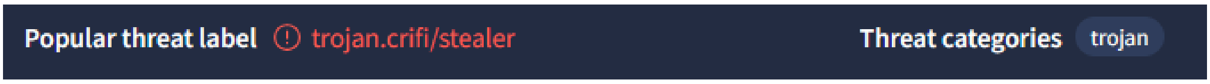
CyberDefenders: Red Stealer Lab

The following writeup is for Red Stealer Lab on CyberDefenders, it involves investigating a given file hash.

Scenario: You are part of the Threat Intelligence team in the SOC (Security Operations Cnetre). 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.

Categorising malware allows for a quicker and easier understanding of the malware, aiding in understanding its distinct behaviours and attack vectors. What's the identified malware's category?

If we enter the given SHA256 hash into VirusTotal, we can see that malware is categories as a Trojan:

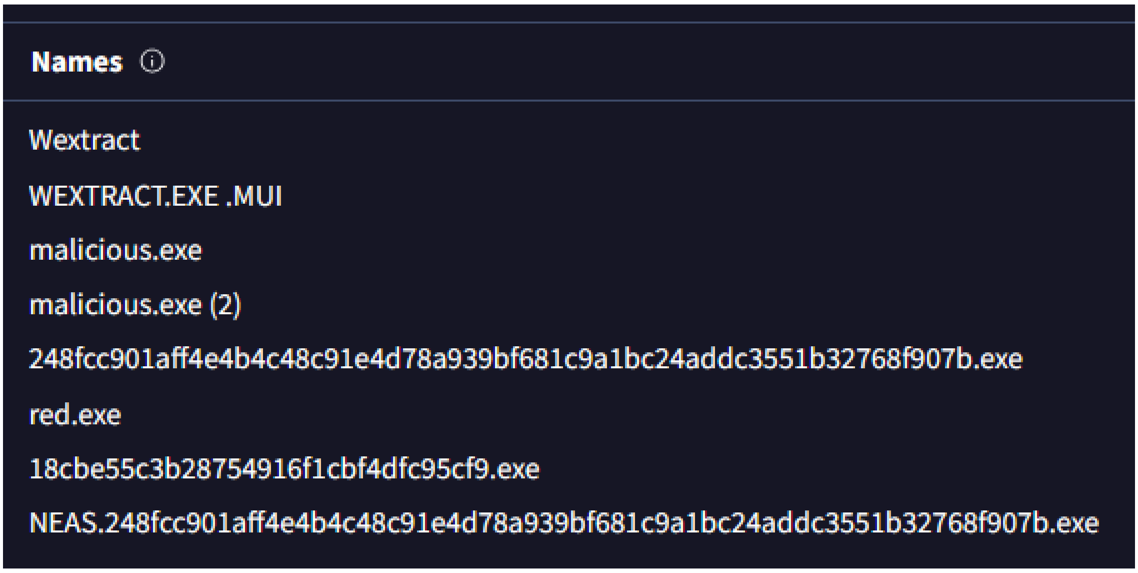


Popular threat label trojan.crifi/stealer

Threat categories trojan

Clear identification of the malware file name facilitates better communication among the SOC team. What's the file name associated with this malware?

If you go to the details tab in VirusTotal, we can see a list of filenames associated with the malware:



Names

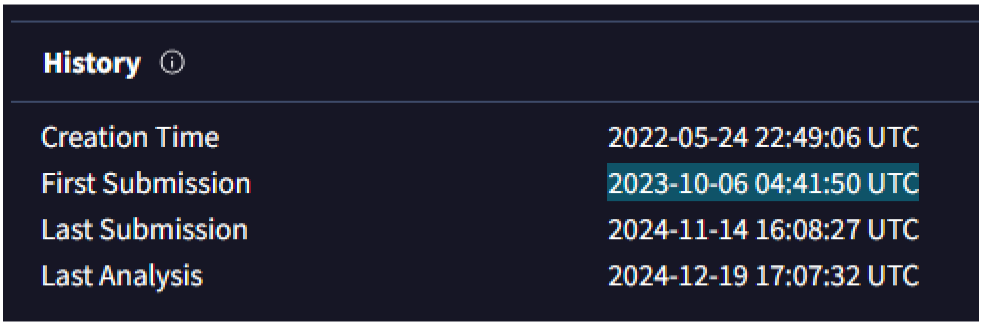
Wextract
WEXTRACT.EXE .MUI
malicious.exe
malicious.exe (2)
248fcc901aff4e4b4c48c91e4d78a939bf681c9a1bc24addc3551b32768f907b.exe
red.exe
18cbe55c3b28754916f1cbf4dfc95cf9.exe
NEAS.248fcc901aff4e4b4c48c91e4d78a939bf681c9a1bc24addc3551b32768f907b.exe

In this case, the answer is Wextract.

Knowing the exact time the malware was first seen can help prioritise actions. If the malware is newly detected, it may warrant more urgent containment and eradication

efforts compared to older, well-known threats. Can you provide the UTC timestamp of first submission of this malware on VirusTotal?

This can be found in the Details tab under the history section:

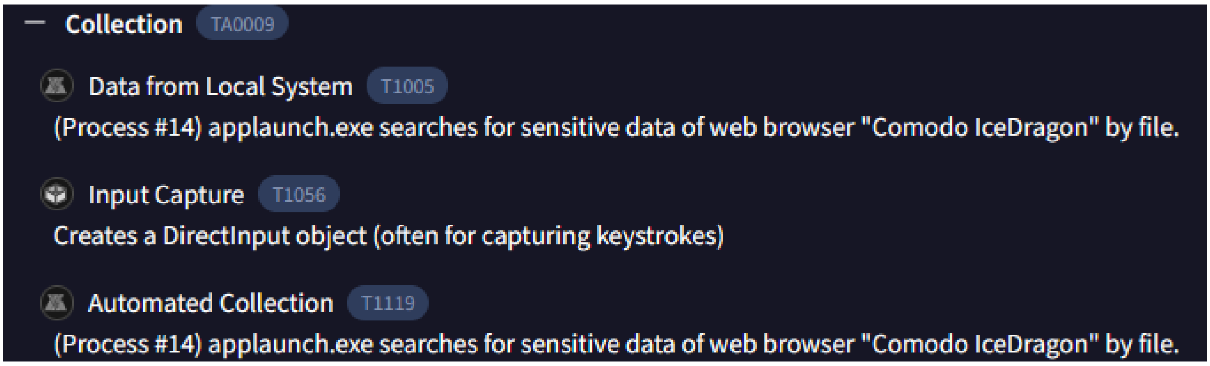


History ⓘ

Creation Time	2022-05-24 22:49:06 UTC
First Submission	2023-10-06 04:41:50 UTC
Last Submission	2024-11-14 16:08:27 UTC
Last Analysis	2024-12-19 17:07:32 UTC

Understanding the techniques used by malware helps in strategic security planning. What is the MITRE ATT&CK technique ID for the malware's data collection from the system before exfiltration?

If you go to the behaviour tab and look at the MITRE ATT&CK Tactics and Techniques section, we can see three techniques are used for collection:



— **Collection** TA0009

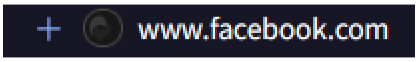
Data from Local System T1005
(Process #14) applaunch.exe searches for sensitive data of web browser "Comodo IceDragon" by file.

Input Capture T1056
Creates a DirectInput object (often for capturing keystrokes)

Automated Collection T1119
(Process #14) applaunch.exe searches for sensitive data of web browser "Comodo IceDragon" by file.

In this case, T1005 is the answer.

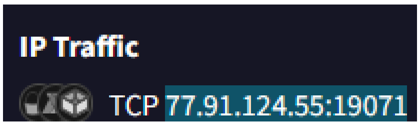
Following execution, what domain name resolution is performed by the malware?



+ www.facebook.com

Once the malicious IP addresses are identified, network security devices such as firewalls can be configured to block traffic to and from these addresses. Can you provide the IP address and destination port the malware communicates with?

You can find this in the behaviour tab:

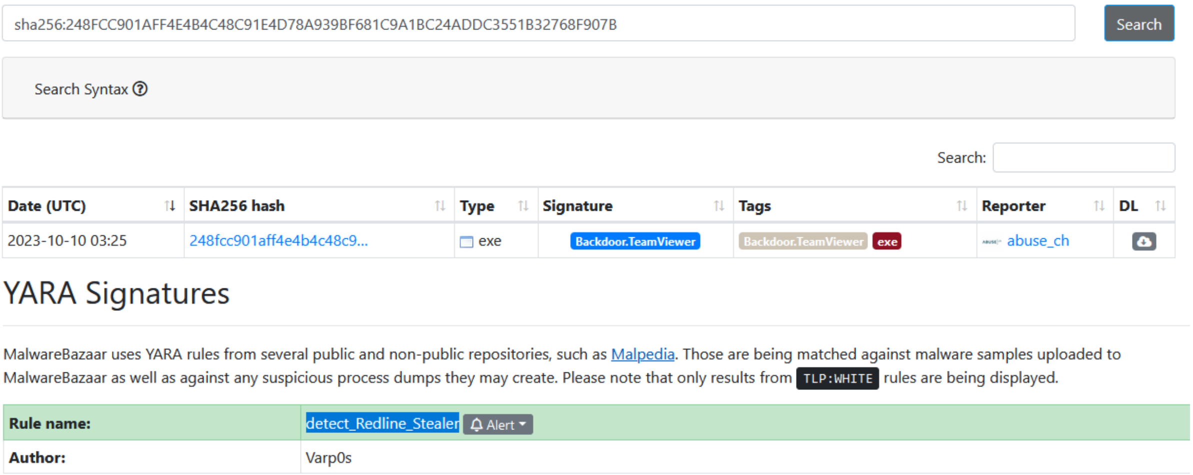


IP Traffic

TCP 77.91.124.55:19071

YARA rules are designed to identify specific malware patterns and behaviours. What's the name of the YARA rule created by "Varp0s" that detects the identified malware?

There would be multiple ways to find the answer to this, however, I simply searched for the file hash in MalwareBazaar and looked at the YARA Signatures section:



sha256:248FCC901AFF4E4B4C48C91E4D78A939BF681C9A1BC24ADDC3551B32768F907B

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2023-10-10 03:25	248fcc901aff4e4b4c48c9...	exe	Backdoor.TeamViewer	Backdoor.TeamViewer exe	abuse_ch	

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
Author:	Varp0s

Understanding which malware families are targeting the organisation helps in strategic security planning for the future and prioritising based on the threat. Can you provide the different malware alias associated with the malicious IP address?

RECORDSTEALER.

By identifying the malware's imported DLLs, we can configure security tools to monitor for the loading or unuusaly usage of these specific DLLs. Can you provide the DLL utiliosed by the malware for privilege escalation?

advapi32.dll