics and Techniques

- + Execution TA0002
- + Persistence TA0003
- + Privilege Escalation TA0004
- + Defense Evasion TA0005
- + Credential Access TA0006
- + Discovery TA0007
- Collection TA0009
 - Data from Local System T1005
(Process #14) appaunch.exe searches for sensitive data of web browser "Comodo IceDragon" by file.
 - Input Capture T1056
Creates a DirectInput object (often for capturing keystrokes)
 - Automated Collection T1119
(Process #14) appaunch.exe searches for sensitive data of web browser "Comodo IceDragon" by file.
- + Command and Control TA0011
- + Impact TA0034
- + Impact TA0040

Question 4 Answer: T1005

Question 5: For this question, I was asked to find the domain name resolutions performed by the malware. I explored the **Behavior** tab and found the **Network Communication** section. After identifying the domains, I cross-referenced them on **VirusTotal** to check if any were flagged as malicious.

Network Communication

HTTP Requests

- + GET https://accounts.youtube.com:443/accounts/CheckConnection?pmo=https%3A%2F%2Faccounts.google.com&v=-198239029×tamp=1696494601857 200
- + GET https://connect.facebook.net:443/security/hsts-pixel.gif 200
- + GET https://facebook.com:443/security/hsts-pixel.gif?c=3.2.5 302
- + GET https://fcdn.net:443/security/hsts-pixel.gif?c=2.5 302
- + GET https://fsbx.com:443/security/hsts-pixel.gif?c=5 302
- + GET https://fonts.gstatic.com:443/s/googlesans/v14/4UaGrENHsxJlGDuGo1OllLU94YtzCwA.woff 200
- + GET https://fonts.gstatic.com:443/s/googlesans/v14/4UabrENHsxJlGDuGo1OllLU94YtzCwA.woff 200
- + GET https://fonts.gstatic.com:443/s/roboto/v18/KFOkCnqEu92Fr1MmgVxIizQ.woff 200

Question 5 Answer: Facebook.com

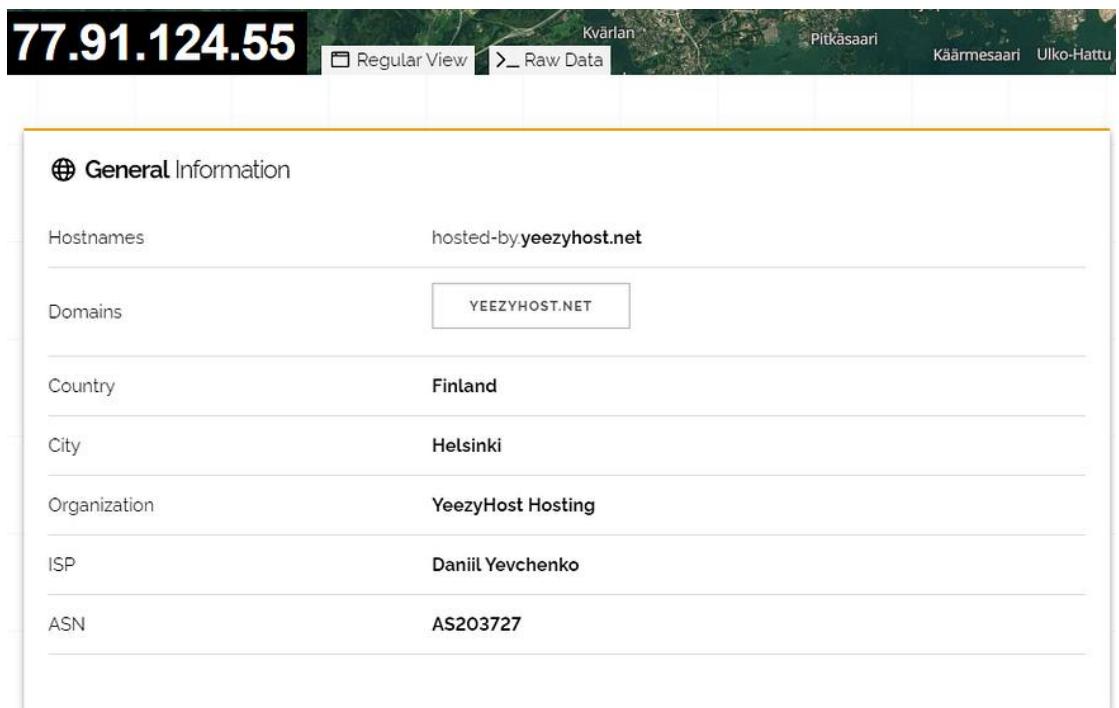
Question 6: This question sought the IP and Port that the malware is communicating with. I stayed in the **Behavior** tab and found the answer in the **IP Traffic** section. I further investigated the contacted IPs on **VirusTotal**, discovering that some were associated with C2 operations by malware like Amadey and Redline.

IP Traffic

- TCP 77.91.124.55:19071
- TCP 31.13.67.35:443 (www.facebook.com)
- TCP 13.107.6.158:443 (business.bing.com)
- TCP 23.48.246.145:443 (bzib.nelreports.net)
- TCP 31.13.88.13:443 (static.xx.fbcdn.net)
- TCP 31.13.88.35:443 (fsbx.com)
- TCP 13.107.253.41:443 (edge-consumer-static.azureedge.net)
- UDP 31.13.88.13:443 (static.xx.fbcdn.net)
- UDP 31.13.67.35:443 (www.facebook.com)
- UDP 31.13.88.35:443 (fsbx.com)

Question 6 Answer: 77.91.124.55:19071

Question 7 (This question was later removed I am keeping it here but the new question 7 is next): Originally, I was asked to find the hosting provider. I would have done this by using **Shodan** to analyze the IP. However, this question was later removed



The screenshot shows the Shodan search interface. At the top, the IP address "77.91.124.55" is displayed in large white text on a black background. Below it are two buttons: "Regular View" and "Raw Data". To the right of the IP are several location names: Kvarlan, Pitkasaari, Käärmesaari, and Ulko-Hattu. The main content area is titled "General Information" and contains the following data:

General Information	
Hostnames	hosted-by yeezyhost.net
Domains	YEEZYHOST.NET
Country	Finland
City	Helsinki
Organization	YeezyHost Hosting
ISP	Daniil Yevchenko
ASN	AS203727

Question 7 Answer: Yeezyhost

Question 7: This question asked me to find the YARA rule created by **Varpos** that can detect and identify the malware. To do this, I searched for the SHA-256 hash on **MalwareBazaar** and located the YARA signature in the **YARA Signatures** section.

YARA Signatures

MalwareBazaar uses YARA rules from several public and non-public repositories, such as [Malpedia](#). Those are being matched against malware samples uploaded to MalwareBazaar as well as against any suspicious process dumps they may create. Please note that only results from **TLP:WHITE** rules are being displayed.

Rule name:	detect_Redline_Stealer ⚠ Alert ▾
Author:	Varpos
Rule name:	INDICATOR_EXE_Packed_ConfuserEx ⚠ Alert ▾
Author:	ditekSHen
Description:	Detects executables packed with ConfuserEx Mod
Rule name:	NET ⚠ Alert ▾
Author:	malware-lu

Question 7 Answer: *detect_Redline_Stealer*

Question 8: For this question, I needed to determine the alias for the malware. I utilized **ThreatFox**, searching “ioc:*ip_address*” and then find the section labeled **Malware Alias** to find the answer.

IOC ID:	1167880
IOC:	77.91.124.55:19071
IOC Type ⓘ:	ip:port
Threat Type ⓘ:	botnet_cc
Malware:	RedLine Stealer
Malware alias:	RECORDSTEALER
Confidence Level ⓘ:	Confidence level is high (100%)
ASN:	AS701 UUNET
Country:	US
First seen:	2023-09-27 01:05:23 UTC
Last seen:	2023-10-03 15:07:51 UTC
UUID:	e1fc3ad6-5cd1-11ee-ab4a-42010aa4000a
Reporter ⓘ:	abuse_ch
Reward ⓘ:	10 credits from edwardcode
Tags:	RedLineStealer

Question 8 Answer: RECORDSTEALER

Question 9: Finally, I was tasked with identifying the DLL that the malware uses for privilege escalation. I returned to **VirusTotal**, examined the **Runtime Modules** section under the **Behavior** tab, and identified several DLLs. I then researched each one to determine which was commonly used for privilege escalation, ultimately finding the correct answer.

Modules loaded ⓘ

Runtime Modules

- APPHELP.DLL
- %SAMPLEPATH%\WEXTRACT.EXE.exe
- %USERPROFILE%\AppData\Local\Temp\IXP000.TMP\Yt8ge85.exe
- %USERPROFILE%\AppData\Local\Temp\IXP001.TMP\GY4IC43.exe
- %USERPROFILE%\AppData\Local\Temp\IXP002.TMP\hE8Zq97.exe
- %USERPROFILE%\AppData\Local\Temp\IXP003.TMP\1Zn59od7.exe
- 1Zn59od7.exe
- advapi32
- **advapi32.dll**
- advpack.dll
- api-ms-win-core-datetime-l1-1-1
- api-ms-win-core-fibers-l1-1-0
- api-ms-win-core-fibers-l1-1-1
- api-ms-win-core-localization-l1-2-1
- api-ms-win-core-localization-obsolete-l1-2-0
- api-ms-win-core-localregistry-l1-1-0.dll
- api-ms-win-core-string-l1-1-0
- api-ms-win-core-synch-l1-2-0
- api-ms-win-security-lsalookup-l1-1-0.dll
- rformar32.dll

Question 9 Answer: *advapi32.dll*

BY: Asad Dafalla