CYBERWEEK OF

SORINTSEC

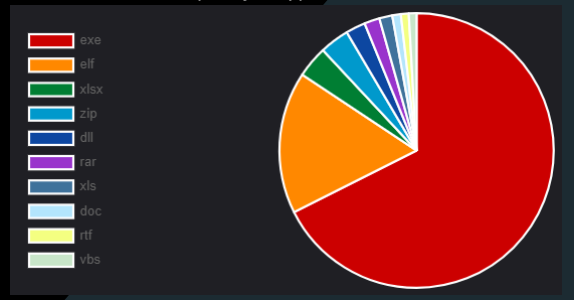
INDEX

GLOBAL WEEKLY THREAT OVERVIEW

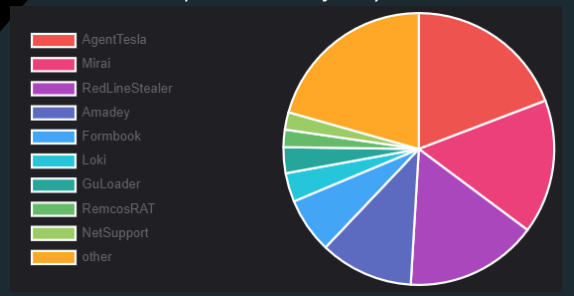
Microsoft has discovered a new version of the BlackCat ransomware that embeds the Impacket networking framework and the Remcom hacking tool, both enabling spreading laterally across a breached network. Soon after, IBM Security X-Force performed a deep dive into the new BlackCat encryptor, warning that the encryptor evolved into a toolkit. According to Microsoft, the BlackCat operation is using the Impacket framework for credential duping and remote service execution to deploy the encryptor across an entire network. In addition to Impacket, Microsoft says that the encryptor embeds the Remcom hacking tool, which is a small remote shell that allows the encryptor to remotely execute commands on other devices on a network.

An ongoing phishing campaign has been underway since at least April 2023 that attempts to steal credentials for Zimbra Collaboration email servers worldwide. According to a report by ESET, phishing emails are sent to organizations worldwide, with no specific focus on certain organizations or sectors. The threat actor behind this operation remains unknown at this time. Hackers commonly target Zimbra Collaboration email servers for cyber espionage to collect internal communications or use them as an initial point of breach to spread to the target organization's network.

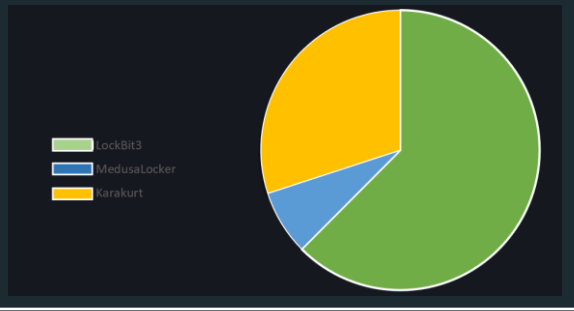
Top 10 file types



Top 10 Malware family



Top 3 Ransomware



GLOBAL WEEKLY NOTABLE ONE

Stordiag LOLBin Abuse – Defense Evasion

For malware authors, the idea of exploiting software already present on the target machine to achieve their malicious purposes is very attractive. This technique makes it possible to hijack an already existing and trusted piece of software to achieve the final or next purpose, thus decreasing the chances of being detected. This well-known technique exploits 'living off the land' binaries, or more commonly 'LOLBins'.
Although not widely exploited in the wild, the LOLBin targeted this week is Stordiag.exe or Storage Diagnostic Tool that allows system administrators to collect and analyse storage-related data, which can help them troubleshoot hard drive and storage diagnostics.
Once executed, Stordiag.exe will execute schtasks.exe, systeminfo.exe and fltmc.exe, but if Stordiag.exe is copied to a folder and an arbitrary executable is renamed to one of these executable names, stordiag.exe will execute it.

THREAT HUNTING ACTIVITY

Stordiag LOLBin Abuse – Defense Evasion

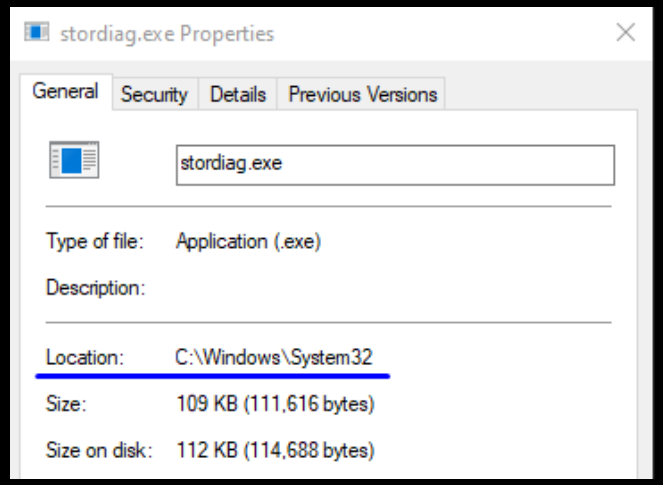
TYPE	Defense Evasion
TACTICS & TECHNIQUES	T1218 – System Binary Proxy Execution

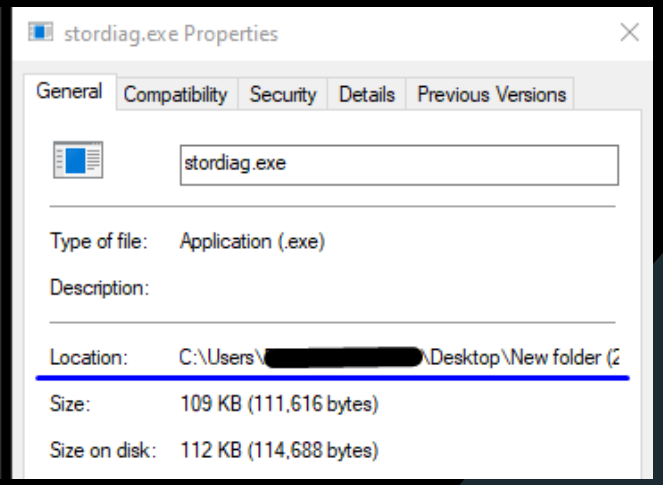
Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands.

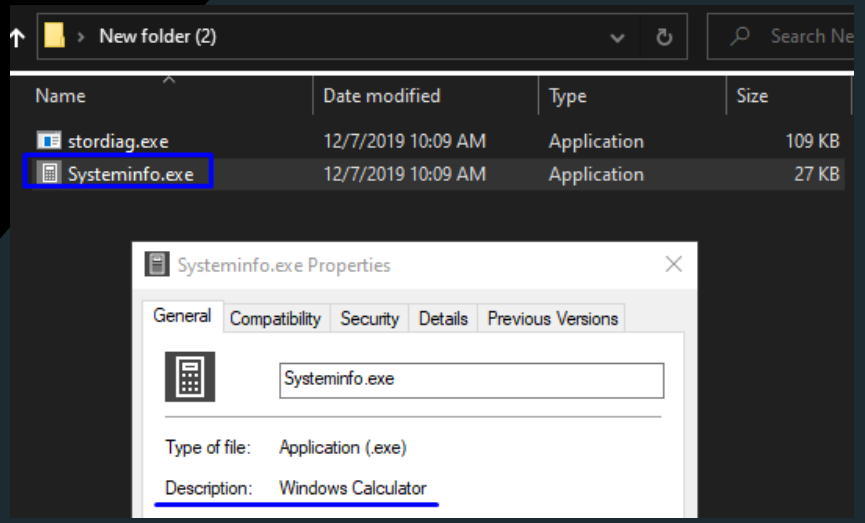
THREAT HUNTING ACTIVITY

Stordiag LOLBin Abuse – Defense Evasion

Threat Detection team tested the execution of the LOLBin first copying stordiag.exe to a new folder, then name calc.exe as Systeminfo.exe .
After the execution of Stordiag.exe it's spawn also calc.exe renamed as Systeminfo.



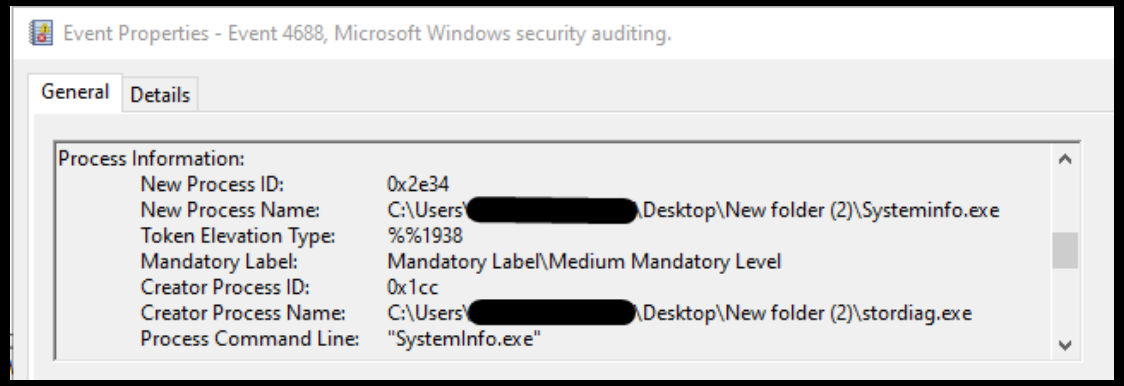


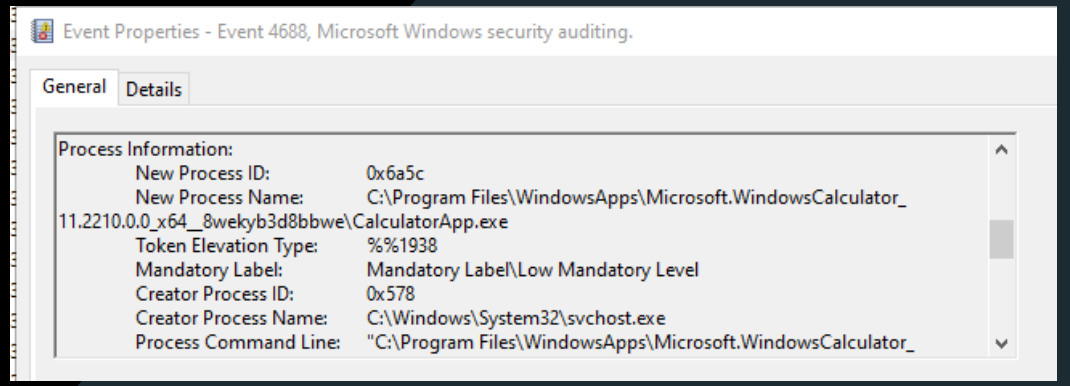


THREAT HUNTING ACTIVITY

Stordiag LOLBin Abuse – Defense Evasion

Detection can be made on evidences from EventID 4688 about the execution of the LOLBin from a not default path.





ABOUT SORINT.SEC

Sorint.SEC is the Network & Security Company of Sorint.LAB group focused on Cyber and Information Security.

Sorint.SEC services:

SOLUTION DESIGN & DELIVERY

Our D&D department can design and implements network and security solutions, evaluating the existing architecture, the
targets and helps in identifying the best solution for the customer.

MANAGED SECURITY SERVICES

24 hours per day, 7 days per week, 365 days per year, we care about Customer security.

CONSULTANCY

We offer consultancy services on all security aspects:
Vulnerability Assessments, Penetration Testing, Red Team, Incident Response and Forensic.

HTTPS://SEC.SORINT.IT
VIA VITTORIO VENETO, 25
BREMBATE (BG)