CYBERWEEK OF

SORINTSEC

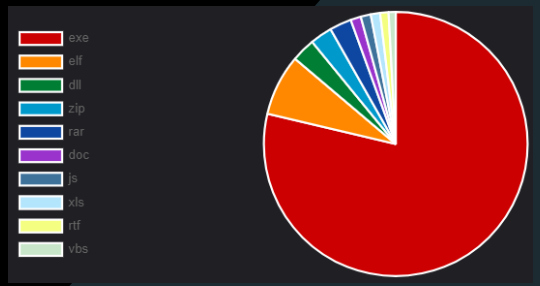
INDEX

GLOBAL WEEKLY THREAT OVERVIEW

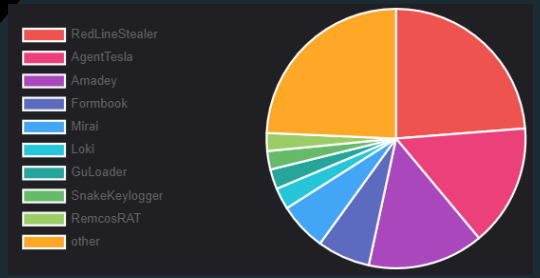
The ALPHV ransomware gang, also referred to as BlackCat, is trying to put more pressure on their victims to pay a ransom by providing an API for their leak site to increase visibility for their attacks. Multiple researchers spotted earlier this week that the ALPHV/BlackCat data leak site added a new page with instructions for using their API to collect timely updates about new victims, despite the “feature” has been partially available for months, it was not available for the larger audience.

The North Korean state-sponsored Lazarus hacking group is breaching Windows Internet Information Service (IIS) web servers to hijack them for malware distribution. The main advantage of this technique is the ease of infecting visitors of websites or users of services hosted on breached IIS servers owned by trustworthy organizations. In the recent attacks observed by ASEC's analysts, Lazarus compromised legitimate South Korean websites to perform 'Watering Hole' attacks on visitors using a vulnerable version of the INISAFE CrossWeb EX V6 software. Exploiting the flaw fetches a malicious 'SCSKAppLink.dll' payload from an IIS web server already compromised before the attack for use as a malware distribution server.

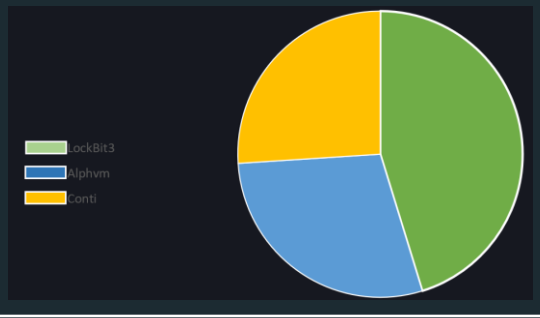
Top 10 file types



Top 10 Malware family



Top 3 Ransomware



GLOBAL WEEKLY NOTABLE ONE

Security Software Discovery – Discovery

Adversaries may use the information from Security Software Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.
Many threat actors perform this type of activity once a foothold is obtained in the target infrastructure. During several Incident Response engagements, security software discovery activities were identified before the precise tampering of the appliance and/or circumvention of the security software.

THREAT HUNTING ACTIVITY

Security Software Discovery – Discovery

TYPE	Discovery
TACTICS & TECHNIQUES	Software Discovery (T1518)

The adversary is trying to figure out your environment. Adversaries may attempt to get a listing of security software, configurations, defensive tools, and sensors that are installed on a system or in a cloud environment. This may include things such as firewall rules and anti-virus.

THREAT HUNTING ACTIVITY

Security Software Discovery – Discovery

Threat Detection Team perform tests by replicating security software discovery activity. This activity can be done via different ways, each method retrieve different information from the system and can be used to gather a better overview of the target system.

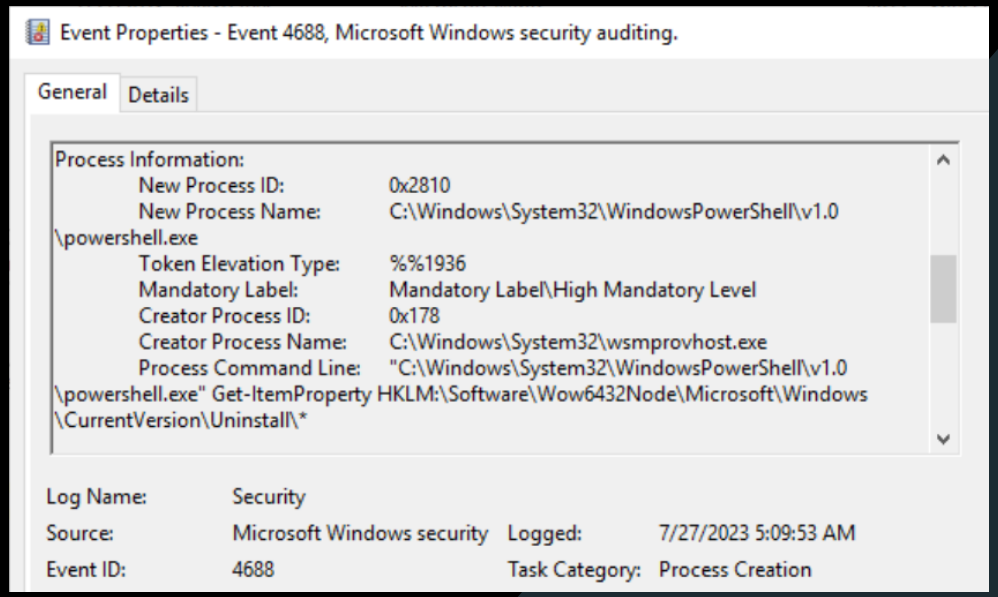
```
*Evil-WinRM* PS C:\Users\Administrator\Documents> tasklist.exe | findstr /i smartscreen
smartscreen.exe               532 RDP-Tcp#12                  1     25,504 K
smartscreen.exe              6256                             2     25,656 K
smartscreen.exe              6332                             3     25,368 K
smartscreen.exe             10140                             4     25,316 K
```

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\* | Se

DisplayName                                                    DisplayVersion  Publisher            InstallDate
-----------                                                    --------------  ---------            -----------
7-Zip 23.00 (x64)                                              23.00           Igor Pavlov


VMware Tools                                                   11.3.5.18557794 VMware, Inc.         20230313
Microsoft Visual C++ 2019 X64 Additional Runtime - 14.28.29913 14.28.29913     Microsoft Corporation 20230313
NXLog-CE                                                       3.2.2329        NXLog Ltd            20230725
UniversalForwarder                                             9.0.2.0         Splunk, Inc.         20230313
Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.28.29913    14.28.29913     Microsoft Corporation 20230313
```

THREAT HUNTING ACTIVITY

Security Software Discovery – Discovery

Detection can be made on evidences from EventID 4688 in order to detect software discovery 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)