

Analyzing Snake Keylogger in ANY.RUN: a Full Walkthrough

By Lena aka LambdaMamba

Published: 2023-10-05 · Archived: 2026-04-05 23:18:03 UTC



Lena aka LambdaMamba

I am a Chief Research Officer at a cybersecurity company. My passions include investigations, experimentations, gaming, writing, and drawing. I also like playing around with hardware, operating systems, and FPGAs. I enjoy assembling things as well as disassembling things! In my spare time, I do CTFs, threat hunting, and write about them. I am fascinated by snakes, which includes the Snake Malware!

Check out:

- [My website](#)
- [My LinkedIn profile](#)

Emails are a common communication method but also a major vector for cyber threats. They can deliver everything from scams and data theft to malware. Unfortunately, one bad email can lead to financial loss, reputational damage, and even escalate into broader system compromise.

To bolster email security, it's essential to understand the types of attacks you're up against. This blog post dives into a real-world example featuring a Snake Keylogger attachment.

Let's dive right into it!

Overview of the Snake Keylogger

The Snake Keylogger is an infostealer malware written in the .NET programming language. It was discovered in November 2020 and is also known as the 404 Keylogger, 404KeyLogger, and Snake.

The Snake Keylogger steals various information from the victim, such as saved credentials, clipboard data, keystrokes, and screenshots of the victim's screen.

This malware also checks and collects the system information, which includes the system's hostname, username, IP address, geolocation, date and time, and more. It then [exfiltrates the collected information](#) through protocols

such as FTP, SMTP, and Telegram.

More information on the Snake Keylogger and its trends can be found in [ANY.RUN's Malware Trends](#).

Sample Collection and Preparation for Analysis

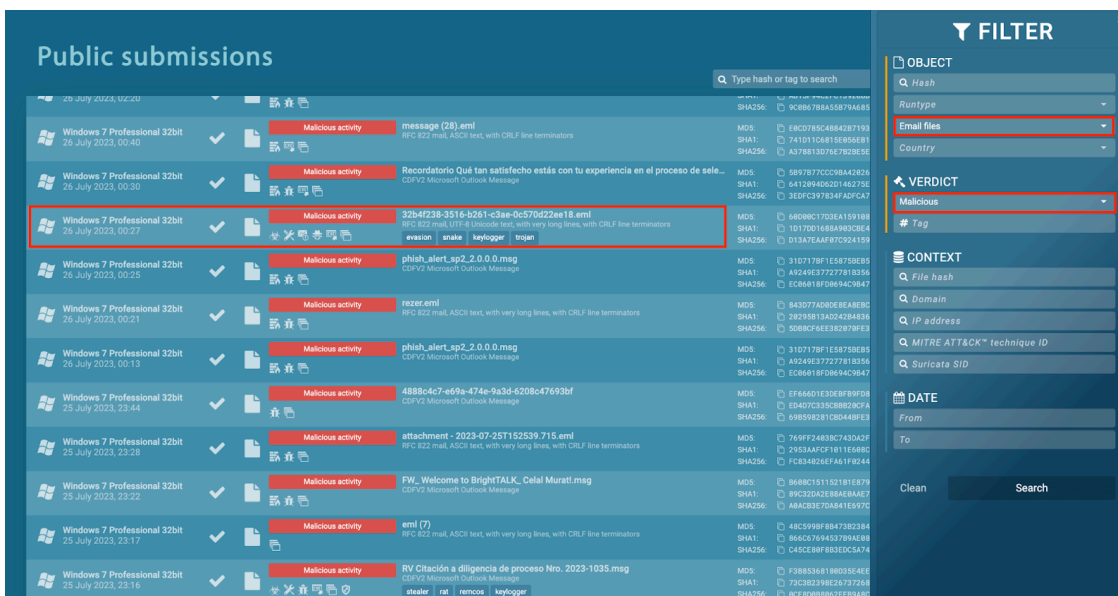
Let's first look at the sample collection method and environment setup.

In [ANY.RUN's Public Submissions](#), the following filters were applied,

- OBJECT > "Email Files"
- VERDICT > "Malicious"

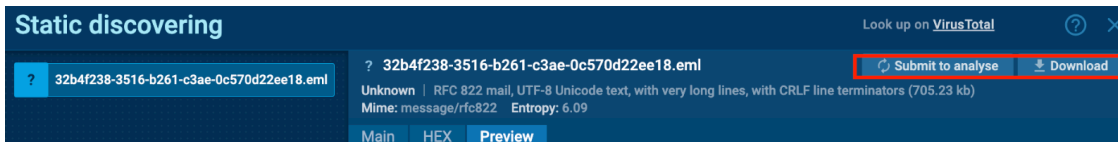
"32b4f238-3516-b261-c3ae-0c570d22ee18.eml" was selected for analysis. This file had the following attributes:

- SHA1 hash of "1D17DD1688A903CBE423D8DE58F8A7AB7ECE1EA5"
- MIME type of "message/rfc822"
- RFC 822 mail, UTF-8 Unicode text, with very long lines, with CRLF line terminators



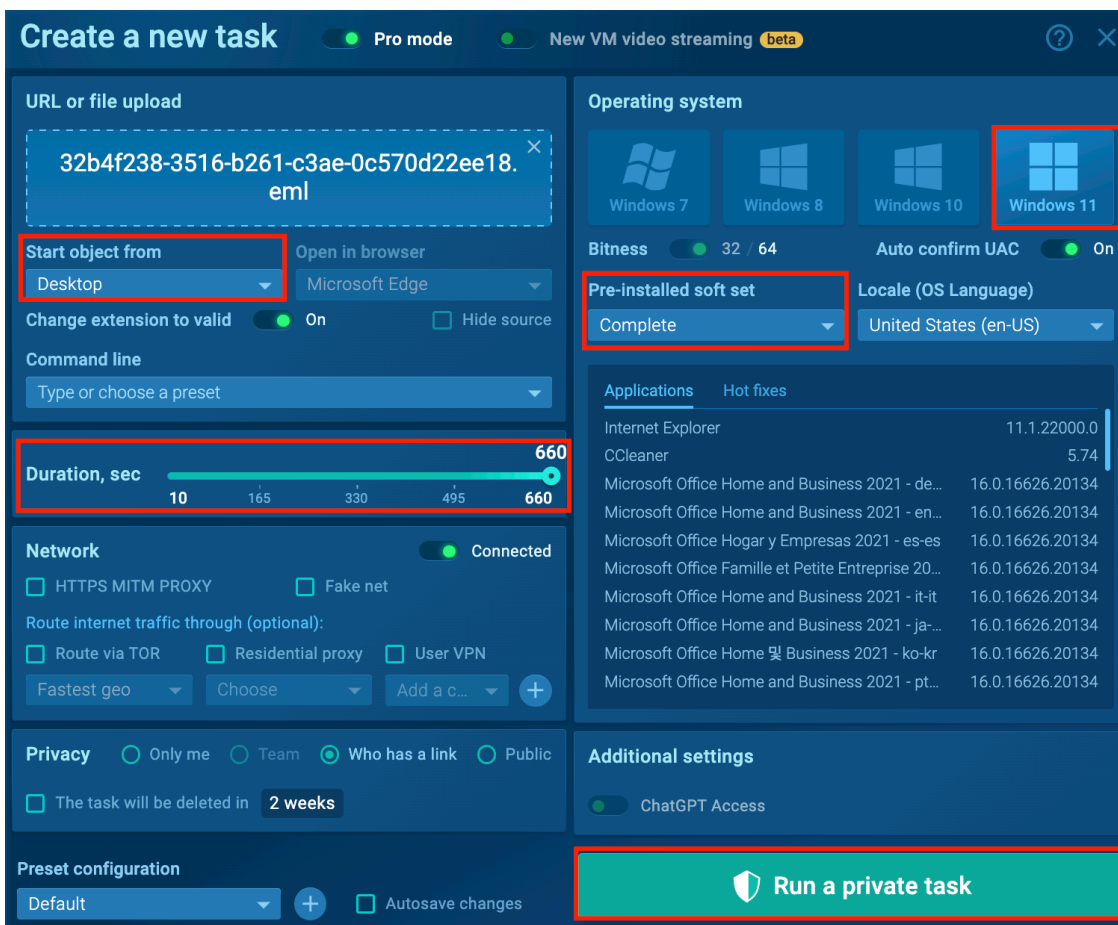
The Filters used to find Malicious Email Files in ANY.RUN's Public submissions

The sample can be downloaded with "Download", and submitted for analysis in ANY.RUN sandbox using "Submit to Analyze" button:



The overview of "32b4f238-3516-b261-c3ae-0c570d22ee18.eml" in *Static Discovering*

A new ANY.RUN task was created for this sample with the following setup:



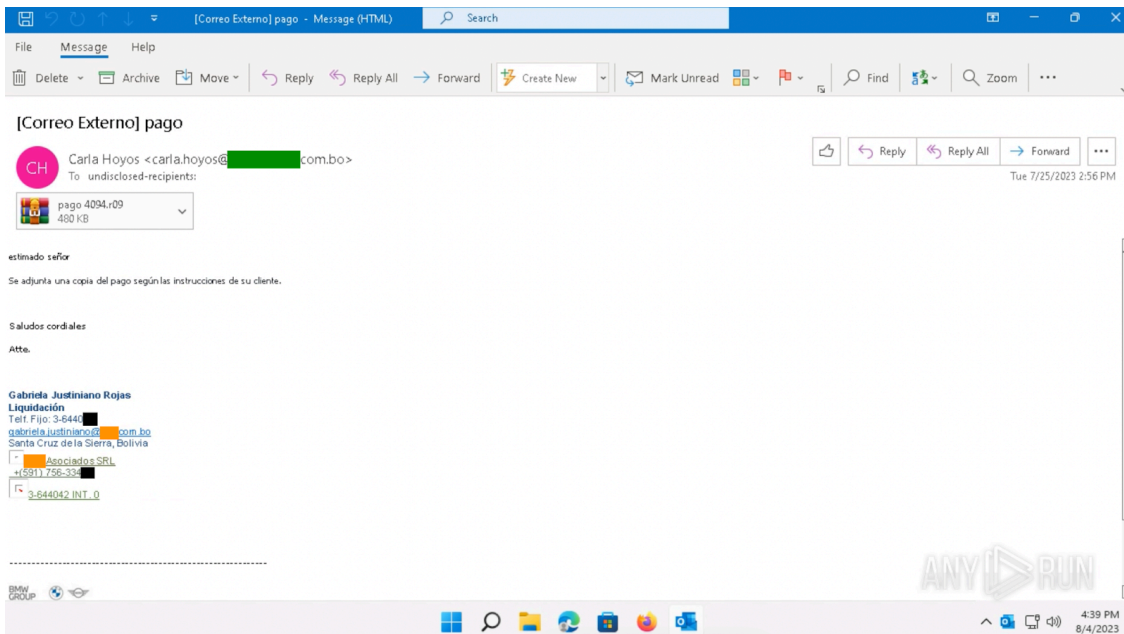
Creation of a New Task, and the setup used for the analysis

The ANY.RUN task for this file can be found [here](#).

Analyzing the Email

Goal of this step: In this section, we'll explore the email body, header, and social engineering tactics.

Opening "32b4f238-3516-b261-c3ae-0c570d22ee18.eml" on Windows 11's Microsoft Outlook showed the email contents:



Opening the email file on Windows 11's Microsoft Outlook

The email body shows the sender attempting to convince the recipient to download and open the email attachment by referencing the “client”. The email signature makes references to a Customs Clearing Agency in Bolivia and uses the BMW Group’s Logo, suggesting that the sender was attempting to exploit familiarity. Familiarity Exploitation is a social engineering tactic where one pretends to be an entity that is familiar to the target.

The email headers can reveal key information and are useful when analyzing the legitimacy of the email. It is crucial to analyze the SPF and DKIM information when attempting to determine an [email’s legitimacy](#).

- SPF (Sender Policy Framework) is a DNS record that is used to verify the legitimacy of email senders. The email recipient’s server checks the SPF record of the sender’s domain to verify they are an approved sender.
- DKIM (DomainKeys Identified Mail) is an email authentication method used to verify the authenticity and integrity of the email. A digital signature is added to the email’s header, which is generated by the sender’s server with a private key. This is verified by the recipient’s server with a public key published in the sender’s DNS records.

The email header reveals that the SPF failed, where the sender IP was IP 45[.]227.X.34. The header mentions “[GREEN].com[.]bo does not designate IP 45[.]227.X.34 as permitted sender”. Also, there was no DKIM and DMARC, and the message was not signed:

```
Authentication-Results: spf=fail (sender IP is 45.227.[REDACTED].134)
smtp.mailfrom=[REDACTED].com.bo; dkim=none (message not signed)
header.d=none;dmARC=none action=none
header.from=[REDACTED].com.bo;compauth=fail reason=001
Received-SPF: Fail (protection.outlook.com: domain of [REDACTED].com.bo does
not designate 45.227.[REDACTED].134 as permitted sender)
receiver=protection.outlook.com; client-ip=45.227.[REDACTED].134;
helo=[REDACTED].controlvps.com;
```

A section of the sample email’s header shows the SPF, DKIM, and DMARC information

The IP address 45[.]227.X.34 is associated with these domains (hidden with purple and blue markers for confidentiality reasons). According to [VirusTotal](#), it appears to be a security company in Argentina:

The screenshot shows the VirusTotal interface for IP address 45.227.X.34. It displays a community score of 0/89 and lists 4 detected files embedding this IP address. Below this, there are two tables: 'Passive DNS Replication (9)' and 'Files Referring (5)'. The 'Passive DNS Replication' table lists dates resolved, detections, resolvers, and domains. The 'Files Referring' table lists scanned dates, detections, types, and names.

Date resolved	Detections	Resolver	Domain
2021-12-05	0 / 89	VirusTotal	soprote[REDACTED].com.ar
2021-12-05	0 / 89	VirusTotal	www.soprote[REDACTED].com.ar
2021-10-18	0 / 89	Offensive Security	cpanel[REDACTED].com.ar
2021-10-01	0 / 89	VirusTotal	monitoreo[REDACTED].com.ar
2021-10-01	0 / 89	VirusTotal	www.monitoreo[REDACTED].com.ar
2021-09-28	0 / 89	VirusTotal	mail[REDACTED].com.ar
2021-09-27	0 / 89	VirusTotal	www[REDACTED].com.ar
2021-09-27	0 / 89	VirusTotal	www[REDACTED].com.ar
2021-09-20	0 / 89	VirusTotal	[REDACTED].controlvps.com

Scanned	Detections	Type	Name
2023-08-21	28 / 60	Email	Temp[119].eml
2023-07-25	13 / 60	Outlook	pago.msg
2023-04-19	19 / 60	Email	00e7f92d9f8e9c15d12c95a72c8c4be22ab4c042915a4d75f84e728fe0ee561
2022-08-19	31 / 61	Email	goblermocta_2011977613_download.eml
2023-07-25	0 / 60	Outlook	pago.msg

Looking up the IP address 45[.]227.X.34 on VirusTotal

The email header shows the authenticated sender, which was “cobranzas@[REDACTED].com.ar”.

```
Received: from [REDACTED].controlvps.com (45.227.[REDACTED].134) by
DM3NAM02FT035.mail.protection.outlook.com (10.13.[REDACTED].78) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
15.20.6631.29 via Frontend Transport; Tue, 25 Jul 2023 14:58:08 +0000
Received: from webmail.[REDACTED].com.ar (localhost [127.0.0.1])
(Authenticated sender: cobranzas@[REDACTED].com.ar)
by [REDACTED].controlvps.com (Postfix) with ESMTPA id D387963E7F;
Tue, 25 Jul 2023 11:55:35 -0300 (-03)
DKIM-Filter: OpenDKIM Filter v2.11.0 [REDACTED].controlvps.com D387963E7F
```

A section of the sample email’s header shows the authenticated sender

The email header also revealed the User-Agent, which was “Roundcube Webmail/1.4.2”. [Roundcube Webmail](#) is a free and open-source webmail software.

```
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="=_8e7887a8909f0688fef98d950324214b"
Date: Tue, 25 Jul 2023 15:55:35 +0100
From: Carla Hoyos <carla.hoyos@[REDACTED].com.bo>
To: undisclosed-recipients;
Subject: [Correo Externo] pago
User-Agent: Roundcube Webmail/1.4.2
Message-ID: <285e785b838658691be29f41afc147@[REDACTED].com.bo>
X-Sender: carla.hoyos@[REDACTED].com.bo
Return-Path: carla.hoyos@[REDACTED].com.bo
```

A section of the sample email’s header shows Date, Time, From, To, Subject, User-Agent, etc.

What did we learn from the header?

It indicates that this email was most likely not legitimate. The contents of the email and the sender’s email address suggest that it was attempting to impersonate a company in Bolivia that provides brokering and insurance

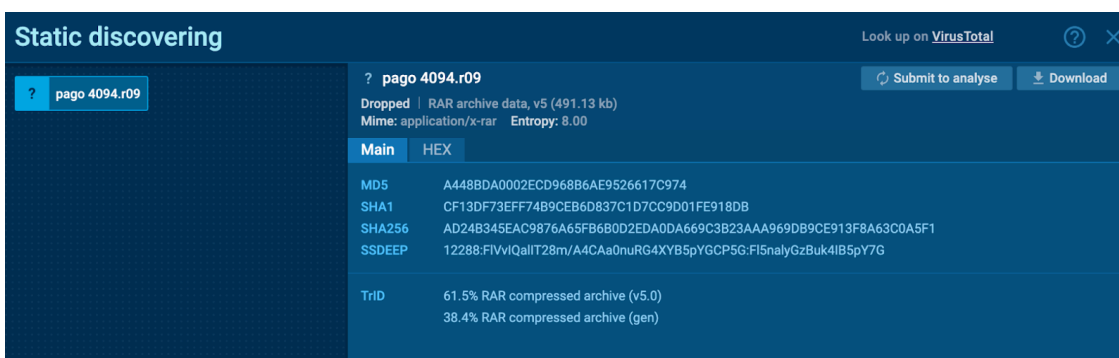
services. Additionally, it utilized social engineering tactics to convince the recipient to download and open the attachment.

Analyzing the Behaviour of the Attachment

Goal of this step: In this section, we'll explore the behavioral analysis of the email's attachment on Windows 11 and examine the involved files.

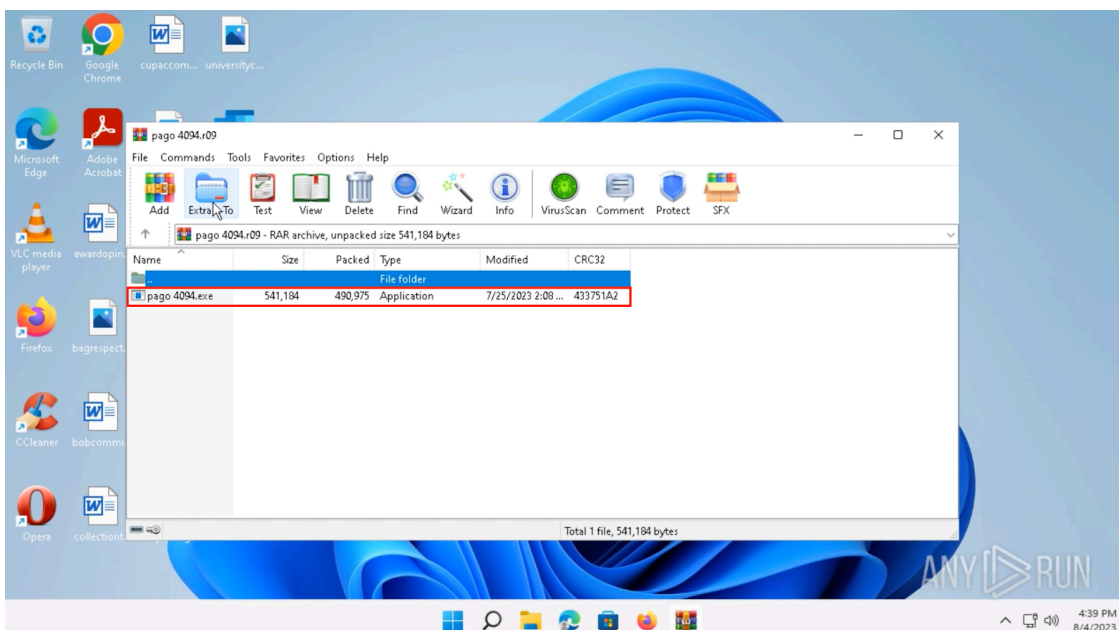
A file called "pago 4094.r09" is attached to this email, with the following attributes:

- SHA1 hash of "CF13DF73EFF74B9CEB6D837C1D7CC9D01FE918DB"
- MIME type of "application/x-rar"
- RAR archive data, v5



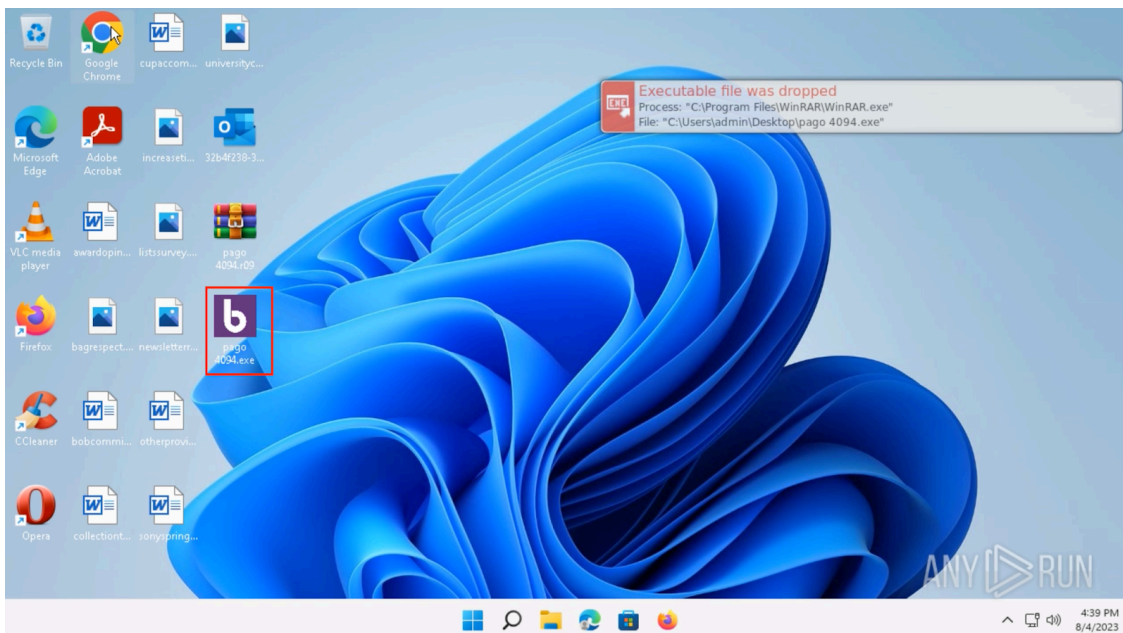
The information for pago 4094.r09 in *Static discovering*

Downloading and opening "pago 4094.r09" in WinRAR shows the existence of an Application called "pago 4094.exe":



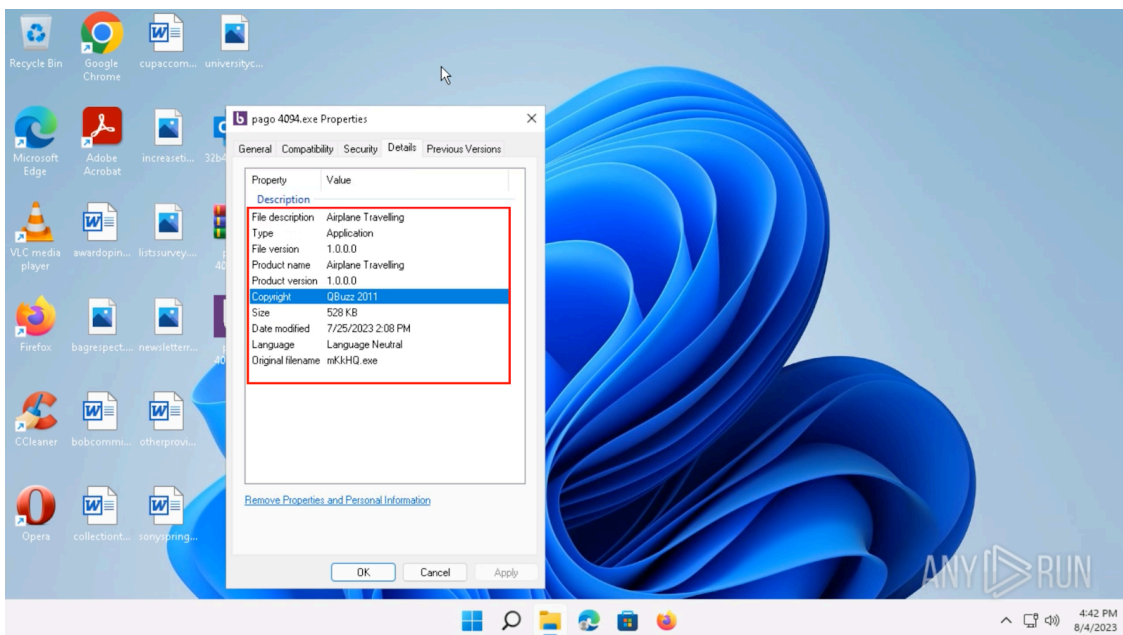
Opening "pago 4094.r09" in WinRAR

Extracting “pago 4094.exe” onto the Desktop reveals that it uses the *Yahoo! Buzz* Icon. [Yahoo! Buzz](#) is a community-based news article website.



The *Yahoo! Buzz* icon

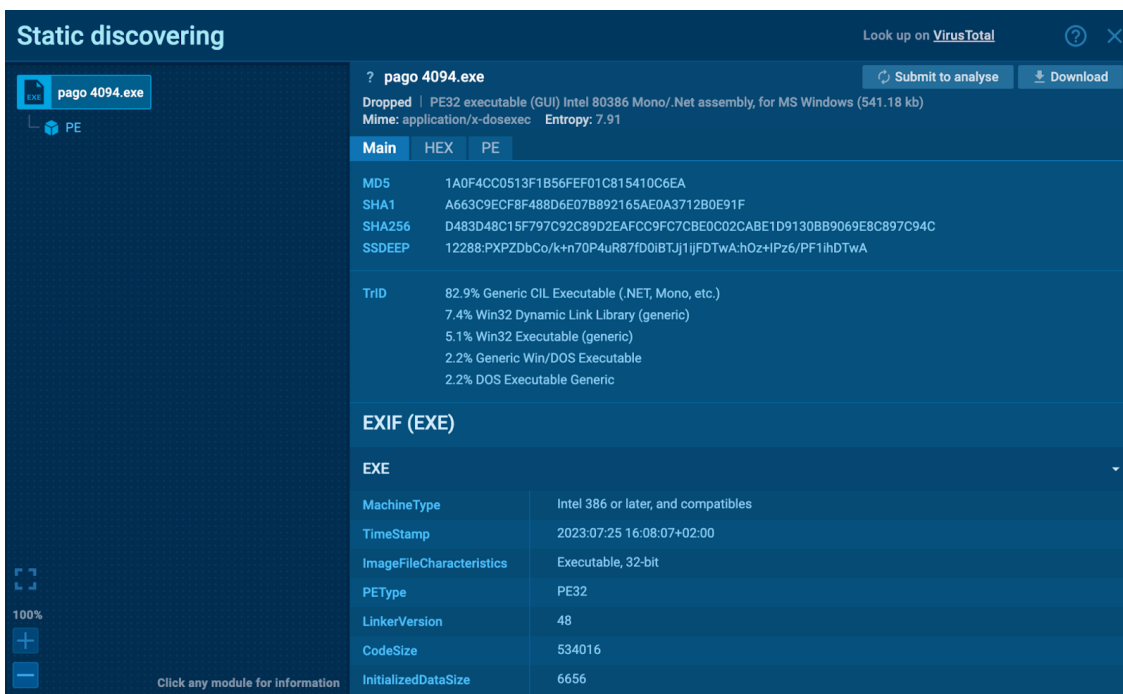
The properties tell us that the original filename was “mKkHQ.exe”, and had the copyright “QBUZZ 2011”:



The Properties for “pago 4094.exe”

This executable “pago 4094.exe” has the following attributes:

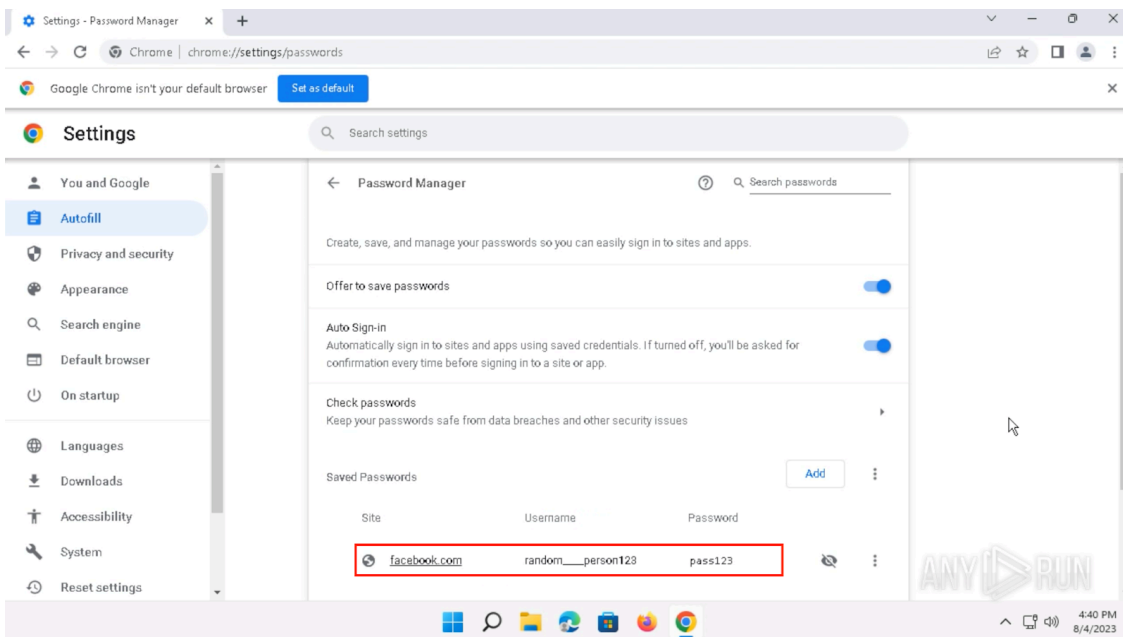
- SHA1 hash of “A663C9ECF8F488D6E07B892165AE0A3712B0E91F”
- MIME type of “application/x-dosexec”
- PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows



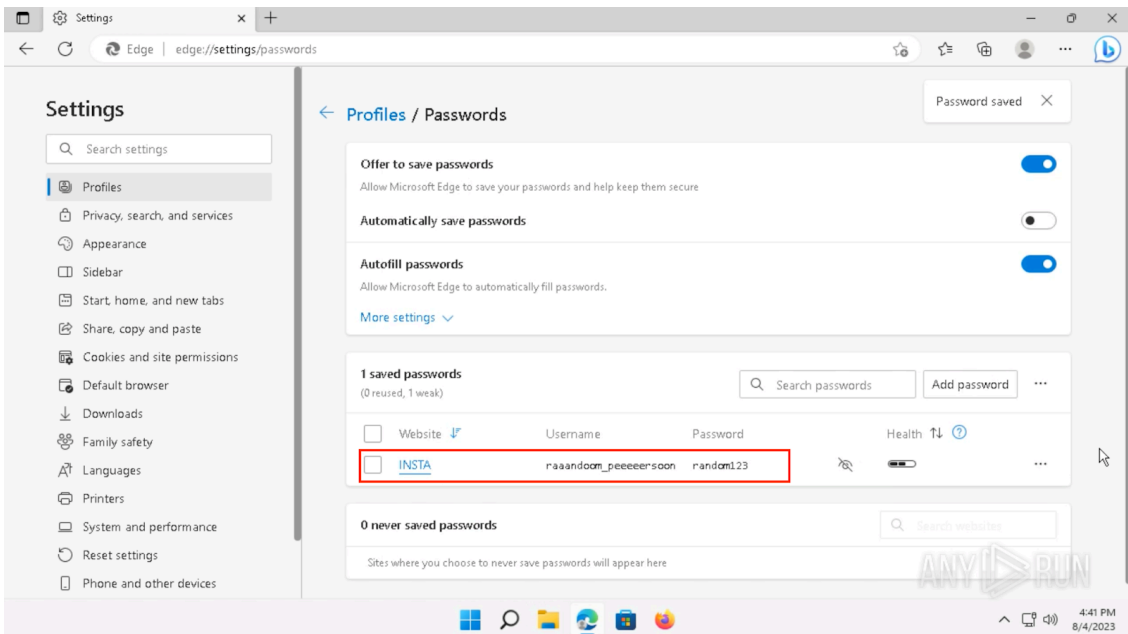
Static Discovering shows the details of the executable “pago 4094.exe”.

Saving credentials in browsers

Before executing “pago 4094.exe”, various fake credentials were purposefully saved onto Browsers like Chrome and Microsoft Edge. This was done to observe the malware’s credential-stealing behavior.



Saving fake Facebook credentials on Chrome, under “chrome://settings/passwords”



Saving fake Instagram credentials on Microsoft Edge, under “edge://settings/passwords”

Once the fake credentials were saved onto the Browsers, “pago 4094.exe” was executed by double-clicking “pago 4094.exe” on the Desktop.

Getting into the execution flow

Around 30 seconds after executing “pago 4094.exe”, the executable file disappears from the Desktop. A child process “C:\Users\admin\Desktop\pago 4094.exe” is created, and an executable file “C:\Users\admin\AppData\Local\Temp\tmpG484.tmp” is dropped. The dropping of the .tmp file is done to secure persistence on the victim machine.



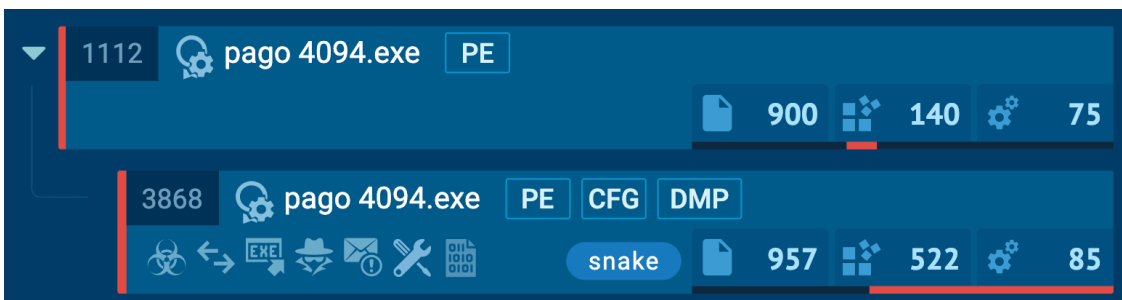
The executable disappears from the Desktop, and “tmpG484.tmp” is dropped in “C:\Users\admin\AppData\Local\Temp\”

Now, the Snake Keylogger is running silently in the background. From the Windows User’s perspective, nothing alarming happens.

Analyzing the Processes

Goal of this section: We’ll explore the analysis of processes associated with the Snake Keylogger.

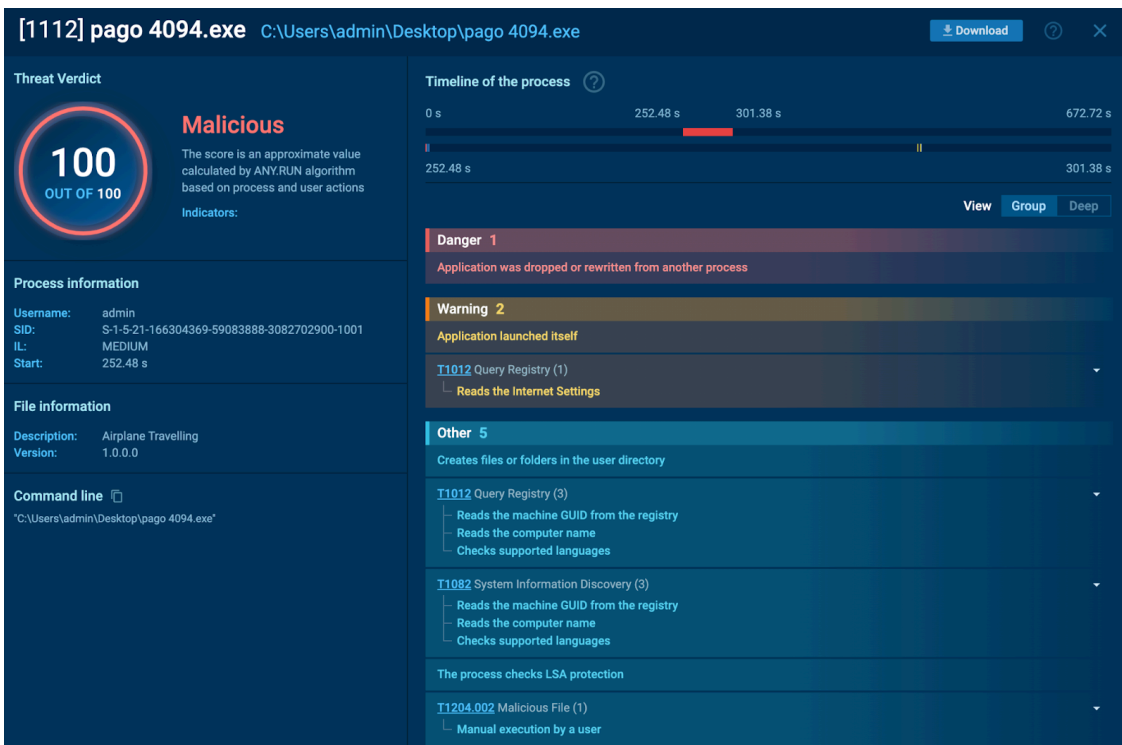
Process 1112 and its child process 3868, are key processes involved in the malicious activities:



The “pago 4094.exe” processes

Detailed look at the process 1112

Process 1112 was detected as 100/100 Malicious under the *Threat Verdict*. It can be observed querying registries, performing system information discoveries, checking LSA protection, dropping another application, etc. This process ran for a total of 48.9 seconds.



Overview of Process 1112, “pago 4094.exe”

Registry changes were seen for Process 1112, and the following Write Operations were conducted:

Time	Operation	Name	Key and value
+35077 ms	Write	ProxyBypass	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1
+35077 ms	Write	IntranetName	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1
+35077 ms	Write	UNCAsIntranet	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1
+35077 ms	Write	AutoDetect	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 0
+35077 ms	Write	ProxyBypass	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1
+35077 ms	Write	IntranetName	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1
+35077 ms	Write	UNCAsIntranet	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1
+35077 ms	Write	AutoDetect	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 0

The Registry changes for Process 1112

Process 1112 also created a new file with the MIME type of “text/plain”, called “pago 4094.exe.log” under “C:\Users\admin\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\”:

Behavior activities
(PID: 1112) pago 4094.exe

Source: files First seen: 277.63 s

Other /
Creates files or folders in the user directory

Operation: CREATE
Device: DISK_FILE_SYSTEM
Object: FILE
Name: C:\Users\admin\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\pago 4094.exe.log
Status: 0x00000000
Created: CREATED
Access: READ_CONTROL, SYNCHRONIZE, FILE_WRITE_DATA, FILE_APPEND_DATA, FILE_WRITE_EA, FILE_READ_ATTRIBUTES, FILE_WRITE_ATTRIBUTES

The creation of “pago 4094.exe.log”

The contents of “pago 4094.exe.log” contained references to *System.Windows.Forms*, *System.Drawing*, etc. which are associated with [.NET API](#). It also contained *PublicKeyToken* values:

```
1. "fusion", "GAC", 0
2. "WinRT", "NotApp", 1
3. "System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e889", 0
4. "System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e889", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System20aep98e0f507201a9c90ca7fcc04351\System.ni.dll", 0
5. "System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=9595f641", 0
6. "System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e889", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\as5a6b855ebaabf048894ecbd1badf29\System.Core.ni.dll", 0
7. "System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\540373304724ec50f100f28161c1c1\System.Configuration.ni.dll", 0
8. "System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e889", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\146b3acd7fc376f4853538484c2290ac\System.Xml.ni.dll", 0
9. "Accessibility, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a", 0
10. "Microsoft.VisualStudio, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a", 0
```

The contents of “pago 4094.exe.log”

Detailed look at the process 3868

Process 3868 plays a significant role in this malware. This process started at 287.76 seconds and ran all the way until the end. It steals credentials from browsers and files and sends these stolen credentials over SMTP:

[3868] pago 4094.exe C:\Users\admin\Desktop\pago 4094.exe

Threat Verdict
100 OUT OF 100
Malicious
 The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions
 Indicators:

Process information
 Username: admin
 SID: S-1-5-21-166304369-59083888-3082702900-1001
 IL: MEDIUM
 Start: 287.76 s

File information
 Description: Airplane Travelling
 Version: 1.0.0.0

Command line
 "C:\Users\admin\Desktop\pago 4094.exe"

Timeline of the process
 0 s — 287.76 s — 672.72 s

Danger 6

- SNAKE detected by memory dumps
- T1555.003 Credentials from Web Browsers (1)
 - Steals credentials from Web Browsers
- T1552.001 Credentials In Files (2)
 - Steals credentials from Web Browsers
 - Actions looks like stealing of personal data
- T1518 Software Discovery (1)
 - Actions looks like stealing of personal data
- SNAKEKEYLOGGER was detected
- Application was dropped or rewritten from another process

Warning 4

- T1071.003 Mail Protocols (1)
 - Connects to SMTP port
- T1016 System Network Configuration Discovery (1)
 - Checks for external IP
- Executable content was dropped or overwritten
- T1012 Query Registry (1)
 - Reads the Internet Settings

Overview of Process 3868, “pago 4094.exe”

The indicators for this process included “Known Threat”, “Connects to the network”, “Executable file was dropped”, “Actions similar to stealing personal data”, “Behavior similar to spam”, “The process has the malware config”, and “The module has a process dump.”




The indicators in Process 3868

It was detected as Snake Keylogger, where the destination IP was 158.101.44[.]242, with a destination port of 80. This IP is associated with *checkip.dyndns[.]com*, and we will explore it in detail in the next section, *Analyzing the Network Information*.

Behavior activities ✕
(PID: 3868) pago 4094.exe

▲ 1 of 2 ▼ Source: network First seen: 278.35 s

 **Danger / Known Threat**
SNAKEKEYLOGGER was detected


Process: C:\Users\admin\Desktop\pago 4094.exe
IpDst: 158.101.44.242
IpSrc: 192.168.100.103
PortDst: 80
PortSrc: 49789

The detection of SNAKEKEYLOGGER

Process 3868 drops “C:\Users\admin\AppData\Local\Temp\tmpG484.tmp”. This has an MD5 hash of 1A0F4CC0513F1B56FEF01C815410C6EA, which is the same as the MD5 hash for the original executable file “pago 4094.exe”. This is done to achieve persistence on the victim machine.

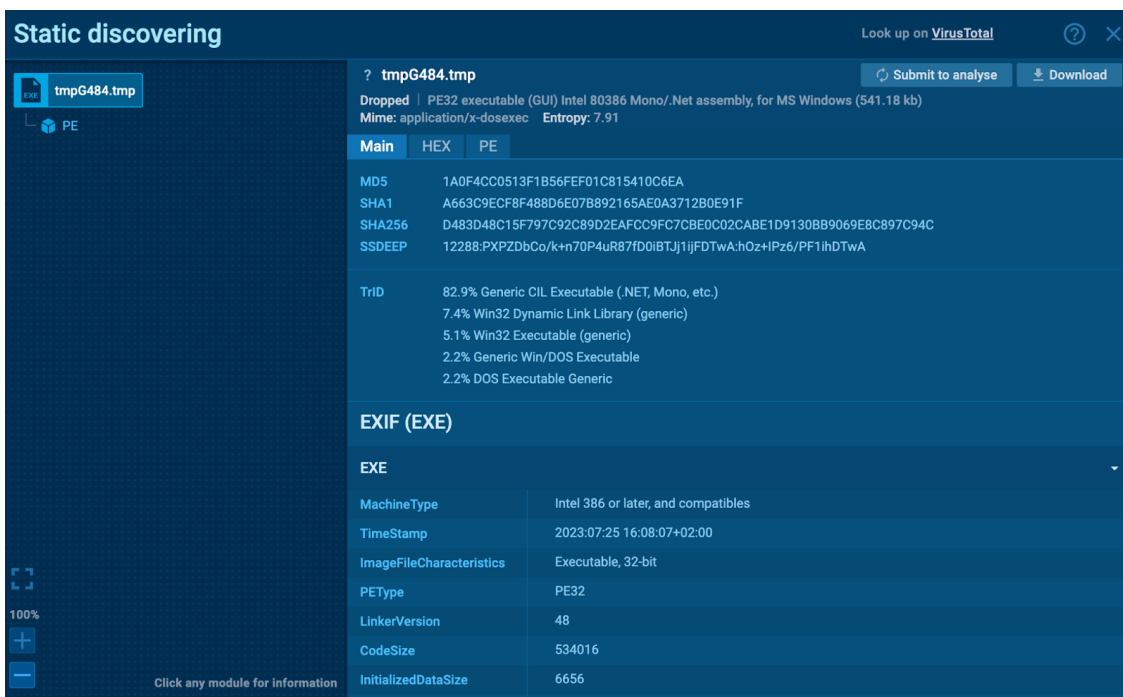
Behavior activities ✕
(PID: 3868) pago 4094.exe

Source: drops First seen: 278.18 s

 **Warning / Installation**
Executable content was dropped or overwritten

Size: 541184
Md5: 1A0F4CC0513F1B56FEF01C815410C6EA
Filename: C:\Users\admin\AppData\Local\Temp\tmpG484.tmp

A .tmp file is dropped

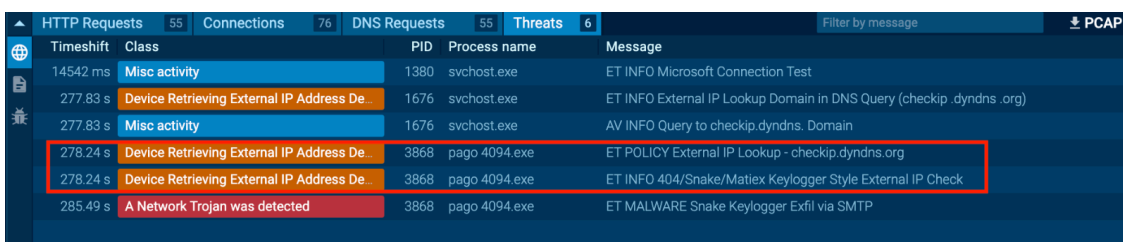


Details of the dropped “C:\Users\admin\AppData\Local\Temp\tmpG484.tmp”

Analyzing the Network Activities

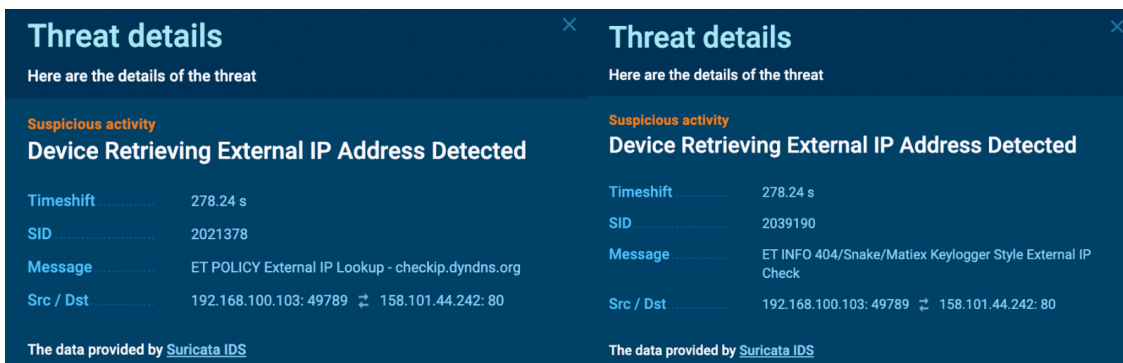
Section goal: In this section, we’ll explore the network activities associated with the Snake Keylogger and examine the packet capture (PCAP) file in detail.

Process 3868, “pago 4094.exe”, attempted to retrieve external IP addresses with *checkip.dyndns[.]org* as shown in the *Threats* Tab:



The *Threats* Tab shows the retrieval of the external IP address

It was seen connecting to 158.101.44[.]242 on port 80. This IP was associated with *checkip.dyn...* according to VirusTotal:



The Threat details show the source and destination IP and port.

3 / 89

3 security vendors flagged this IP address as malicious

158.101.44.242 (158.101.0.0/16)
AS 31898 (ORACLE-BMC-31898)

US Last Analysis Date 9 hours ago

Community Score

DETECTION DETAILS RELATIONS COMMUNITY 13

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Passive DNS Replication (18)

Date resolved	Detections	Resolver	Domain
2023-03-10	0 / 88	VirusTotal	hasenbau.familiemeister.ch
2022-10-19	0 / 89	VirusTotal	pass.familiemeister.ch
2021-09-10	0 / 89	VirusTotal	www.hostedservice.hk
2021-09-03	0 / 89	VirusTotal	box.hostedservice.hk
2021-09-03	0 / 89	VirusTotal	barracuda.hkg.cool
2021-08-31	0 / 89	VirusTotal	meuip.us.es.inf.br
2021-08-31	0 / 89	VirusTotal	mst.familiemeister.ch
2021-08-30	0 / 89	VirusTotal	smtp.comune.hkg.cool
2021-08-29	0 / 89	VirusTotal	mxt0.familiemeister.ch
2021-08-29	0 / 89	VirusTotal	rds-sh.familiemeister.ch
2021-08-28	0 / 88	VirusTotal	mst.meister-it.ch
2021-08-28	0 / 89	VirusTotal	rds-sh.meisterfamily
2021-08-27	0 / 89	VirusTotal	mbox.meister-it.ch
2021-08-27	0 / 89	VirusTotal	rds.familiemeister.ch
2021-08-26	0 / 88	VirusTotal	rds-gw.familiemeister.ch
2021-07-20	0 / 89	VirusTotal	checkip.dyndns.org
2021-07-20	0 / 89	VirusTotal	checkip.dyndns.com
2021-07-19	1 / 89	VirusTotal	checkip.dyn.com

The IP 158.101.44[.]242 was associated with checkip.dyn according to VirusTotal

The host *checkip.dyndns[.]org* is associated with IP checking. According to Dyn, “CheckIP will return the remote socket’s IP address. If a client sends a Client-IP or a X-Forwarded-For HTTP header, [CheckIP](#) will return that value instead.”

The packet capture (PCAP) file was downloaded for further analysis. The following filter was applied on the PCAP in Wireshark.

```
ip.dst == 158.101.44.242 || ip.src == 158.101.44.242
```

This is done to check for packets where the destination or source IP was 158.101.44[.]242.

No.	Time	Source	Destination	Protocol	Source port	Dest port	Length	Info
100995	279.139053	192.168.100.103	158.101.44.242	TCP	49789	80	66	49789 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
101009	279.170392	158.101.44.242	192.168.100.103	TCP	80	49789	66	80 → 49789 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1104 SACK_PERM=1 WS=256
101011	279.170561	192.168.100.103	158.101.44.242	TCP	49789	80	54	49789 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
101013	279.170860	192.168.100.103	158.101.44.242	HTTP	49789	80	205	GET / HTTP/1.1
101009	279.201450	158.101.44.242	192.168.100.103	TCP	80	49789	54	80 → 49789 [ACK] Seq=1 Ack=152 Win=64256 Len=0
101005	279.491172	158.101.44.242	192.168.100.103	HTTP	80	49789	320	HTTP/1.1 200 OK (text/html)
101095	279.530930	192.168.100.103	158.101.44.242	TCP	49789	80	54	49789 → 80 [ACK] Seq=152 Ack=275 Win=262400 Len=0
124742	344.490467	158.101.44.242	192.168.100.103	TCP	80	49789	54	80 → 49789 [FIN, ACK] Seq=275 Ack=152 Win=64256 Len=0
124743	344.490604	192.168.100.103	158.101.44.242	TCP	49789	80	54	49789 → 80 [ACK] Seq=152 Ack=276 Win=262400 Len=0
127713	379.505216	192.168.100.103	158.101.44.242	TCP	49789	80	54	49789 → 80 [FIN, ACK] Seq=152 Ack=276 Win=262400 Len=0
127714	379.535771	158.101.44.242	192.168.100.103	TCP	80	49789	54	80 → 49789 [RST] Seq=276 Win=0 Len=0

Packets where the Destination or Source IP is 158.101.44[.]242

Following the TCP stream revealed that it checked the current IP with *checkip[.]dyndns.org*, which was 45.130.136[.]51:

```
GET / HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;)
Host: checkip.dyndns.org
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Fri, 04 Aug 2023 16:43:14 GMT
Content-Type: text/html
Content-Length: 105
Connection: keep-alive
Cache-Control: no-cache
Pragma: no-cache

<html><head><title>Current IP Check</title></head><body>Current IP Address: 45.130.136.51</body></html>
```

Following the TCP steam shows the current IP address

A Network trojan was detected for process 3868, “pago 4094.exe” under the *Threats* tab:

Timeshift	Class	PID	Process name	Message
14542 ms	Misc activity	1380	svchost.exe	ET INFO Microsoft Connection Test
277.83 s	Device Retrieving External IP Address De...	1676	svchost.exe	ET INFO External IP Lookup Domain in DNS Query (checkip_dyndns.org)
277.83 s	Misc activity	1676	svchost.exe	AV INFO Query to checkip.dyndns.Domain
278.24 s	Device Retrieving External IP Address De...	3868	pago 4094.exe	ET POLICY External IP Lookup - checkip.dyndns.org
278.24 s	Device Retrieving External IP Address De...	3868	pago 4094.exe	ET INFO 404/Snake/Matiex Keylogger Style External IP Check
285.49 s	A Network Trojan was detected	3868	pago 4094.exe	ET MALWARE Snake Keylogger Exfil via SMTP

The Detected Network Trojan

A *Snake Keylogger Exil via SMTP* was observed, where the destination IP was 208.91.199[.]255 and the destination port was 587. SMTP on [port 587 is a secure and authenticated method](#) for sending emails from email clients to email servers. It typically uses STARTTLS or TLS/SSL for encryption.

Threat details

Here are the details of the threat

Malicious activity

A Network Trojan was detected

Timeshift 285.49 s

SID 2044767

Message ET MALWARE Snake Keylogger Exfil via SMTP

Src / Dst 192.168.100.103: 49790 ⇄ 208.91.199.225: 587

The data provided by [Suricata IDS](#)

The *Threat Details* of the Network Trojan

Applying the *smtp* filter on the PCAP in Wireshark showed the data exfiltration taking place over SMTP:

No.	Time	Source	Destination	Protocol	Source port	Dest port	Length	Info
104615	285.227443	208.91.199.225	192.168.100.103	SMTP	587	49790	102	S: 220 us2.outbound.mailhostbox.com ESMTP Postfix
104616	285.228357	192.168.100.103	208.91.199.225	SMTP	49790	587	76	C: EHLO DESKTOP-BFTPUHP
104618	285.415865	208.91.199.225	192.168.100.103	SMTP	587	49790	263	S: 250-us2.outbound.mailhostbox.com PIPELINING SIZE 41648128 VRFY ETRN
104619	285.417488	192.168.100.103	208.91.199.225	SMTP	49790	587	95	C: AUTH Login User: [REDACTED]
104620	285.606542	208.91.199.225	192.168.100.103	SMTP	587	49790	72	S: 354 UGfac3dvcm06
104621	285.606520	192.168.100.103	208.91.199.225	SMTP	49790	587	72	C: Pass: [REDACTED]
104623	285.799191	208.91.199.225	192.168.100.103	SMTP	587	49790	91	S: 235 2.7.0 Authentication successful
104624	285.799473	192.168.100.103	208.91.199.225	SMTP	49790	587	89	C: MAIL FROM: [REDACTED]
104625	285.987312	208.91.199.225	192.168.100.103	SMTP	587	49790	68	S: 250 2.1.0 Ok
104626	285.987578	192.168.100.103	208.91.199.225	SMTP	49790	587	87	C: RCPT TO: [REDACTED]
104627	286.197707	208.91.199.225	192.168.100.103	SMTP	587	49790	68	S: 250 2.1.5 Ok
104628	286.198029	192.168.100.103	208.91.199.225	SMTP	49790	587	60	C: DATA
104630	286.305411	208.91.199.225	192.168.100.103	SMTP	587	49790	91	S: 354 End data with <CR><LF>,<CR><LF>
104631	286.389371	192.168.100.103	208.91.199.225	SMTP	49790	587	290	C: DATA fragment, 245 bytes
104632	286.389501	192.168.100.103	208.91.199.225	SMTP	49790	587	200	C: DATA fragment, 146 bytes
104634	286.389502	192.168.100.103	208.91.199.225	SMTP	49790	587	225	C: DATA fragment, 207 bytes
104635	286.389708	192.168.100.103	208.91.199.225	SMTP	49790	587	1158	C: DATA fragment, 1104 bytes
104636	286.389719	192.168.100.103	208.91.199.225	SMTP	49790	587	798	C: DATA fragment, 744 bytes
104637	286.389758	192.168.100.103	208.91.199.225	SMTP	49790	587	220	C: DATA fragment, 166 bytes
104638	286.389800	192.168.100.103	208.91.199.225	SMTP	49790	587	900	C: DATA fragment, 926 bytes
104639	286.389830	192.168.100.103	208.91.199.225	SMTP	49790	587	111	C: DATA fragment, 57 bytes
104640	286.389853	192.168.100.103	208.91.199.225	SMTP	49790	587	56	C: DATA fragment, 2 bytes
104641	286.389877	192.168.100.103	208.91.199.225	SMTP/DMF	49790	587	59	From: [REDACTED] subject: Pc Name: admin Snake Tracker, (text/pla
104646	286.725940	208.91.199.225	192.168.100.103	SMTP	587	49790	91	S: 250 2.0.0 Ok: queued as 1C087640275
127736	384.787549	192.168.100.103	208.91.199.225	SMTP	49790	587	60	C: QUIT
127738	384.975485	208.91.199.225	192.168.100.103	SMTP	587	49790	69	S: 221 2.0.0 Bye

Data exfiltration over SMTP

Following the TCP stream revealed the SMTP Authentication taking place. The email address used to send the stolen information was likely hacked by malicious actors. According to OSINT, the hacked email address belonged to a physical security company in South America.

The same is confirmed in the PCAP:

```
220 us2.outbound.mailhostbox.com ESMTP Postfix
EHLO DESKTOP-BFTPUHP
250-us2.outbound.mailhostbox.com
250-PIPELINING
250-SIZE 41648128
250-VERFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250 CHUNKING
AUTH login ██████████ ← Hacked email address in Base64
334 UGFzc3dvcmQ6
██████████ ← Password for hacked email address in Base64
235 2.7.0 Authentication successful
MAIL FROM:<██████████> ← Hacked email address
250 2.1.0 Ok
RCPT TO:<██████████> ← Email address that receives the stolen data
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
```

Following the TCP stream shows the authentication taking place

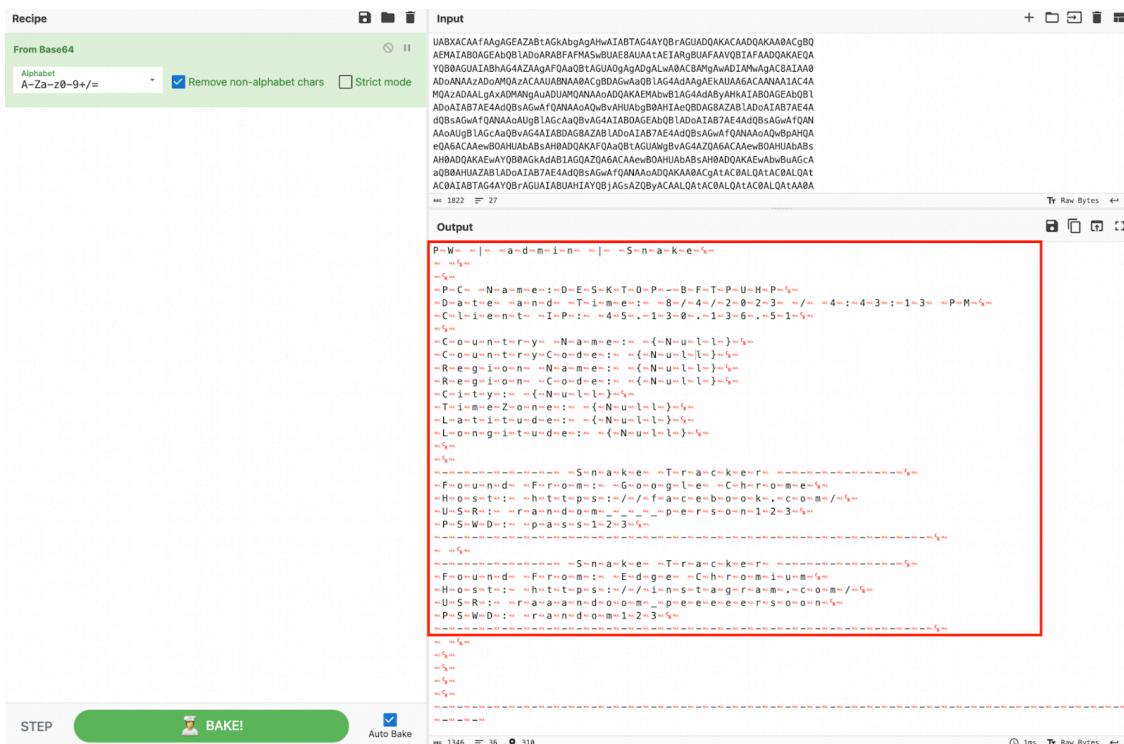
```
MIME-Version: 1.0
From: ██████████ ← Hacked email address sends the stolen data
To: ██████████ ← Email address that receives the stolen data
Date: 4 Aug 2023 16:43:21 +0000
Subject: Pc Name: admin | Snake Tracker ← Subject contains computer's username
Content-Type: multipart/mixed;
boundary=--boundary_0_b54624be-313f-460d-abf5-ae3601c63b62
-----boundary_0_b54624be-313f-460d-abf5-ae3601c63b62
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: quoted-printable
```

A section of the email header

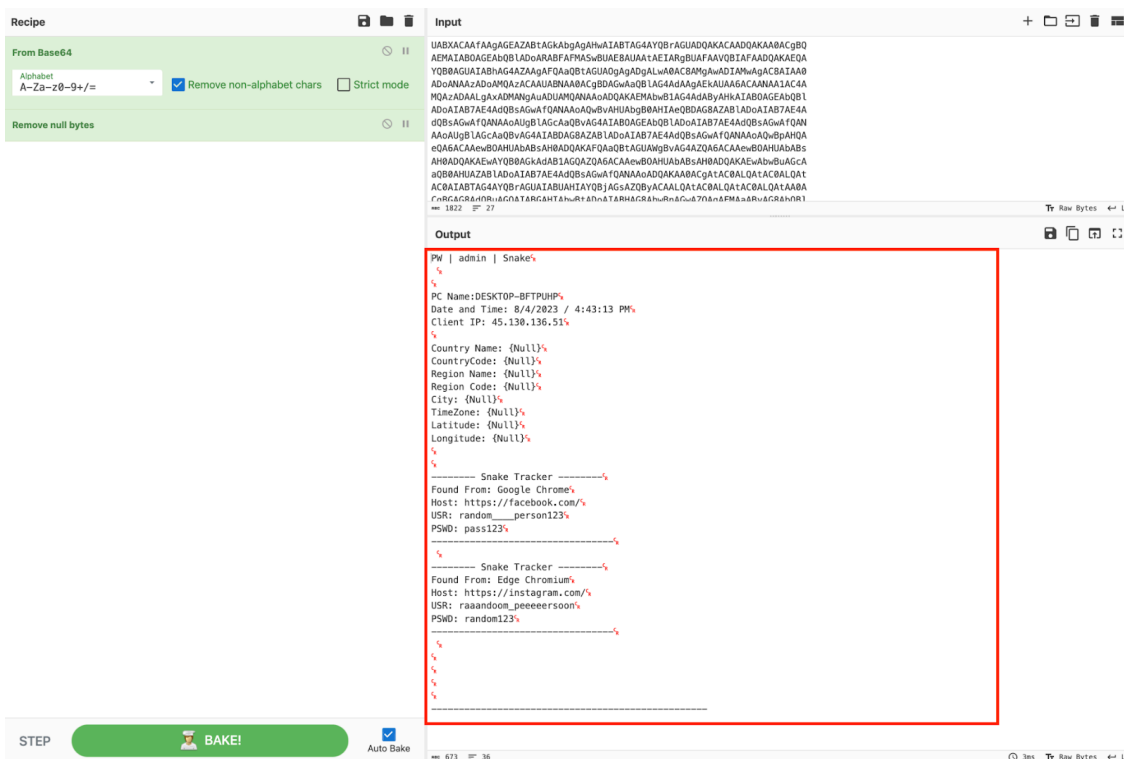
The email has an attachment called “Passwords.txt”, which contains the stolen information. The contents of “Passwords.txt” are in Base64 inside the PCAP as shown:

Decoding the contents of "Passwords.txt"

Decoding the contents of "Passwords.txt" from Base64 on [CyberChef](#) reveals that it contained the computer name ("DESKTOP-BFTPUHP"), the date and time (8/4/2023 4:43:13 PM), IP address (45.130.136[.].51). It also contained the fake credentials that were saved onto Google Chrome and Microsoft Edge:

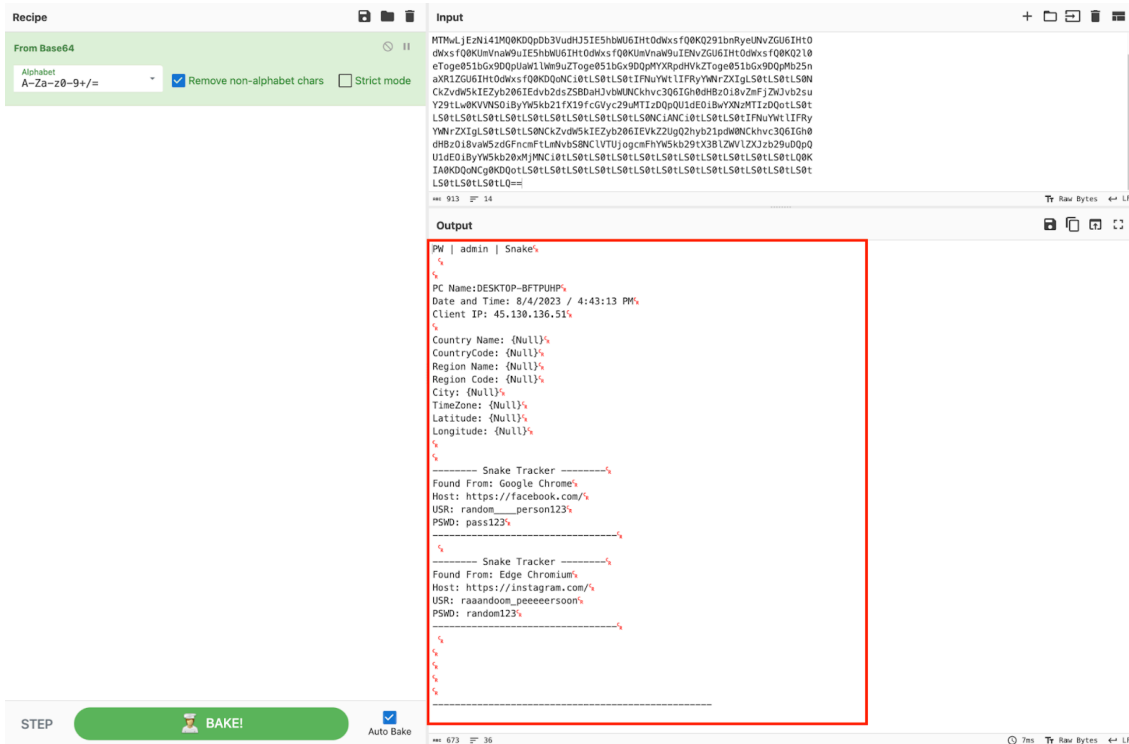


Decoding "Passwords.txt" from Base64 on CyberChef



Removing the null bytes for improved readability

Decoding the contents of “User.txt” from Base64 on CyberChef resulted in something similar to “Passwords.txt”, though it did not contain null bytes, and was in a more human-readable format:



Decoding “User.txt” from Base64 on CyberChef

MITRE ATT&CK

Section goal: In this section, we’ll explore the MITRE ATT&CK for the Snake Keylogger and examine the involved Tactics and Techniques.

The MITRE ATT&CK Matrix for this Snake Keylogger includes five Tactics, namely *Initial Access*, *Execution*, *Credential Access*, *Discovery*, and *Command and Control (C & C)*.



MITRE ATT&CK Matrix

MITRE ATT&CK: Initial Access

Firstly, the phishing email “32b4f238-3516-b261-c3ae-0c570d22ee18.eml” entices the recipient to download and open the attachment via social engineering (as seen in *Analyzing the Email*). The email has a RAR archive

attachment “pago 4094.r09”, which contains an executable file “pago 4094.exe”.

The technique here is [T1566](#) (Phishing), and the subtechnique is [T1566.001](#) (Phishing: Spearphishing Attachment).

MITRE ATT&CK: Execution

The “pago 4094.exe”, namely process 1112, is manually executed by the user. In this case, “pago 4094.exe” was executed by double-clicking the Desktop icon.

The technique here is [T1204](#) (User Execution), and the subtechnique is [T1204.002](#) (User Execution: Malicious File).

The screenshot shows the 'Techniques details' page for T1204 (User Execution). The page is divided into two main sections: 'Subtechniques' and 'Malicious File'. The 'Subtechniques' section is expanded to show '«User Execution»'. Below this, there is a list of 'Permissions required' and a list of 'Data sources'. The 'Malicious File' section is expanded to show a list of processes, with '1112 pago 4094.exe (1)' highlighted in a red box. The page also includes a 'Get to know what this threat is about' section and a 'Other (4)' link.

Techniques details of *User Execution*

MITRE ATT&CK: Credential Access

Process 3868 attempted to steal credentials from web browsers and files. The technique here is [T1555](#) (Credentials from Password stores), and the subtechnique is [T1555.003](#) (Credentials from Password Stores: Credentials from Web Browsers).

Techniques details

Get to know what this threat is about ✕

● Danger (56)

Subtechniques ▼ [T1555](#)

«Credentials from Password Stores»

Permissions required: Administrator

Data sources: Process: Process Access, Process: OS API Execution, File: File Access, Process: Process Creation, Command: Command Execution

Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications that store passwords to make it easier for users manage and maintain. Once

Credentials from Web Browsers ▲

- Steals credentials from Web Browsers (56)
3868 pago 4094.exe (56)

Operation: CREATE
Device: DISK_FILE_SYSTEM
Object: UNKNOWN TYPE
Name: C:\Users\admin\AppData\Local\Amigo\User Data\Default>Login Data
Status: 0xC000003A
Created: SUPERSEDED
Access: FILE_READ_ATTRIBUTES

◀ 1 of 56 ▶

Techniques details of *Credentials from Password Stores*

It is also technique [T1552](#) (Unsecured Credentials), and the subtechnique is [T1552.001](#) (Unsecured Credentials: Credentials In Files).

Techniques details

Get to know what this threat is about ✕

● Danger (134)

Subtechniques ▼ [T1552](#)

«Unsecured Credentials»

Permissions required: User, Administrator, SYSTEM

Data sources: Windows Registry: Windows Registry Key Access, Command: Command Execution, User Account: User Account Authentication, Process: Process Creation, File: File Access

Adversaries may search compromised systems to find and obtain insecurely stored credentials. These credentials can be stored and/or misplaced in many locations on a system, including plaintext files (e.g. [Bash History](#)), operating system or application-specific repositories (e.g. [Credentials in](#)

Credentials In Files ▲

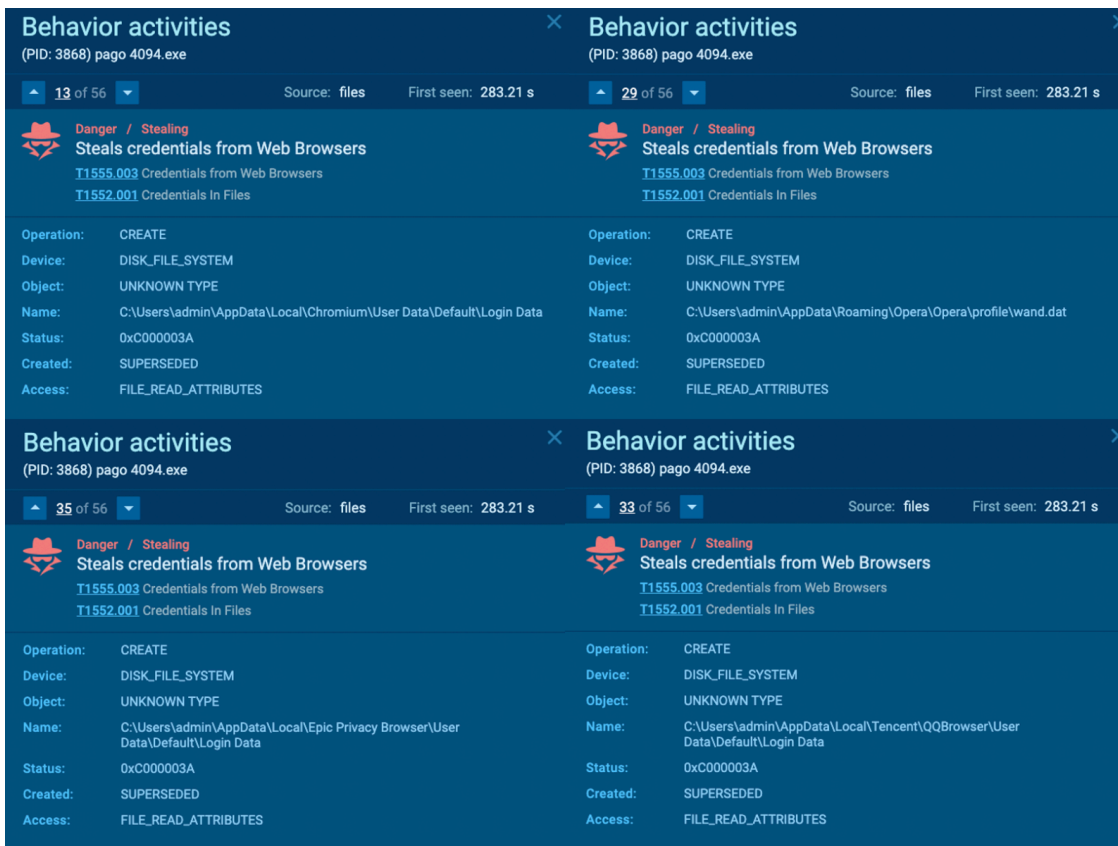
- Steals credentials from Web Browsers (56)
3868 pago 4094.exe (56)
- Actions looks like stealing of personal data (78)
3868 pago 4094.exe (78)

Operation: CREATE
Device: DISK_FILE_SYSTEM
Object: UNKNOWN TYPE
Name: C:\Users\admin\AppData\Local\Yandex\YandexBrowser\User Data\Default\Ya Login Data
Status: 0xC000003A
Created: SUPERSEDED
Access: FILE_READ_ATTRIBUTES

◀ 1 of 78 ▶

Techniques details of *Unsecured Credentials*

Process 3868 attempted “FILE_READ_ATTRIBUTES” access on files associated with browsers under the “C:\Users\admin\AppData\Local\...” and “C:\Users\admin\AppData\Roaming\...” directory.



Process 3868 attempted to steal credentials from Chromium, Opera, Epic Privacy Browser, QQ Browser, etc.

Before executing “pago 4094.exe”, fake credentials were saved in Google Chrome and Microsoft Edge.

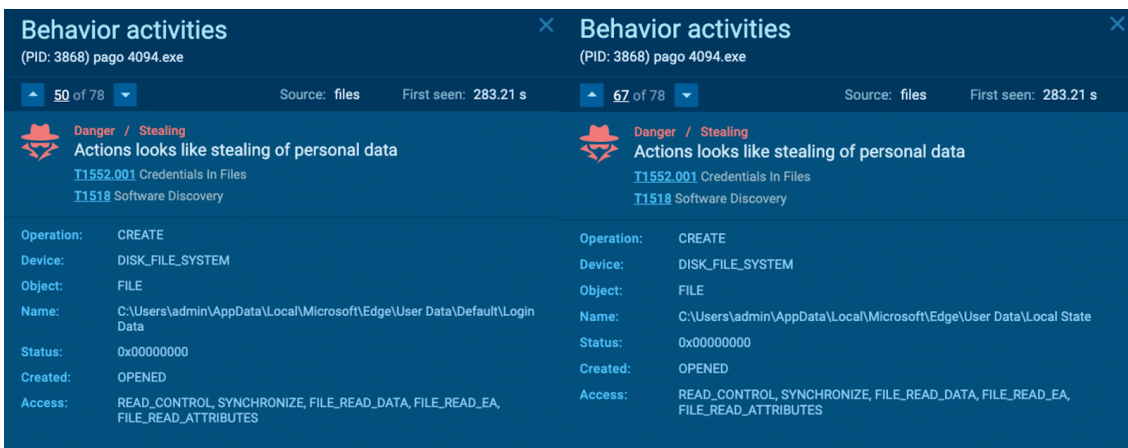
Thus, process 3868 attempted the following accesses on files related to Google Chrome, which were in “C:\USERS\ADMIN\APPDATA\LOCAL\GOOGLE\CHROME\USER DATA\DEFAULT\LOGIN DATA” and “C:\Users\admin\AppData\Local\Google\Chrome\User Data\Local State”:

- FILE_READ_ATTRIBUTES
- READ_CONTROL
- SYNCHRONIZE
- FILE_READ_DATA
- FILE_READ_EA
- FILE_READ_ATTRIBUTES

This process also attempted these accesses on files related to Microsoft Edge, which were in “C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Default\Login Data” and “C:\Users\admin\AppData\Local\Microsoft\Edge\User Data\Local State”:



Data being stolen from Google Chrome



Data being stolen from Microsoft Edge

MITRE ATT&CK: Discovery

Processes 1112 and 3868 attempts to query the registry. The registry contains a lot of crucial system information, such as OS, configuration, software, and security. The technique here is [T1012](#) (Query Registry).

The processes attempted the following:

Techniques details ✕

Get to know what this threat is about ● Danger (24) ● Warning (20) ● Other (19)

T1012

«Query Registry»

Permissions required: User, Administrator, SYSTEM

Data sources: Process: OS API Execution, Process: Process Creation, Command: Command Execution, Windows Registry: Windows Registry Key Access

Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.

The Registry contains a significant amount of information about the operating system, configuration, software, and security. (Citation: Wikipedia Windows Registry)

- Reads the Internet Settings (20)
 - 1112 pago 4094.exe (10)
 - 3868 pago 4094.exe (10)
- Reads the machine GUID from the registry (2)
 - 1112 pago 4094.exe (1)
 - 3868 pago 4094.exe (1)
- Reads the computer name (5)
 - 5416 identity_helper.exe (1)
 - 3640 OfficeClickToRun.exe (1)
 - 5712 identity_helper.exe (1)
 - 1112 pago 4094.exe (1)
 - 3868 pago 4094.exe (1)
- Checks supported languages (5)
 - 5416 identity_helper.exe (1)
 - 3640 OfficeClickToRun.exe (1)
 - 5712 identity_helper.exe (1)
 - 1112 pago 4094.exe (1)
 - 3868 pago 4094.exe (1)

Techniques details of *Query Registry*

Techniques details ✕

Get to know what this threat is about ● Danger (24) ● Warning (20) ● Other (19)

T1012

«Query Registry»

Permissions required: User, Administrator, SYSTEM

Data sources: Process: OS API Execution, Process: Process Creation, Command: Command Execution, Windows Registry: Windows Registry Key Access

Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.

The Registry contains a significant amount of information about the operating system, configuration, software, and security. (Citation: Wikipedia Windows Registry)

- Checks proxy server information (1)
 - 3868 pago 4094.exe (1)
- Reads Environment values (2)
 - 3640 OfficeClickToRun.exe (1)
 - 3868 pago 4094.exe (1)
- Scans artifacts that could help determine the target (24)
 - 3640 OfficeClickToRun.exe (24)
- Reads CPU info (3)
 - 3640 OfficeClickToRun.exe (3)
- Reads Microsoft Office registry keys (1)
 - 3640 OfficeClickToRun.exe (1)

Techniques details of *Query Registry*

Process 1112 and 3868 attempts to discover system information, and tries to gather crucial system information. The technique here is [T1082](#) (System Information Discovery).

There are overlaps between this and the previous subtechnique [T1012](#):

Techniques details ✕

Get to know what this threat is about ● Other (17)

T1082

«System Information Discovery»

Permissions required:

Data sources: Process: OS API Execution, Process: Process Creation, Command: Command Execution

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](#) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully

- Reads the machine GUID from the registry (2)
 - 1112 pago 4094.exe (1)
 - 3868 pago 4094.exe (1)
- Reads Environment values (2)
 - 3640 OfficeClickToRun.exe (1)
 - 3868 pago 4094.exe (1)
- Reads the computer name (5)
 - 5416 identity_helper.exe (1)
 - 3640 OfficeClickToRun.exe (1)
 - 5712 identity_helper.exe (1)
 - 1112 pago 4094.exe (1)
 - 3868 pago 4094.exe (1)
- Checks supported languages (5)
 - 5416 identity_helper.exe (1)
 - 3640 OfficeClickToRun.exe (1)
 - 5712 identity_helper.exe (1)
 - 1112 pago 4094.exe (1)
 - 3868 pago 4094.exe (1)

Techniques details of *System Information Discovery*

Process 3868 attempts to discover installed software, and it attempted to access various locations associated with Browsers. The technique here is [T1518](#) (Software Discovery).

Techniques details ✕

Get to know what this threat is about ● Danger (78)

T1518

«Software Discovery»

Permissions required: User, Administrator

Data sources: Process: OS API Execution, Firewall: Firewall Enumeration, Command: Command Execution, Firewall: Firewall Metadata, Process: Process Creation

Adversaries may attempt to get a listing of software and software versions that are installed on a system or in a cloud environment. Adversaries may use the information from [Software Discovery](#) during automated discovery to shape follow-on behaviors, including whether or not

- Actions looks like stealing of personal data (78)
 - 3868 pago 4094.exe (78)

Operation: CREATE

Device: DISK_FILE_SYSTEM

Object: UNKNOWN TYPE

Name: C:\Users\admin\AppData\Local\Yandex\YandexBrowser\User Data\Default\Ya Login Data

Status: 0xC000003A

Created: SUPERSEDED

Access: FILE_READ_ATTRIBUTES

◀ 1 of 78 ▶

Techniques details of *Software Discovery*

Process 3868 attempts to discover the system network configuration. It checked for external IP, where the destination IP was 158.101.44[.]242 and the destination port was 80. The technique here is [T1016](#) (System Network Configuration Discovery).

Techniques details ×

Get to know what this threat is about ● Warning (1)

[T1016](#)

«System Network Configuration Discovery»

Permissions required:

Data sources: Command: Command Execution, Script: Script Execution, Process: Process Creation, Process: OS API Execution

Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include [Arp](#), [ipconfig/ifconfig](#), [nbtstat](#), and [route](#). Adversaries may also leverage a

● Checks for external IP (1)

3868 pago 4094.exe (1)

Process: C:\Users\admin\Desktop\pago 4094.exe

IpDst: 158.101.44.242

IpSrc: 192.168.100.103

PortDst: 80

PortSrc: 49789

1 of 1

Techniques details of *System Network Configuration Discovery*

MITRE ATT&CK: C&C

Process 3868 then communicates with the application layer protocol. Due to the existing background traffic, communication using the application layer protocols may fly under the radar. It was seen connecting to the SMTP port 587, where the destination IP was 208.91.199[.]225.

The technique here is [T1071](#) (Application Layer Protocol), and the subtechnique is [T1071.003](#) (Application Layer Protocol: Mail Protocols).

The screenshot shows the 'Techniques details' interface for T1071. The title is '«Application Layer Protocol»'. It includes a 'Warning (1)' indicator. Under 'Mail Protocols', there is a bullet point 'Connects to SMTP port (1)' with a red box around the entry '3868 pago 4094.exe (1)'. The 'Process' field is 'C:\Users\admin\Desktop\pago 4094.exe'. Other fields include 'IpDst: 208.91.199.225', 'PortDst: 587', 'PortSrc: 49790', and 'Protocol: TCP'. A navigation bar at the bottom shows '1 of 1'.

Techniques details of *Application Layer Protocol*

Finally, the malware configuration for the Snake Keylogger can be seen in ANY.RUN's *Malware Configuration*:

The screenshot shows the 'Malware configuration' interface for SnakeKeylogger. It includes a description: 'Snake is a modular keylogger written in .NET. Adversaries use this malware to exfiltrate confidential data, such as keystrokes, screen captures, and login credentials.' The configuration is for PID: 3868 pago 4094.exe. It lists 'Keys' (DES: 6fc98cd6) and 'Options' (SMTP User, Password, Host, SendTo, Port). A JSON configuration snippet is shown on the right, including fields for *Keys, *Options, *SMTP User, *SMTP Password, *SMTP Host, *SMTP SendTo, and *SMTP Port.

The *Malware Configuration* for the Snake Keylogger

Conclusion

This analysis showed how a single malicious email can lead to multiple security risks, including financial and reputational damage. We used various techniques like email and attachment analysis, process and network analysis, and applied the MITRE ATT&CK.

The focus was on an email with a Snake Keylogger attachment. It collects system info, establishes persistence, steals credentials, and exfiltrates data.

Given that emails remain a top threat vector often exploiting human error, staying vigilant against email threats is crucial.

About ANY.RUN

ANY.RUN is a cloud malware sandbox that handles the heavy lifting of malware analysis for SOC and DFIR teams. Every day, 300,000 professionals use our platform to investigate incidents and streamline threat analysis.

Request a demo today and enjoy 14 days of free access to our Enterprise plan.

[Request demo →](#)

Appendix 1: IOCs

Analyzed files:

Name	32b4f238-3516-b261-c3ae-0c570d22ee18.eml
MD5	60D00C17D3EA15910893EEF868DE7A65
SHA1	1D17DD1688A903CBE423D8DE58F8A7AB7ECE1EA5
SHA256	D13A7EAAF07C924159EA7BB8F297DAB1D8DA0F9AF46E82E24052D6A9BF5E4087
SSDEEP	12288:vZ1Tzm0D2acQLqgVIjejueFyhaCV2JKKS7hoxSSqkljhEi9lV7j:z7K8FuuzCV2JKkxPOQ3
Name	pago 4094.exe
MD5	1A0F4CC0513F1B56FEF01C815410C6EA
SHA1	A663C9ECF8F488D6E07B892165AE0A3712B0E91F
SHA256	D483D48C15F797C92C89D2EAFCC9FC7CBE0C02CABE1D9130BB9069E8C897C94C
SSDEEP	12288:PXPZDbCo/k+n70P4uR87fD0iBTJj1ijFDTwA:hOz+IPz6/PF1ihDTwA

Connections:

- 158.101.44[.]242 • *checkip.dyndns[.]org*
- 208.91.199[.]255 • *us2.smtp.mailhostbox[.]com*

Appendix 2: MITRE MATRIX

Tactics	Techniques	Description
TA0001: Initial Access	T1566: Phishing	Send phishing messages to gain access to victim systems.
TA0002: Execution	T1204: User Execution	Rely upon specific actions by a user in order to gain execution.
TA0006: Credential Access	T1555: Credentials from Password Stores	Search for common password storage locations to obtain user credentials.
	T1552: Unsecured Credentials	Search compromised systems to find and obtain insecurely stored credentials.
TA0007: Discovery	T1012: Query Registry	Interact with the Windows Registry to gather information.
	T1082: System Information Discovery	Get detailed information about the operating system and hardware.
	T1518: Software Discovery	Get a listing of software and software versions that are installed.
	T1016: System Network Configuration Discovery	Look for details about the network configuration and settings.
TA0011: Command and Control	T1071: Application Layer Protocol	Communicate using OSI application layer protocols to avoid detection.

 lena-aka-lambdamamba

Lena aka LambdaMamba

Chief Research Officer

I am a Chief Research Officer at a cybersecurity company. My passions include investigations, experimentations, gaming, writing, and drawing. I also like playing around with hardware, operating systems, and FPGAs. I enjoy assembling things as well as disassembling things! In my spare time, I do CTFs, threat hunting, and write about them. I am fascinated by snakes, which includes the Snake Malware! Check out:

- [My website](#)
- [My LinkedIn profile](#)

Source: https://any.run/cybersecurity-blog/analyzing-snake-keylogger/