Lumma Stealer Threat Analysis

Malware analysis, TTPs, IoCs and security measures

Author:

Ángel Luis Rodríguez Martín-Palomino

Table of Contents

Introduction **3**
Executive Summary 3
Malware Analysis **4**
Virus Total 4
Any.RUN 8
Joe Sandbox 11
Intelligence and Artifacts **13**
Attack Vectors 13
TTPs 14
IoCs 15
Conclusions and Recommendations **16**
References **17**

List of Figures

Figure 1. VirusTotal analysis of the Lumma Stealer sample 4
Figure 2. Domains contacted by the LummaStealer executable 5
Figure 3. URLs contacted by the sample 6
Figure 4. Summary of the Lumma Stealer sample's activity 6
Figure 5. Discovery tactic used by the sample 6
Figure 6. Clipboard read by a process of the executable 7
Figure 7. Attempt by the sample to establish itself as an AutoRun 7
Figure 8. Alerts generated by IDS rules 7
Figure 9. Suspicious operating system calls 8
Figure 10. Alerts generated by ANY.RUN when executing the sample 8
Figure 11. ANY.RUN process graph 9
Figure 12. Analysis of the core.exe process in ANY.RUN 10
Figure 13. Communications of the core.exe process in ANY.RUN 10
Figure 14, C2 domain contacted by the sample in ANY.RUN 11
Figure 15. Joe Sandbox report types 11
Figure 16. Malware classification diagram in Joe Sandbox 12
Figure 17. Registry keys accessed by the sample in Joe Sandbox 12
Figure 18. Creation of the core.exe process by KMSPico 13
Figure 19. Example of a ClickFix message 14
Figure 20. Lumma Stealer TTPs in ANY.RUN 14

Introduction

This report aims to carry out a basic analysis of a sample of the *Lumma Stealer* malware using online tools and *sandbox* platforms such as ANY.RUN, Joe Sandbox or VirusTotal, so that a detailed study of the malware's behavior can be carried out safely in a virtualized environment.

Specifically, the sample was obtained from *Malware Bazaar* at the following link.

File Name	KMSPico.exe
MD5	56c6b5cb4714c8754c2721a4fd794522
SHA256	fcf8d40fe2db604954c51451d753a0e965996c43154bf506fdbdfbb3885ffce4

This sample was chosen over others because of its high number of recent victims: according to official sources, more than 394,000 Windows computers were affected by this family between March 16 and May 16, 2025.

Executive Summary

THREAT	***Lumma Stealer***
MODEL	MaaS
COUNTRY OF ORIGIN	Russia
FIRST SEEN	2022
MOTIVATION	Information Theft
ATTACK VECTOR	*Phishing / Fake Captcha / Trojan*
TARGET SYSTEM	Windows
IMPACT	**HIGH**

Lumma Stealer is an *Info Stealer*-type malware, that is, one whose main goal is to steal confidential information from infected devices. It usually disguises itself as a seemingly benign application or file, such as a browser extension or, in the case of this sample, a Windows license activator, in order to gain access to systems and carry out its malicious actions.

It is a MaaS (*Malware-as-a-Service*), and according to official researchers it is believed to be of Russian origin, since it began to be distributed on Russian-speaking forums from at least August 2022. The information it tries to access is highly varied and depends on the sample, but it generally focuses on:

- Cryptocurrency wallets.
- 2FA browser extensions.
- Capture of sensitive information such as credentials or credit cards through keystroke logging.
- Sensitive documents, photos and videos.
- Clipboard contents.

Once the target data has been obtained, it is exfiltrated to a C2 via `HTTP POST` requests using the user agent "`TeslaBrowser/5.5`". In addition, it has other capabilities besides information theft, such as taking control of the infected device to download and install other malware, evasion techniques such as obfuscation and encryption, and it is even capable of adding a backdoor to the device so that it becomes part of a *botnet* of infected computers.

Malware Analysis

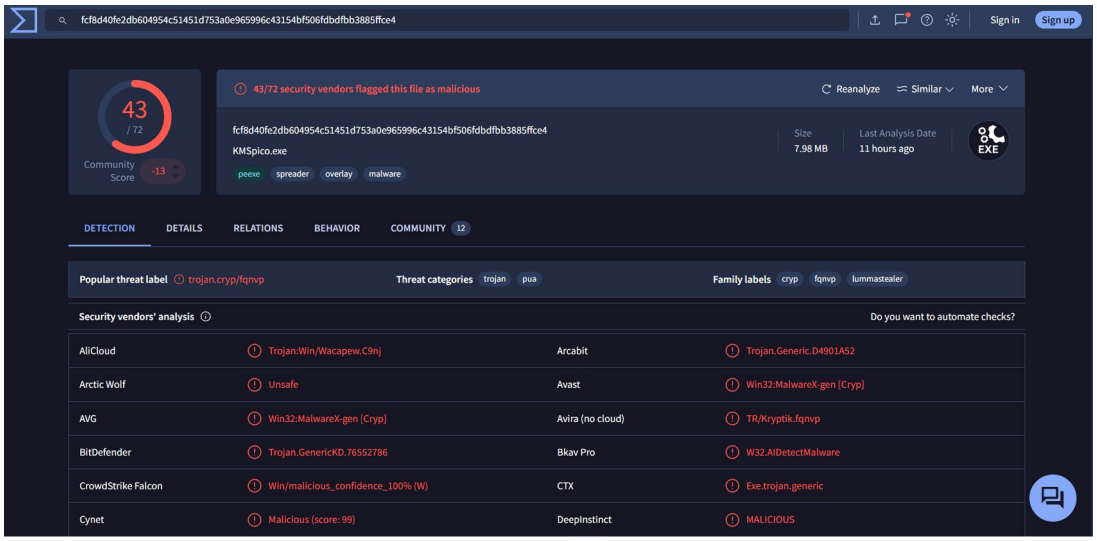
This section analyzes the malware using different online platforms in order to identify its capabilities, infection stages, TTPs, IoCs, attack vectors and, in general, how this threat works at a high level and what changes it makes to the system.

Virus Total

VirusTotal is an *online* platform that allows files to be scanned based on their hash, so that the verdict of a large number of antivirus vendors on the legitimacy of the resource can be obtained. It also integrates *sandboxing* sections that make it possible to extract *insights* about the application's behavior, in this case, such as its network connections or file access/modification. In short, it is a very useful option as a first contact with a sample to get an overview of what is being dealt with, and it serves to quickly obtain TTPs and IoCs.

Below is an image of the result of scanning the sample in VirusTotal.

Figure 1. *VirusTotal analysis of the Lumma Stealer sample.*

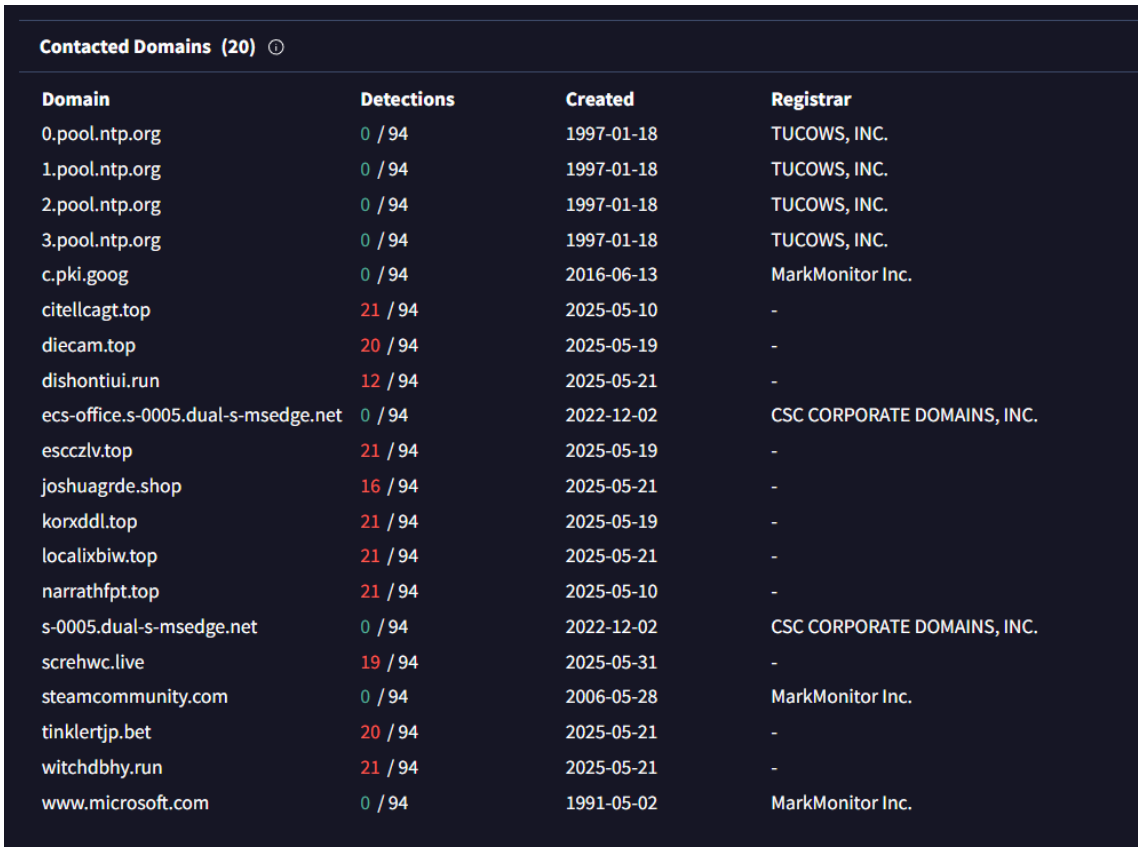


As can be seen, the results are not very encouraging: the sample has been flagged as malicious by 43 of the 75 security vendors on VirusTotal and by 13 community users.

Furthermore, at a glance we can see that the sample has been classified as a trojan, and tags have been added that may indicate methods used by the malware, such as *overlays* and *spreader*, that is, it has the capability to spread to other devices.

In the relations section we can see the communications made by the executable at the IP or domain level.

Figure 2. *Domains contacted by the LummaStealer executable.*



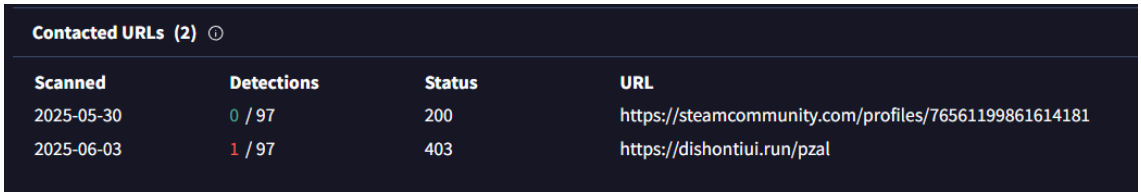
Contacted Domains (20)

Domain	Detections	Created	Registrar
0.pool.ntp.org	0 / 94	1997-01-18	TUCOWS, INC.
1.pool.ntp.org	0 / 94	1997-01-18	TUCOWS, INC.
2.pool.ntp.org	0 / 94	1997-01-18	TUCOWS, INC.
3.pool.ntp.org	0 / 94	1997-01-18	TUCOWS, INC.
c.pki.goog	0 / 94	2016-06-13	MarkMonitor Inc.
citellcagt.top	21 / 94	2025-05-10	-
diecam.top	20 / 94	2025-05-19	-
dishontiui.run	12 / 94	2025-05-21	-
ecs-office.s-0005.dual-s-msedge.net	0 / 94	2022-12-02	CSC CORPORATE DOMAINS, INC.
escczlv.top	21 / 94	2025-05-19	-
joshuagrde.shop	16 / 94	2025-05-21	-
korxddl.top	21 / 94	2025-05-19	-
localixbiw.top	21 / 94	2025-05-21	-
narrathfpt.top	21 / 94	2025-05-10	-
s-0005.dual-s-msedge.net	0 / 94	2022-12-02	CSC CORPORATE DOMAINS, INC.
screhwc.live	19 / 94	2025-05-31	-
steamcommunity.com	0 / 94	2006-05-28	MarkMonitor Inc.
tinklertjp.bet	20 / 94	2025-05-21	-
witchdbhy.run	21 / 94	2025-05-21	-
www.microsoft.com	0 / 94	1991-05-02	MarkMonitor Inc.

In this case, since this is a `KMSPico.exe` that runs on Windows systems to activate licenses, some of the contacted domains are legitimate, such as Microsoft, msedge or the NTP servers. However, most of the domains have rather strange names and are flagged as malicious by several vendors. In fact, when looking at the community comments on these domains, it is common to find references to *Lumma Stealer*, which seems to indicate that they may be part of the infrastructure used by the malware.

Also noteworthy in this relations section are the contacted URLs, among which is one from the famous video game distribution platform Steam, specifically, the profile of a community user.

Figure 3. *URLs contacted by the sample.*



Contacted URLs (2)

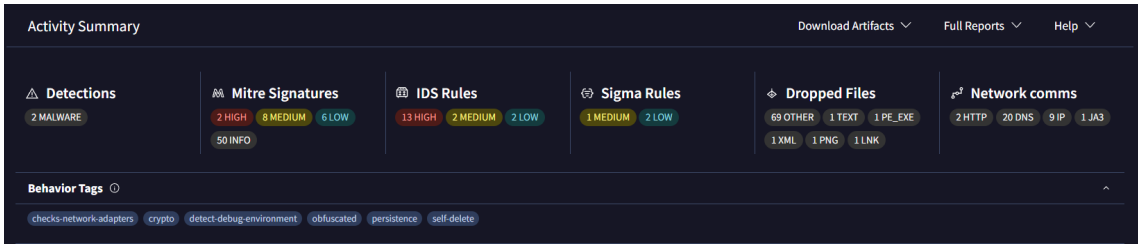
Scanned	Detections	Status	URL
2025-05-30	0 / 97	200	https://steamcommunity.com/profiles/76561199861614181
2025-06-03	1 / 97	403	https://dishontiui.run/pzal

At first glance, this URL appears to be completely legitimate, since Steam is a company with several years in the industry, but after investigating it more closely, it appears to be

one of the "*fallback*" servers used to exfiltrate information, as indicated by official Microsoft reports[1].

While the relations section is very useful, perhaps the most interesting section of VirusTotal is *Behaviour*, since that is where all the intelligence generated by the different *sandbox* providers is gathered. In the following image we can see a summary of the sample's activity.

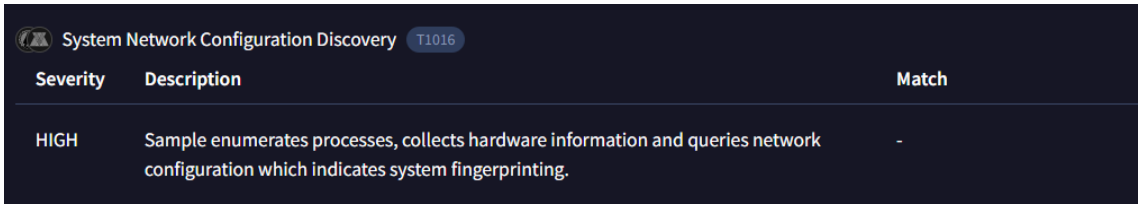
Figure 4. *Summary of the Lumma Stealer sample's activity.*



The previous image shows how the executable has triggered several MITRE tactic and technique signatures and 13 high-risk IDS rules, and how it has installed several files and communicated with several hosts.

Below are some of the techniques classified as most dangerous by MITRE in VirusTotal.

Figure 5. *Discovery tactic used by the sample.*

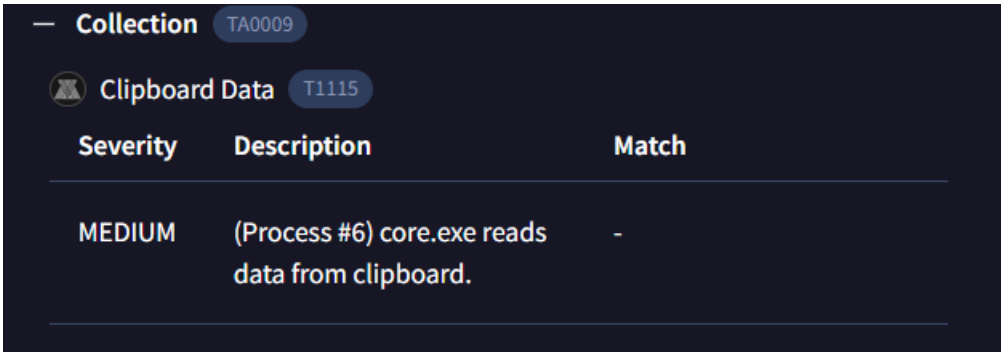


The previous image shows how the sample uses technique `T1016` to obtain information about internal processes on the machine, hardware information, network configuration and, in general, *fingerprinting* actions, which are typically used as one of the first phases to profile the victim and know how to act accordingly.

We can also see that one of the created processes reads the contents of the clipboard, which often contains copied sensitive information.

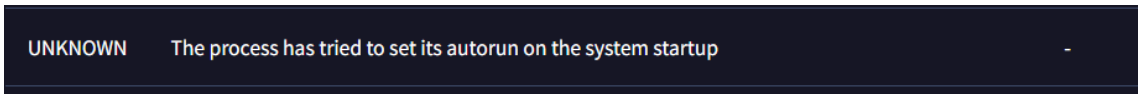
[1] The "C2 Communication" section of the following link shows how the Steam server is mentioned as an alternative C2, https://www.microsoft.com/en-us/security/blog/2025/05/21/lumma-stealer-breaking-down-the-delivery-techniques-and-capabilities-of-a-prolific-infostealer/

Figure 6. *Clipboard read by a process of the executable.*



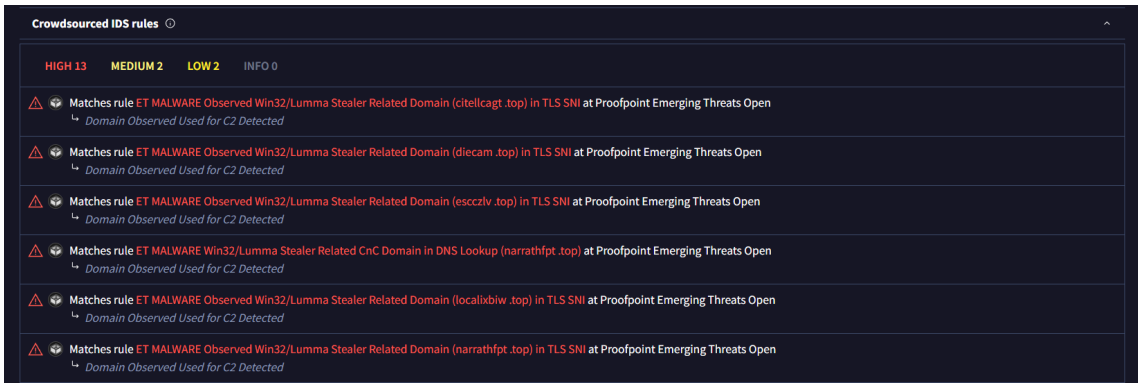
Or, for example, how it has tried to establish itself as an `AutoRun`, which is usually a way of gaining persistence on the system.

Figure 7. *Attempt by the sample to establish itself as an AutoRun.*



As for the IDS rules shown in the following image, most appear to be triggered by interactions with domains flagged as part of the *Lumma Stealer* infrastructure, detected through the TLS SNI field.

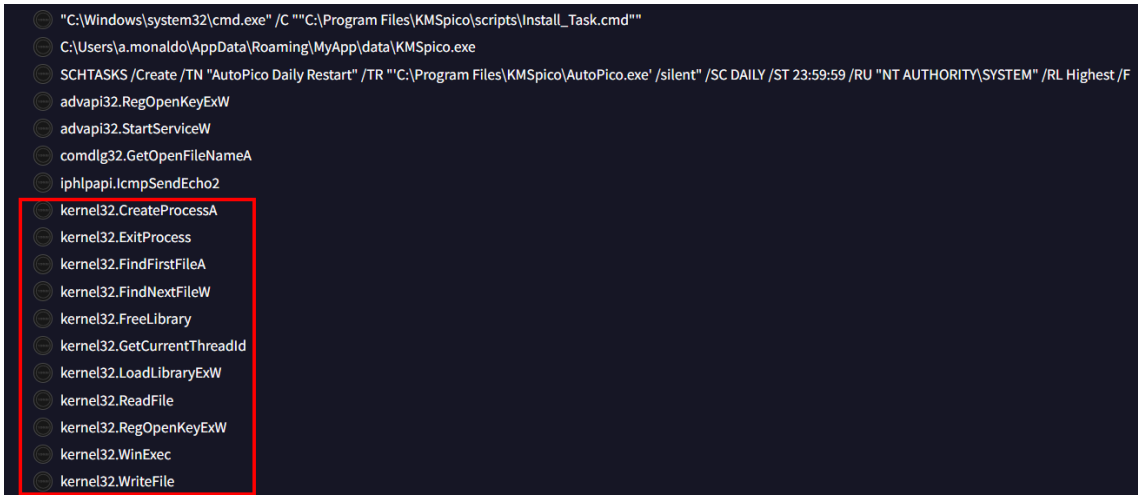
Figure 8. *Alerts generated by IDS rules.*



Finally, the *Highlighted Actions* section in Virus Total is worth highlighting, as it shows us actions executed by the sample that are considered suspicious, whether due to the use of cryptography or because they make certain operating system calls.

The following image shows an excerpt of those actions, among which the creation of an *AutoPico* service with administrator privileges and certain calls to the Windows `kernel32` API stand out. The creation of the service may be something “normal”, since the sample is a `KMSPico.exe` file, so it may be an action required to perform its function. However, the use of `kernel32` calls such as `CreateProcessA`, `LoadLibraryExW`, `RegOpenKeyExW` or `WinExec` is very common in malware to create other malicious processes or modify registry keys; while this is not entirely conclusive, since these calls can be used legitimately, it is noteworthy and worth mentioning.

Figure 9. *Suspicious operating system calls.*

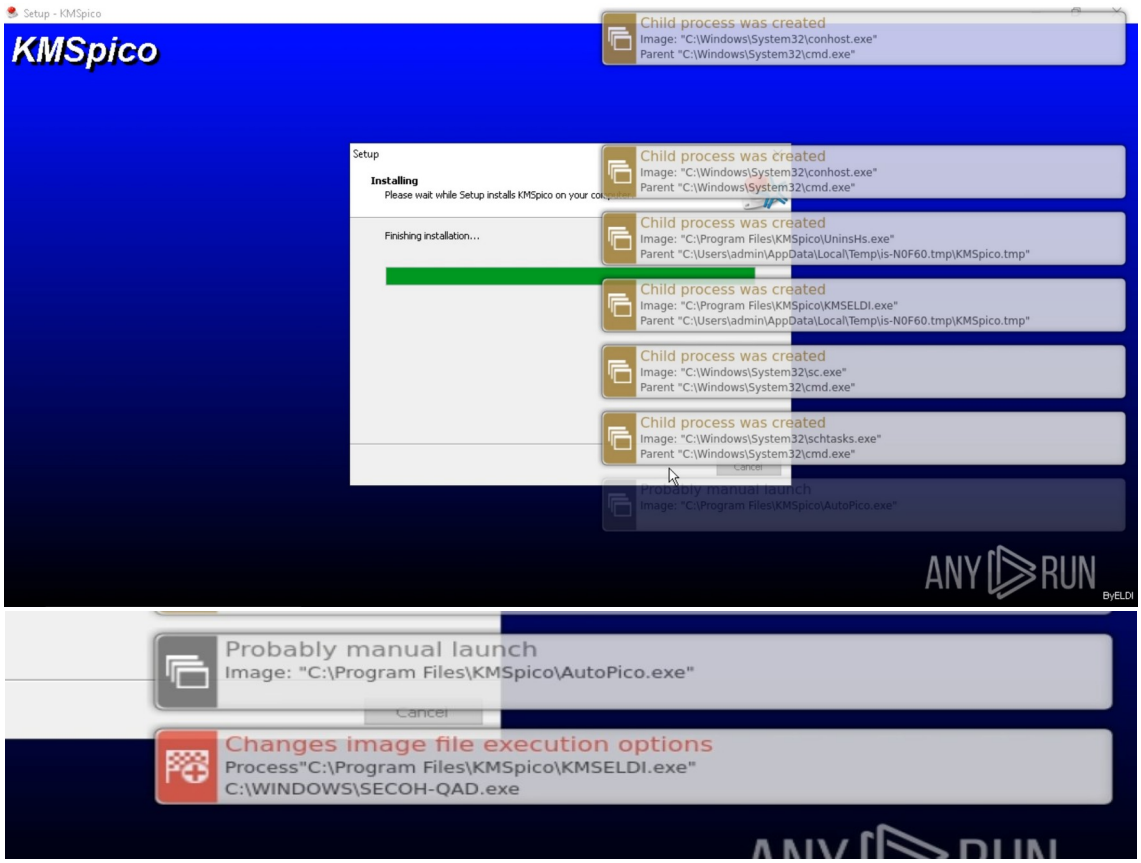


Any.RUN

Another tool that can be used after carrying out a preliminary analysis with VirusTotal is ANY.RUN. The strength of this solution is, among other things, that it allows you to interact through the browser with the desktop of the deployed machine and visualize the changes to the system graphically.

Below you can see the interaction with the sample's `KMSPico.exe` program and how multiple alerts appear in ANY.RUN when the process finishes.

Figure 10. *Alerts generated by ANY.RUN when executing the sample.*



Another strength of ANY.RUN is that it lets us visualize, by means of a graph, the creation flow of the different processes and services, as shown in the following image.

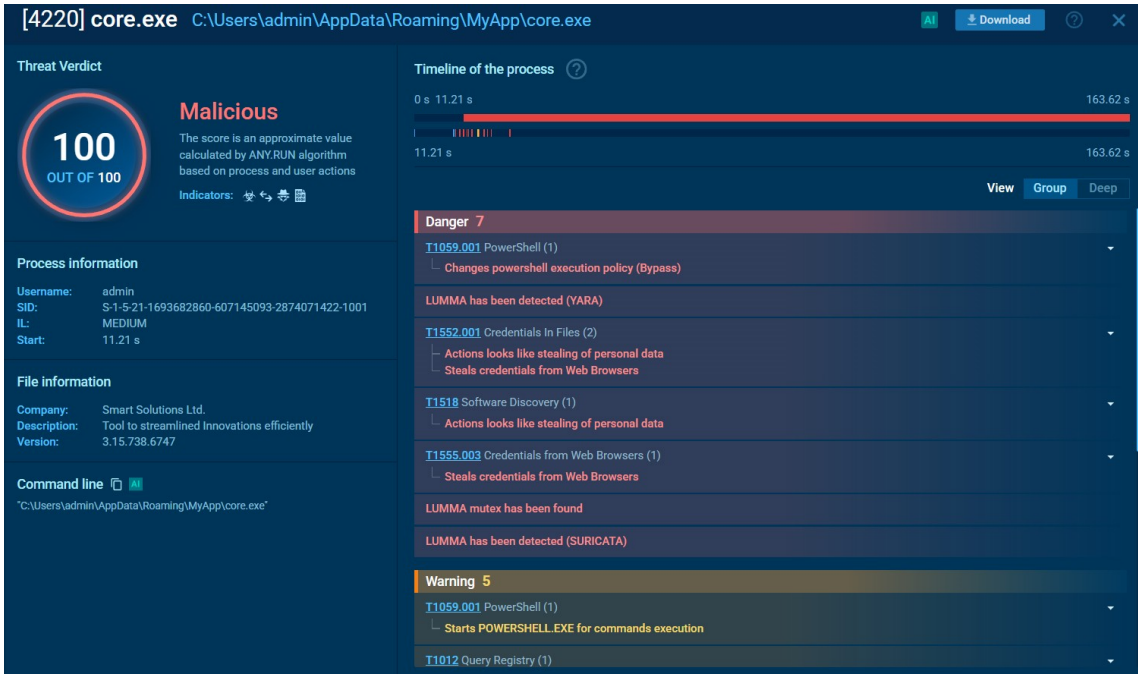
Figure 11. *ANY.RUN process graph.*



The previous image shows how, after the `KMSPico.exe` process is executed, two branches of processes are created. The upper one appears to correspond to the normal installation flow of the KMSPico license activator. However, at the same time as that branch is created, so is the `core.exe` process, which is tagged as `#LUMMA` by ANY.RUN and is 100/100 malicious.

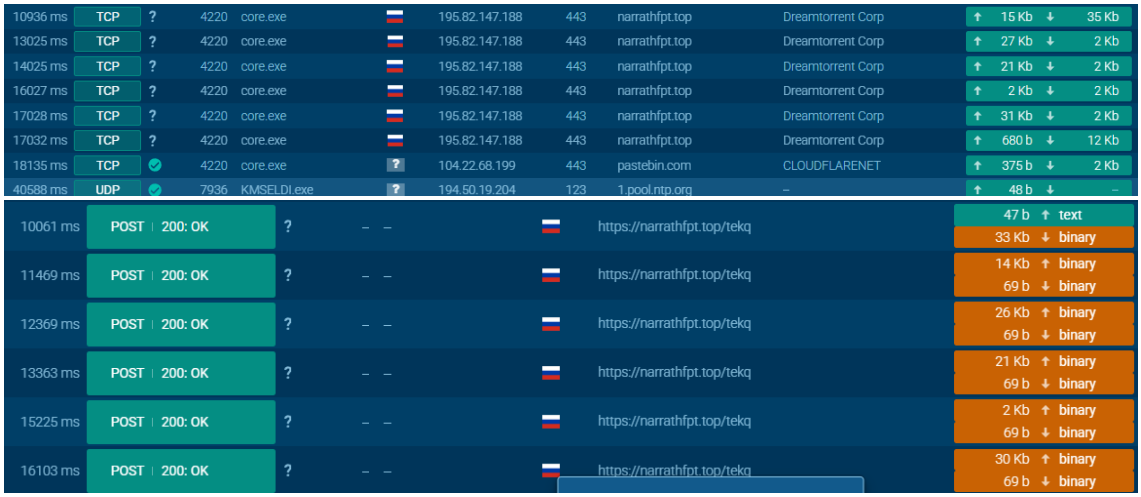
Looking more closely at the `core.exe` process, it turns out that it uses different MITRE techniques, such as creating a PowerShell process with `powershell -exec bypass` to enable script execution from the terminal, and searching for sensitive personal data in files and web browsers. It also triggers some YARA rules and SURICATA alerts, as shown in the following image.

Figure 12. *Analysis of the core.exe process in ANY.RUN.*



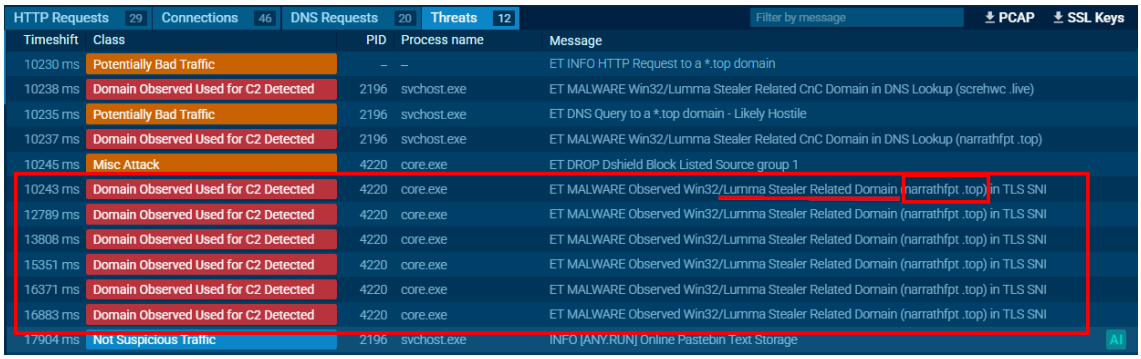
It is also worth noting how this process appears to communicate with a series of Russian IPs through the domain `narrathtfpt[.]top`, which makes sense given the origin of this threat.

Figure 13. *Communications of the core.exe process in ANY.RUN.*



In fact, this domain is flagged in ANY.RUN as a C2 server used by *LummaStealer*.

Figure 14, *C2 domain contacted by the sample in ANY.RUN.*

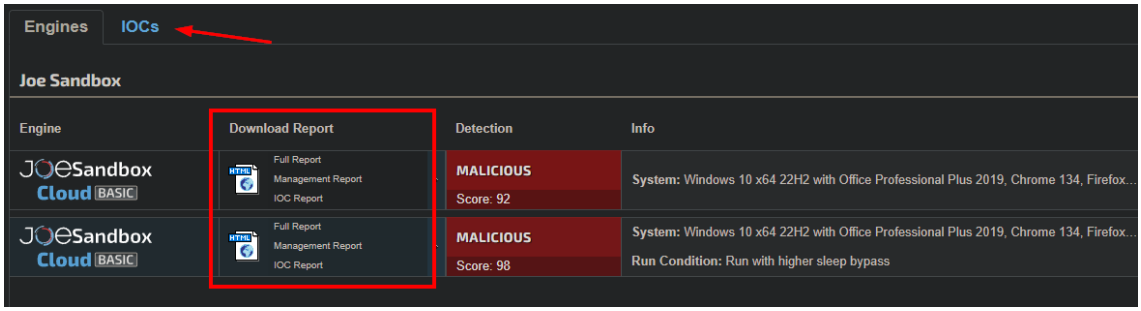


Joe Sandbox

Apart from VirusTotal and ANY.RUN, there are many online tools that allow basic malware analysis to be performed in a *sandbox*. To highlight one of them, perhaps the best known among the alternatives, Joe Sandbox will be used in this section. However, since it is the same sample, the results obtained by the different tools are very similar, so only a few interesting sections of this tool will be provided.

One of the advantages of Joe Sandbox is that it can generate an online report in HTML format summarizing the findings of the analysis at several levels, with more or less condensed information and a different presentation.

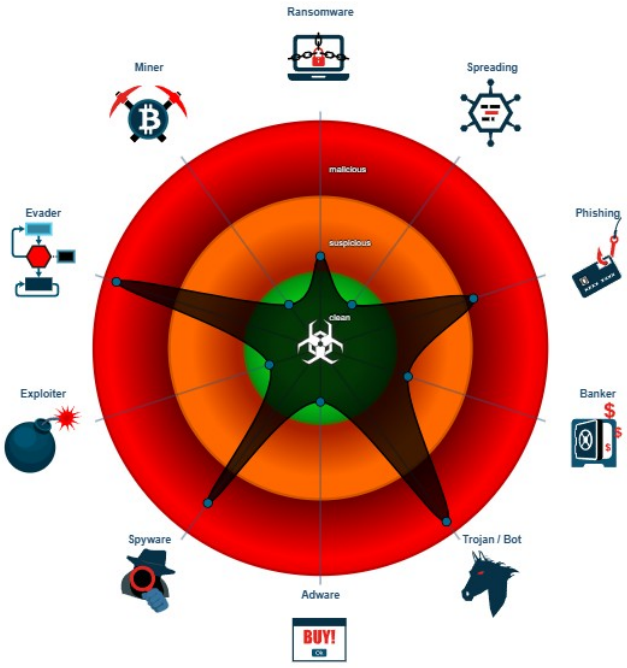
Figure 15. *Joe Sandbox report types.*



The previous image shows that there is a complete report with all the information (*Full Report*), a more concise one for management (*Management Report*) and another one for the IoCs, as well as another specific tab.

In the findings of the full report we can see information ranging from more general to more specific depending on the need. For example, the first section shows the classification of the *malware* in a diagram so that we can quickly know what type of sample we are dealing with and its capabilities.

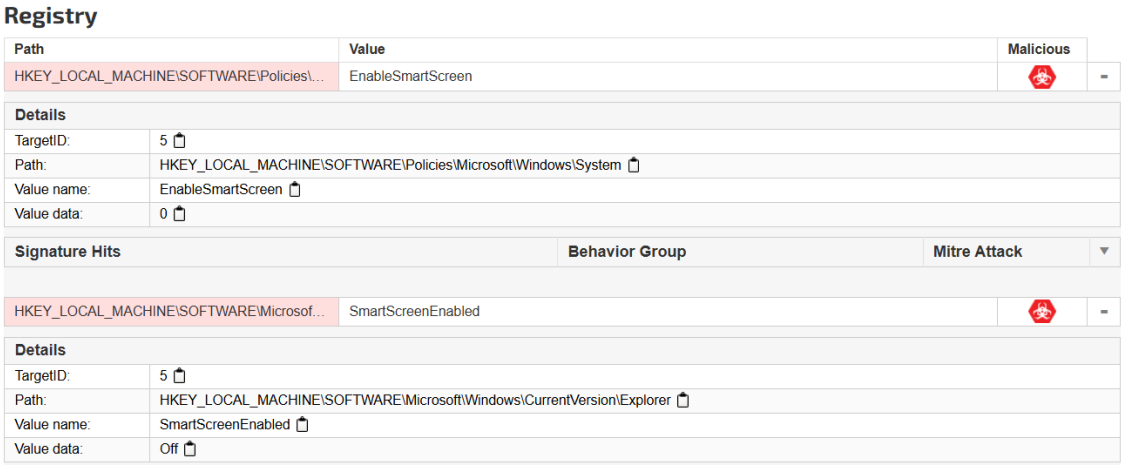
Figure 16. *Malware classification diagram in Joe Sandbox.*



In the case of this sample, as can be seen in the previous image, it is a trojan/spyware with evasion capabilities that uses techniques such as phishing for intrusion.

Much more specific information can also be obtained, such as the registry keys accessed or modified, in the tool's IoC report.

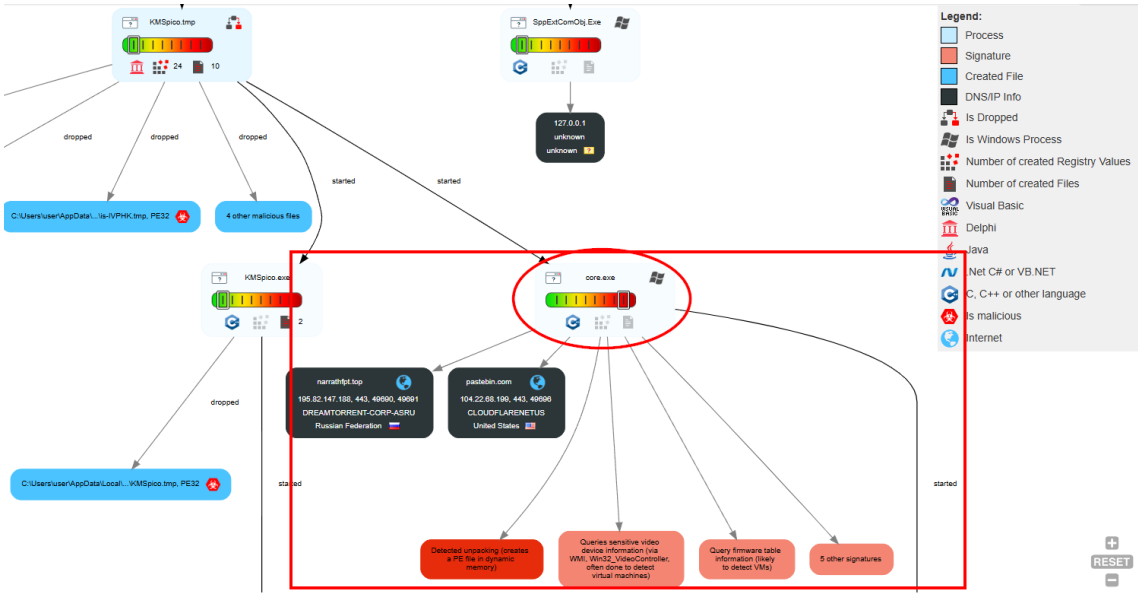
Figure 17. *Registry keys accessed by the sample in Joe Sandbox.*



The previous image shows that keys related to the *SmartScreen* feature of the infected Windows device were accessed with the aim of disabling its protection, since this is a Microsoft Defender feature that blocks malicious or phishing sites and prevents files from being downloaded from untrusted Internet sources.

Finally, one of the most powerful features of this tool is the behavior graph, which shows the different processes created by the sample, the connections, and its actions and capabilities in text. Given the size of this graph, only an excerpt showing the creation of the core.exe process and its actions will be shown; however, a link to the report is attached so that the full graph can be viewed.

Figure 18. *Creation of the core.exe process by KMSPico.*



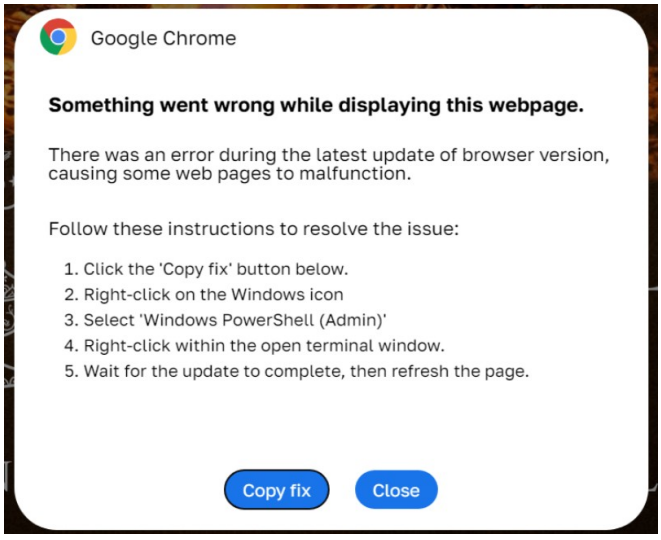
Intelligence and Artifacts

Attack Vectors

Lumma Stealer deploys a wide range of delivery techniques that evolve and adapt over time in order to evade defenses and improve the success of infections. Some of the attack vectors used by this threat to infect its victims are listed below.

- **Phishing/Email:** These are usually emails impersonating a well-known entity and containing a link or attachment that holds the payload. They are typically characterized by creating a sense of urgency or offering some kind of incentive to interact quickly with the *email*.
- **Malvertising**: Fraudulent ads are sometimes used to promote an update for an application such as the Chrome web browser, but they actually lead to a cloned web page that downloads the *stealer*.
- **ClickFix**: This consists of tricking the user through social engineering into running a base64-encoded PowerShell script in the system's Run window, usually as a way of verifying a captcha or fixing errors. In reality, this launches a command that downloads Lumma Stealer and runs it in memory.

Figure 19. *Example of a ClickFix message.*

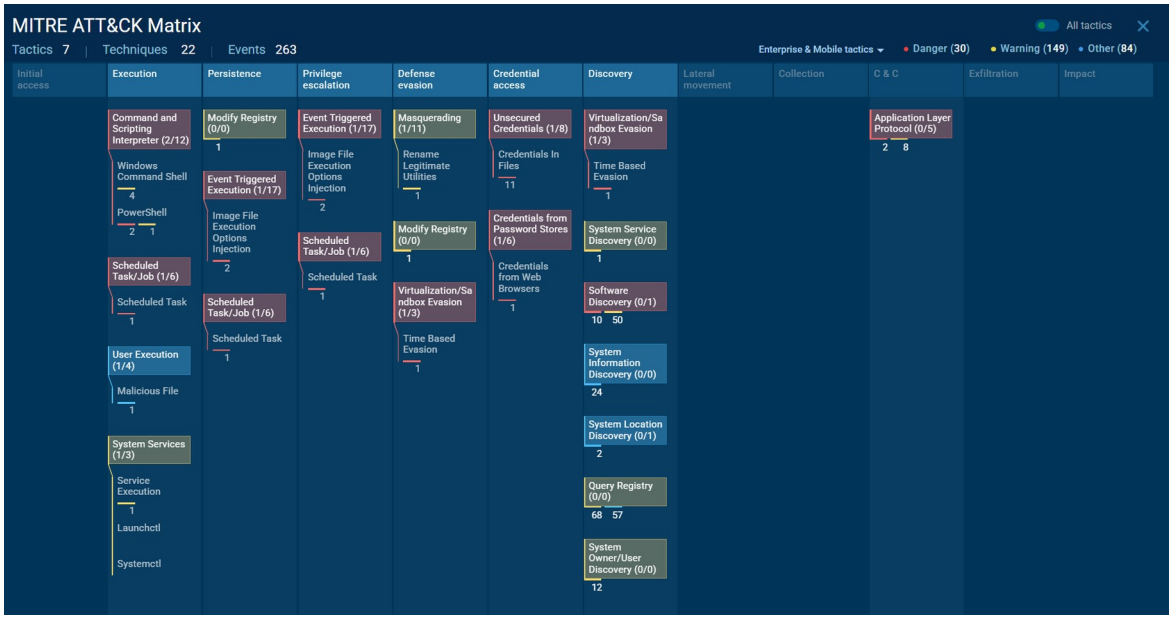


- **Trojanized applications**: Some campaigns use *pirated* versions of legitimate software in which the *stealer* is bundled, and they are distributed through file-sharing platforms. These campaigns are stealthier, since there is no visible element when running the target software. This is the case of the KMSPico sample.

TTPs

Below is the MITRE matrix with the Tactics, Techniques and Procedures used by the sample's malware during execution in ANY.RUN.

Figure 20. *Lumma Stealer TTPs in ANY.RUN*



IoCs

Indicator	Type	Description
`escczlv[.]top`	Domain	Lumma Infrastructure Domain
`narrathtfpt[.]top`	Domain	Lumma Infrastructure Domain
`screhwc[.]live`	Domain	Lumma Infrastructure Domain
TeslaBrowser/5.5	User Agent	Lumma C2 POST Request
144.76.173[.]247	IP	Lumma Stealer C2 Infrastructure
45.9.74[.]78	IP	Lumma Stealer C2 Infrastructure
77.73.134[.]68	IP	Lumma Stealer C2 Infrastructure
82.117.255[.]127	IP	Lumma Stealer C2 Infrastructure
`C:\Users\user\AppData\Roaming\MyApp\core.exe`	Process	Malware `core.exe` process.
`HKLM\SOFTWARE\Policies\Microsoft\Windows\System`	Registry	Registry key accessed by Lumma Stealer
`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer`	Registry	Registry key accessed by Lumma Stealer
`C:\Users\user\AppData\Local\Temp\is-00FUR.tmp\KMSpico.tmp`	File	File installed by the sample.

Conclusions and Recommendations

After analyzing a sample of the *Lumma Stealer* malware using different online *sandboxing* tools such as ANY.RUN, VirusTotal or Joe Sandbox, a number of conclusions have been drawn.

This is a sophisticated threat designed to extract credentials, browsing data and critical files from infected systems. Its ability to evade detection through obfuscation, encryption and persistence techniques highlights the importance of having advanced security solutions as well as continuous monitoring processes. The speed with which this malware can compromise user accounts and facilitate lateral movement across the network underscores the risk of operational disruptions and possible leaks of strategic information, which could lead to a significant reputational and financial impact for the organization.

To mitigate the impact that an infection by this type of malware can have, it is recommended to follow a defense-in-depth approach, starting with a continuous cybersecurity training and awareness plan for staff to prevent attack vectors such as *phishing*, *fake captcha*, *clickflix* or trojanized applications.

The deployment of advanced endpoint security systems such as EDR is also recommended, which not only detect and block known attacks based on signatures but also leverage the power of artificial intelligence to detect anomalies and prevent infections. Likewise, networks should be properly segmented to prevent the rapid spread of the *malware*. Finally, it is recommended to apply access control lists, role-based access control (RBAC) and to have at least a second authentication factor. However, these measures must be adapted and implemented according to the specific needs and capabilities of the organization.

References

- Intelligence report on Lumma Stealer delivery methods, *Microsoft*, https://www.microsoft.com/en-us/security/blog/2025/05/21/lumma-stealer-breaking-down-the-delivery-techniques-and-capabilities-of-a-prolific-infostealer/
- VirusTotal analysis, https://www.virustotal.com/gui/file/fcf8d40fe2db604954c51451d753a0e965996c43154bf506fdbdfbb3885ffce4/behavior
- ANY.RUN analysis, https://app.any.run/tasks/ec9a9a09-0415-4e36-8e5a-5456740a8118/
- Joe Sandbox analysis, https://www.joesandbox.com/analysis/1707440
- Information about Lumma Stealer, *Incibe*, https://www.incibe.es/servicio-antibotnet/info/LummaStealer
- Malware description, *Malpedia*, https://malpedia.caad.fkie.fraunhofer.de/details/win.lumma