CYBERWEEK OF

SORINTSEC

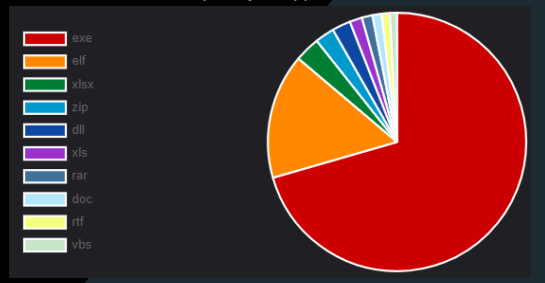
INDEX

GLOBAL WEEKLY THREAT OVERVIEW

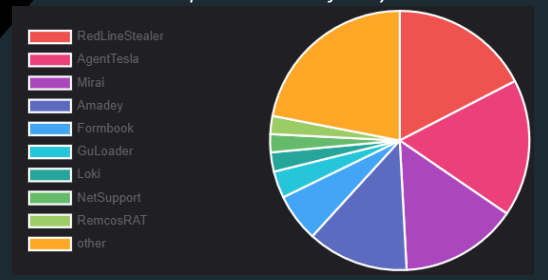
The developers of Raccoon Stealer information-stealing malware promote a new 2.3.0 version of the malware to cyber criminals. Raccoon 2.3.0 has introduced several "quality of life" and OpSec improvements that make it easier and safer to use, making it easier to use for less skilled threat actors and less likely for them to be traced by researchers and law enforcement. As this type of malware not only steals credentials, but also cookies, it could allow threat actors to use those stolen session cookies to bypass multi-factor authentication and breach corporate networks. Once they establish a foothold on the network, it could lead to a variety of attacks, including data theft, ransomware, BEC scams, and cyber espionage.

The Monti ransomware gang has returned, after a two-month break from publishing victims on their data leak site, using a new Linux locker to target VMware ESXi servers, legal, and government organizations. Researchers at Trend Micro analyzing the new encryption tool from Monti found that it has "significant deviations from its other Linux-based predecessors." Previous versions of the Monti locker were heavily based (99%) on the leaked code from Conti ransomware but the similarities in the new locker are just 29%.

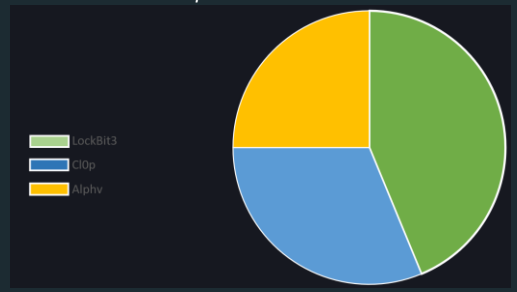
Top 10 file types



Top 10 Malware family



Top 3 Ransomware



GLOBAL WEEKLY NOTABLE ONE

Disable Local Account Filter via RegKey – Privilege Escalation

Ransomware attacks and groups are constantly growing in number and becoming more sophisticated. Threat actors can quickly impact a company's operations and business if it is not properly prepared.
BlackByte Group, discovered in July 2021, during last tracked attacks employed a range of tools and techniques, culminating in the deployment of BlackByte 2.0 ransomware to achieve their objectives. Among the capabilities used by the BlackByte 2.0 ransomware, there is the modification of a registry key to facilitate the execution process with high privileges on the impacted device.

GLOBAL WEEKLY NOTABLE ONE

Disable Local Account Filter via RegKey – Privilege Escalation

To better protect users who are members of the local Administrators group, Miscrosoft implement UAC remote restrictions on the network, this mechanism helps prevent local malicious software from running remotely with administrative rights. For any non-RID 500 local admin account remotely connecting to a Windows Vista+ machine the token returned is “filtered” (i.e. medium integrity) even though the user is a local administrator, so when the user attempts to access a privileged resource remotely (e.g. C$), they receive an “Access is Denied” message despite technically having administrative access.
BlackByte 2.0 ransomware set the LocalAccountTokenFilterPolicy registry key (disabled by default) in order to elevate local privilege.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

THREAT HUNTING ACTIVITY

Disable Local Account Filter via RegKey – Privilege Escalation

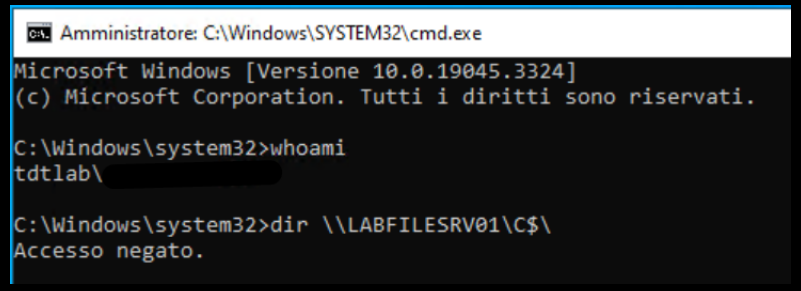
TYPE	Privilege Escalation
TACTICS & TECHNIQUES	Disable Local Account Filter via RegKey (T1134)

Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives.

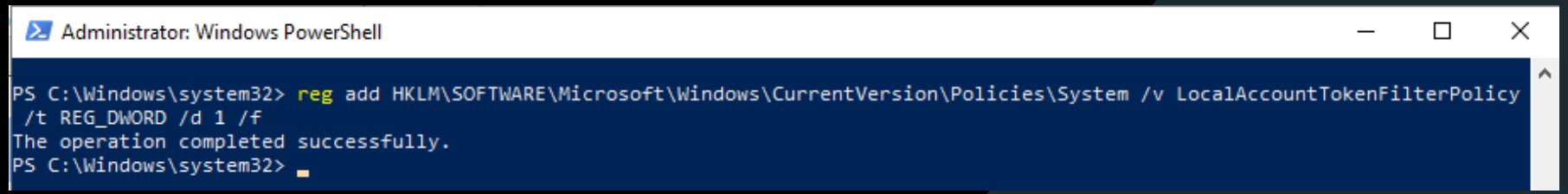
THREAT HUNTING ACTIVITY

Disable Local Account Filter via RegKey – Privilege Escalation

Threat Detection Team perform tests replicating ransomware behaviour, trying to enumerate C$ with a local admin user with filtered tokens spawning on the target machine a process with medium integrity level returning the access denied error.



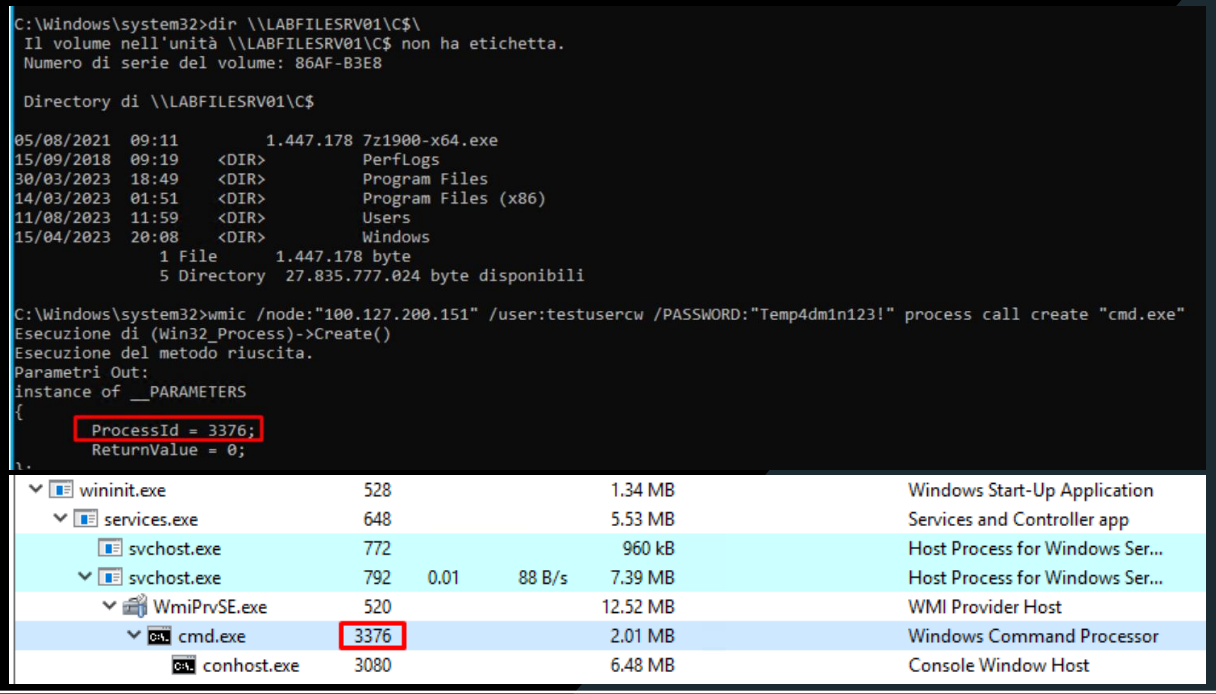
Then, to perform priv esc on remote target machine, the registry key LocalAccountTokenFilterPolicy was integrated.



THREAT HUNTING ACTIVITY

Disable Local Account Filter via RegKey – Privilege Escalation

Following the registry key set, the folder enumeration does not return any errors, Threat Detection Team also verifying remote execution of a cmd instance.



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)