SORINT SEC

THREAT HUNTING

LAB

WEEK 10/02/2025 - 14/02/2025

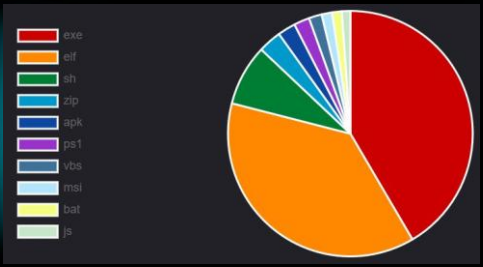
PUBLIC

Index

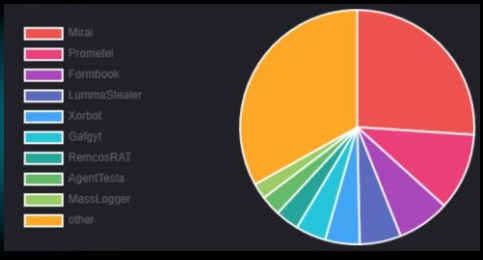
Global Weekly Threat Overview

WinRAR 7.10 was released yesterday with numerous features, such as larger memory pages, a dark mode, and the ability to fine-tune how Windows Mark-ofthe-Web flags are propagated when extracting files. One new feature that stood out is a new setting that lets you strip information that may be considered a privacy risk from the Mark of The Web alternate data stream. For those unfamiliar with the Mark-of-the-Web (MoTW), it is an alternative data stream named "Zone.Identifier" that is added to files downloaded from the Internet, including from websites and email. When attempting to open a downloaded file, Windows will check if a MoTW exists and, if so, display additional warnings to the user, asking if they are sure they wish to run the file.

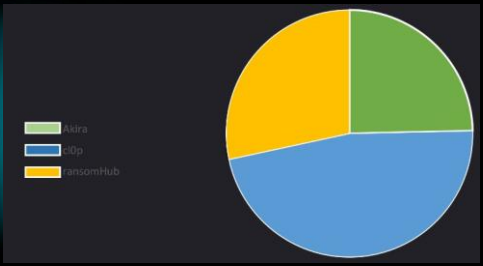
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



Hackers are launching attacks against Palo Alto Networks PAN-OS firewalls by exploiting a recently fixed vulnerability (CVE-2025-0108) that allows bypassing authentication. The security issue received a high-severity score and impacts the PAN-OS management web interface and allows an unauthenticated attacker on the network to bypass authentication and invoke certain PHP scripts, potentially compromising integrity and confidentiality. The researchers demonstrated how the flaw could be leveraged to extract sensitive system data, retrieve firewall configurations, or potentially manipulate certain settings within PAN-OS.

Global Weekly Notable One

Obfuscated Files or Information: Defense Evasion

The espionage operation identified as CL-STA-004 allegedly linked to a group known as Mustang Panda, a Chinese state-sponsored cyberespionage group primarily targeting governmental entities in Southeast Asia since 2021, highlight a rare technique exploited for evade defenses.

Known for sophisticated tactics, they utilize advanced malware like ToneShell and ShadowPad to infiltrate networks and exfiltrate sensitive information. Their operations have evolved from initial reconnaissance activities to deploying complex command-and-control strategies, reflecting their adaptability to security measures. By focusing on high-value individuals within government sectors, Mustang Panda poses a significant threat to national security. Continued vigilance and enhanced cybersecurity measures are crucial for organizations to mitigate risks associated with this persistent threat actor.

Global Weekly Notable One

Once establishing a foothold in the network, threat actor employed a rare technique called Hex Staging, delivering payloads in hex-encoded chunks. This method, named by Unit 42, evades common detection systems by avoiding direct file writes during payload delivery. Notably in the recent CL-STA-0048 espionage campaign attributed to Chinese interests, this method involves incrementally writing hex-encoded data into temporary files using commands executed via cmd.exe.

By delivering payloads in chunks, attackers can evade detection systems that typically monitor for direct file writes. Once the hex data is fully assembled, tools like Certutil are employed to decode it back into executable code. This technique allows for covert delivery and execution of malicious software, such as Cobalt Strike and PlugX, while bypassing conventional security measures. Hex Staging exemplifies advanced tactics in cyberespionage, highlighting the need for enhanced detection and protection strategies against such sophisticated attacks.

Threat Hunting Activity

SORINTSEC

TACTIC

Defense Evasion

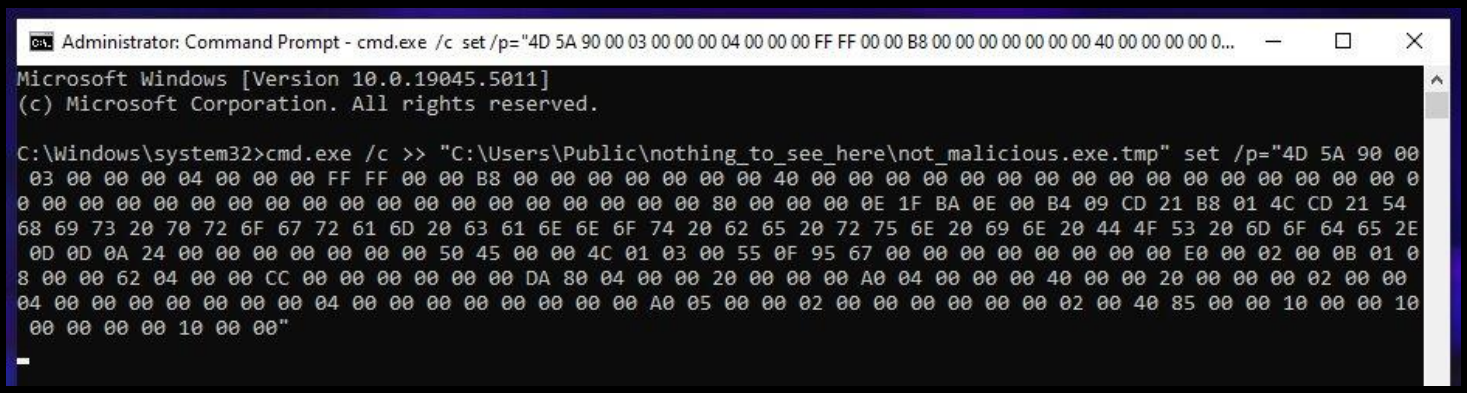
TECHNIQUES

T1027 – Obfuscated Files or Information

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled.

Threat Hunting Activity

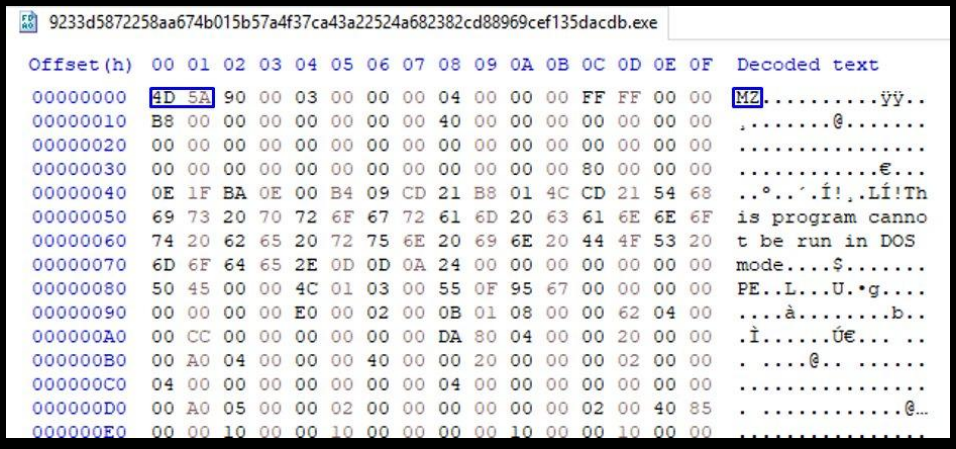
Below is the first part of the Hex Staging technique, where via cmd.exe temporary file is incrementally writes containing the contents of the binary splitted by chunks. It can also seen that the beginning of the binary has the values 4D 5A, representing the magic bytes.



Binary chunks creation

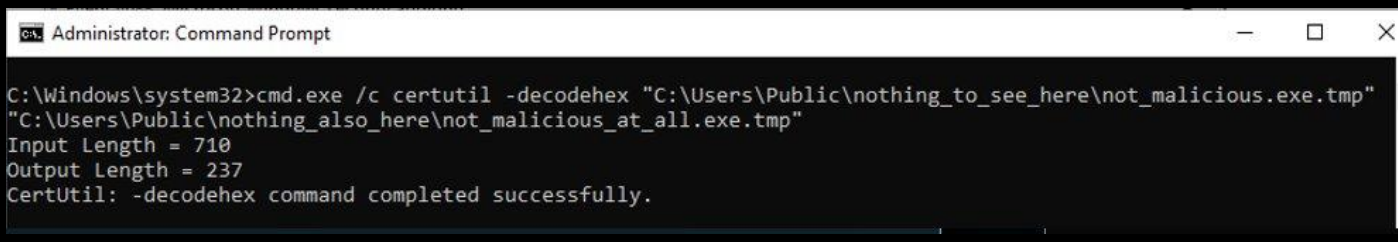
Magic bytes, also known as file signatures, are unique identification numbers found at the beginning of a file. These bytes indicate the file's type and provide information about the data it contains, using this signature can be determined how to read the file or which application to open it with.

The hexadecimal values 4D 5A correspond to the ASCII characters "MZ". The "MZ" header is a magic number that identifies a file as an executable.



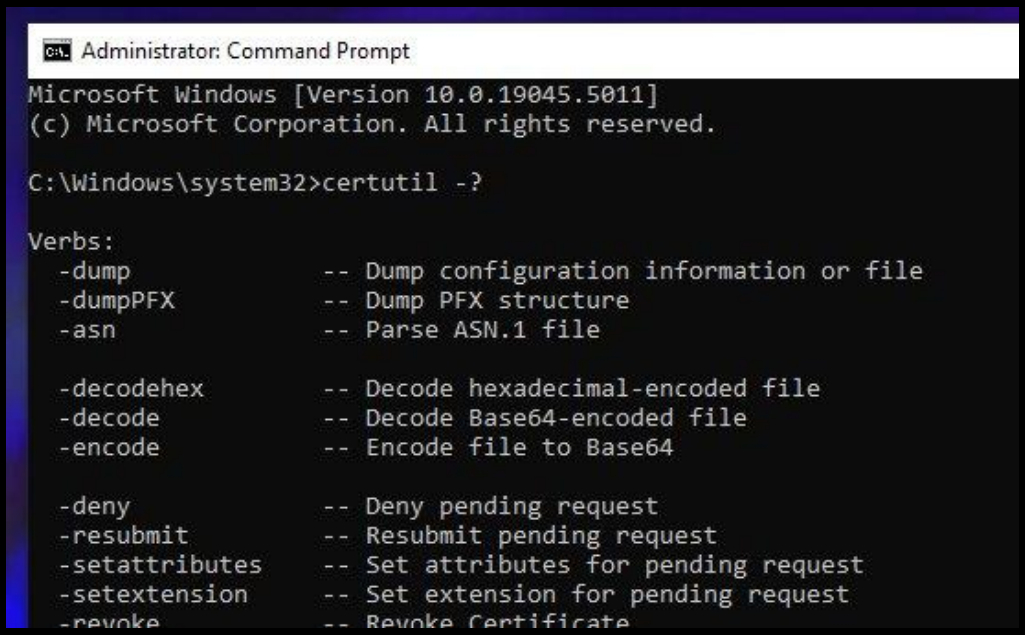
Threat Hunting Activity

Shown below the second part of the Hex Staging technique, whereby through the use of certutil.exe the decoding of the chunks is performed. Once the contents have been reassembled and decoded it will be possible to proceed in executing the now complete and executable malware.



Certutil chunks decode

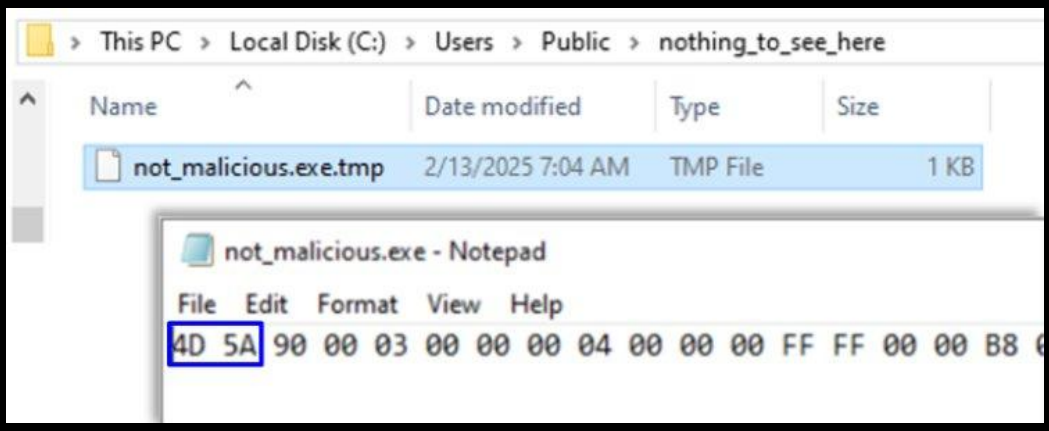
Certutil is a command-line utility included with Windows, primarily designed for managing and viewing cryptographic certificates. In addition to its legitimate uses, threat actors have exploited Certutil for malicious purposes, including downloading files from the internet and executing payloads.

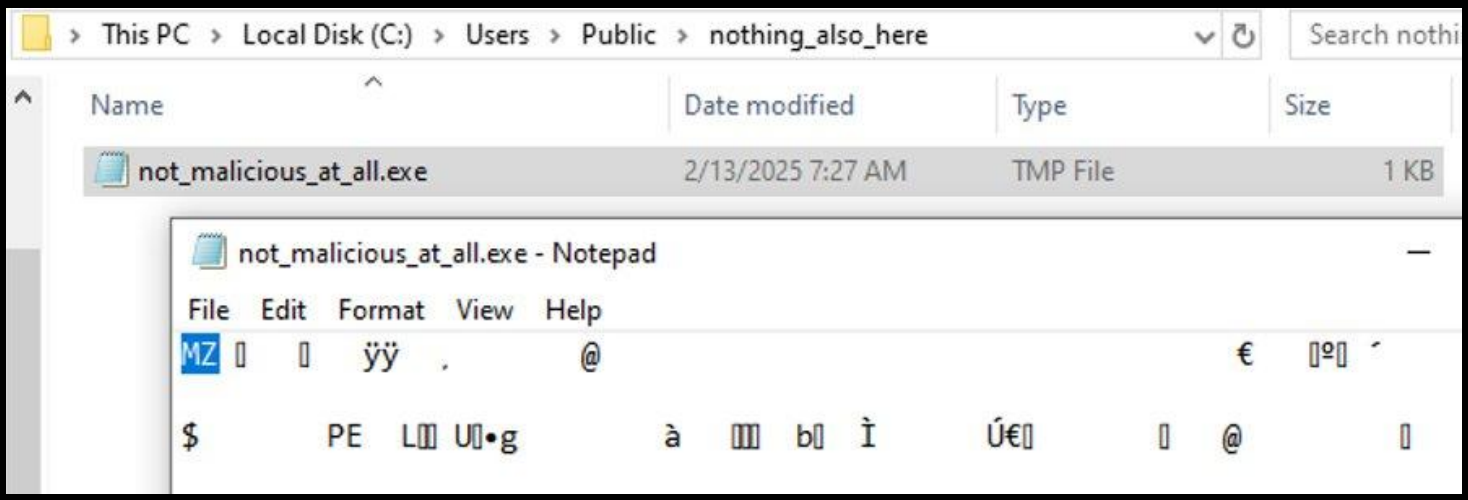


Certutil

Threat Hunting Activity

Below we can see the difference between the files created during the Hex Staging technique, where first the chunks are created in hexadecimal and then they are decoded to be reassembled into the malicious binary.





Hex Staging created files

Threat Hunting Activity

EID 4688 help to detect Hex Staging where the first chunk creation with the magic bytes can be intercepted.

EID 4688

Basic EDRs do not flag it as malicious, while more advanced EDRs raise an alert when they intercept similar activities, but these are often reported only after they have been linked to other suspicious activities. Therefore, early detection of these behaviors is necessary because they should be recognized as a malicious symptom.

PUBLIC