CYBERWEEK OF

SORINTSEC

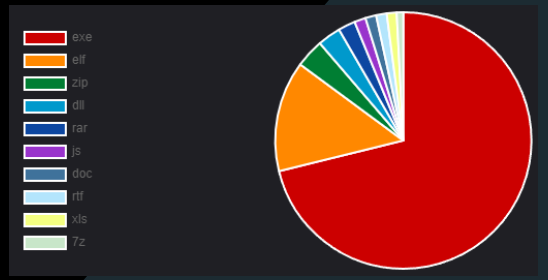
INDEX

GLOBAL WEEKLY THREAT OVERVIEW

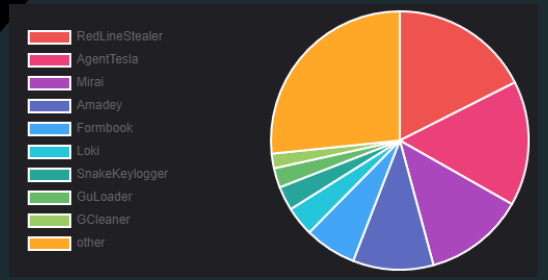
GitHub is warning of a social engineering campaign targeting the accounts of developers in the blockchain, cryptocurrency, online gambling, and cybersecurity sectors to infect their devices with malware. The campaign was linked to the North Korean state-sponsored Lazarus hacking group, also known as Jade Sleet (Microsoft Threat Intelligence) and TraderTraitor (CISA). The hacking group has a long history of targeting cryptocurrency companies and cybersecurity researchers for cyberespionage and to steal cryptocurrency. GitHub warns that the Lazarus Group is compromising legitimate accounts or creating fake personas that pretend to be developers and recruiters on GitHub and social media.

Threat actors are showing an increased interest in generative artificial intelligence tools, with hundreds of thousands of OpenAI credentials for sale on the dark web and access to a malicious alternative for ChatGPT. Both less skilled and seasoned cybercriminals can use the tools to create more convincing phishing emails that are customized for the intended audience to grow the chances of a successful attack. In six months, the users of the dark web and Telegram mentioned ChatGPT, OpenAI's artificial intelligence chatbot, more than 27,000 times. A report in June from cybersecurity company Group-IB said that illicit marketplaces on the dark web traded logs from info-stealing malware containing more than 100,000 ChatGPT accounts.

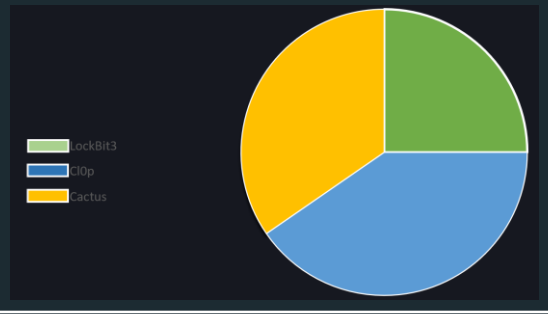
Top 10 file types



Top 10 Malware family



Top 3 Ransomware



GLOBAL WEEKLY NOTABLE ONE

AMSI bypass – Impair Defenses

As covered in a January CyberWeek report, there are several methods to impair defenses by bypassing AMSI.
Introduced with Windows 10, AMSI stands for "Antimalware Scan Interface", an API that enables to sending content to vendor endpoint security agent, each command or script that it is run in a Powershell session e.g. is fetched by AMSI and sent to installed antivirus software for inspection.
When an application attempts to submit content to be scanned by a vendor agent, the application loads amsi.dll and calls its functions in order to establish an AMSI session, the content to be scanned is then submitted and checked.
This technique exploits error generation to perform AMSI bypass.

THREAT HUNTING ACTIVITY

AMSI bypass – Impair Defenses

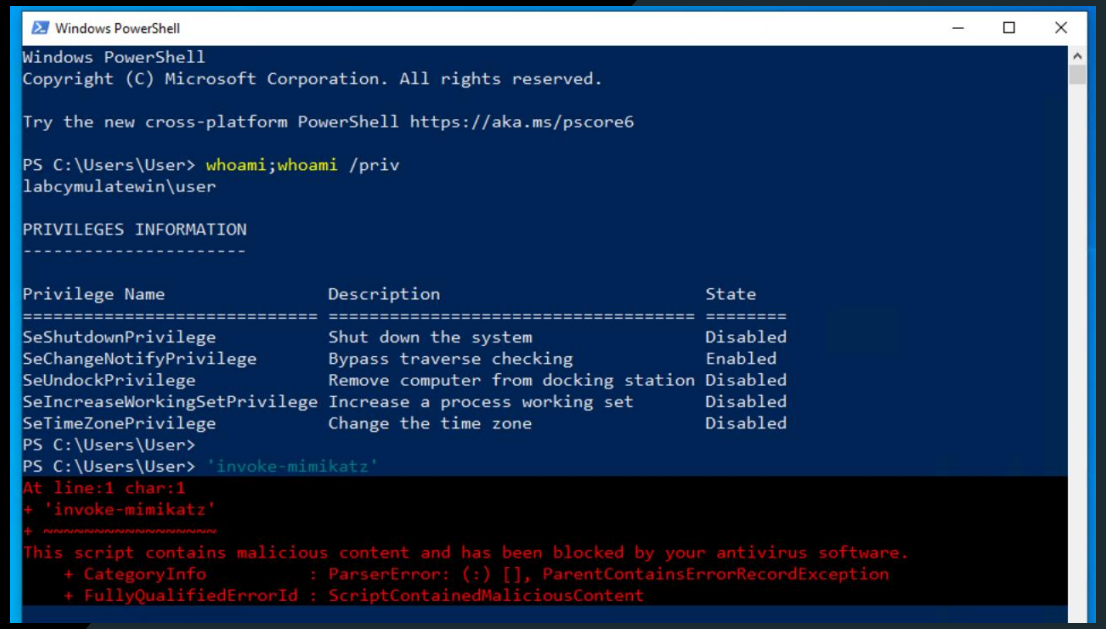
TYPE	Defense Evasion
TACTICS & TECHNIQUES	T1562 – Impair Defenses

Adversaries may modify and/or disable security tools to avoid possible detection of their malware/tools and activities. Adversaries may also tamper with artifacts deployed and utilized by security tools.

THREAT HUNTING ACTIVITY

AMSI bypass – Impair Defenses

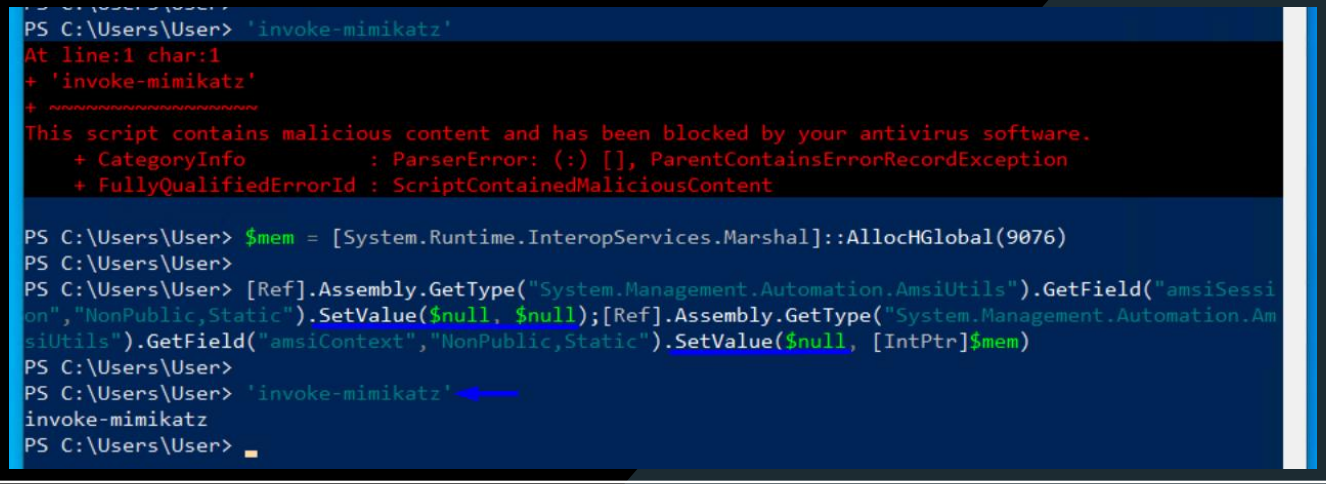
Leaving aside the process by which AMSI performs checks,
if in a low priv Powershell session we want to run cmdlet (e.g Invoke-Expression), before being executed, AMSI checks the command and if it does not match security parameters, the command is not executed returning an error.
Among the known techniques to bypass in-memory this process is to force an error condition on opening the AMSI session, so any cmdlet can be run without AMSI blocks. Until recently there was a technique to force the initialization of AMSI via the `amsiInitFailed` function, resulting in no scan being initialized for the current process/session.
Microsoft has developed a signature for this technique to prevent its exploitation, so it can no longer be used to bypass AMSI.



THREAT HUNTING ACTIVITY

AMSI bypass – Impair Defenses

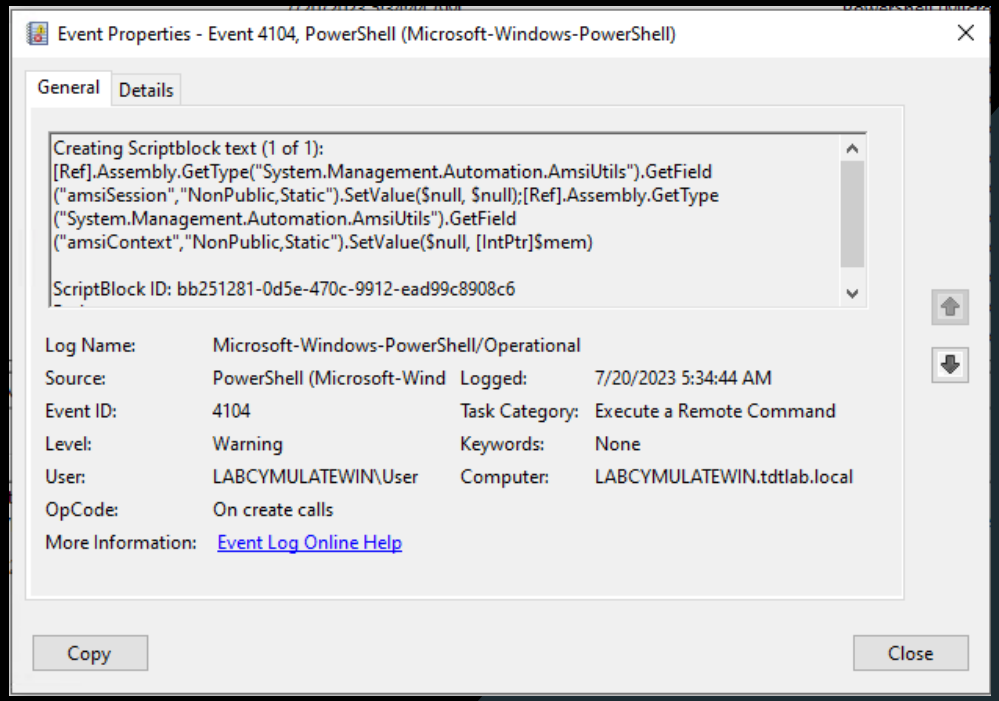
TDT tested an alternative method to force that error, this bypass allocates memory for "amsiContext" by forcing to "null" the value of `AmsiOpenSenssion` by returning an error.
When Powershell attempts to submit content to be scanned by a vendor agent that refers to as an AMSI provider, it loads `amsi.dll` and calls its `AmsiOpenSession` function in order to establish an AMSI session. If we can get `AmsiOpenSenssion()` to be invoked with an "amsiContext" pointer wich does not contains a 4 bytes value of AMSI at offset 0x00, an error will be returned from the function of 0x80070057, or "`E_INVALIDARG`". When the error is returned to Powershell session, `amsiInitFailied` will be set. As evident from the test performed after the bypass, AMSI does not intervene as in the previous test.



THREAT HUNTING ACTIVITY

AMSI bypass – Impair Defenses

Detection can be made on evidences from Powershell Operational Logs EventID 4104 in order to detect AMSI bypass attempt.



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)