CYBERWEEK OF

SORINTSEC

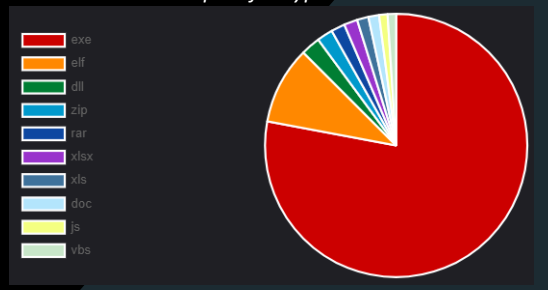
INDEX

GLOBAL WEEKLY THREAT OVERVIEW

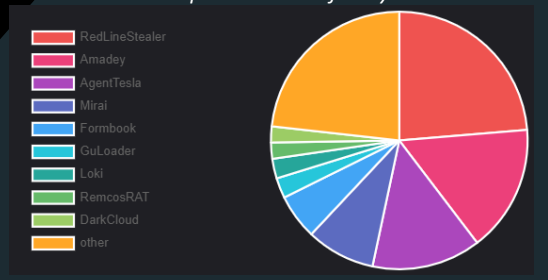
Clop has begun to use torrents to distribute data stolen from MOVEit attack. According to security researcher Dominic Alvieri, who first spotted this new tactic, torrents have been created for twenty victims, including Aon, K & L Gates, Putnam, Delaware Life, Zurich Brazil, and Heidelberg. As part of this new extortion method, Clop has set up a new Tor site providing instructions on how to use torrent clients to download the leaked data and lists of magnet links for the twenty victims. As torrents use peer-to-peer transfer among different users, the transfer speeds are faster than the traditional Tor data leak sites.

Hackers are increasingly abusing the legitimate Cloudflare Tunnels feature to create stealthy HTTPS connections from compromised devices, bypass firewalls, and maintain long-term persistence. The technique isn't entirely new, as Phylum reported in January 2023 that threat actors created malicious PyPI packages that used Cloudflare Tunnels to stealthy steal data or remotely access devices. However, it appears that more threat actors have started to use this tactic, seeing an uptick in activity. Also, if the attacker wants to be even more stealthy, they can abuse Cloudflare's 'TryCloudflare' feature that lets users create one-time tunnels without creating an account.

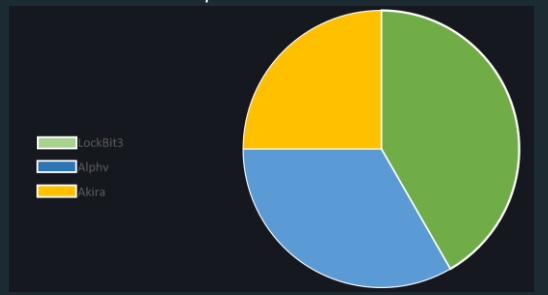
Top 10 file types



Top 10 Malware family



Top 3 Ransomware



GLOBAL WEEKLY NOTABLE ONE

Bypass User Account Control (UAC) – Privilege Escalation

Adversaries need to elevate their privileges to proceed with their activities and achieve their goals. An effective method that has already been observed in the wild is the integration of a module to bypass the UAC. This 'feature' has been observed in very different malware samples: Trojans such as Toitoin, LPE tools such as JuicyPotato, and many ransomware such as Darkside, Blackcat and Lockbit.
User Account Control (UAC) reduces the risk of malware by limiting the ability of malicious code to execute with administrator privileges, each application that requires the administrator access token must prompt the end user for consent. Windows protects processes by marking their integrity levels, a process with a lower integrity level can’t write to an object with a higher integrity level, bypassing this protection can be exploited by malware to execute code with administrator privileges.

GLOBAL WEEKLY NOTABLE ONE

Bypass User Account Control (UAC) – Privilege Escalation

By malware implementation of this module is responsible for performing User Account Control (UAC) bypass via Elevation Moniker.
The Elevation Moniker is used to activate a COM class related to specified CLSID, that is a globally unique identifier that identifies a COM class object, to accomplish a specific and limited function that requires elevated privileges.

```
hr = CoGetObject(L"Elevation:Administrator!new:{3AD05575-8857-4850-9277-11B85BDB8E09}", &bindOptions,
                 IID_IFileOperation,
                 reinterpret_cast<void**>(&fileOperation));

hr = CoGetObject(L"Elevation:Administrator!new:{BDB57FF2-79B9-4205-9447-F5FE85F37312}", &bindOptions,
                 IID_IeAxiAdminInstaller,
                 reinterpret_cast<void**>(&adminInstaller));
```

In the context of UAC bypass, the malware leverages the COM Elevation Moniker "Elevation:Administrator!new:" along with specific elevated COM Objects utilizing he CLSID {3AD05575-8857-4850-9277-11B85BDB8E09}, which provides functionalities related to copy, move, rename, delete, and link operations. Additionally, the CLSID {BDB57FF2-79B9-4205-9447-F5FE85F37312} is employed, specifically designed for the installation of Internet Explorer add-ons. By exploiting these elevated COM Objects, the malware aims to elevate its privileges and carry out malicious activities without being hindered by UAC restrictions.

THREAT HUNTING ACTIVITY

Bypass User Account Control (UAC) – Privilege Escalation

TYPE	Privilege Escalation
TACTICS & TECHNIQUES	Abuse Elevation Control Mechanism: Bypass UAC (T1548)

Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Windows User Account Control (UAC) allows a program to elevate privileges its to perform a task under administrator-level permissions, possibly by prompting the user for confirmation.

THREAT HUNTING ACTIVITY

Bypass User Account Control (UAC) – Privilege Escalation

Threat Detection Team perform tests using COM Elevation Moniker to bypass User Account Control and execute a shell with administrative privileges. After the execution of the UAC bypass module the high integrity level Internet Explorer Add-on Installer “ieinstal.exe” is triggered through the COM object, executing “[1]bdeunlock.exe” (a copy of the signed “bdeunlock.exe” permitted by the first COM Elevation Moniker). The process is launched with specific arguments “/C start cmd.exe” that allows execute the signed binary with elevated permissions.

```
system32 = system32.substr(0, system32.find(L"\\bdeunlock.exe"));
    system32 += L"\\cmd.exe";
    if (!CopyFileW(system32.c_str(), file, FALSE))

system32 = system32.substr(0, system32.find(L"\\cmd.exe"));
    auto* const workingDirectory = SysAllocString(system32.c_str());

    std::wstring commandLine{targetFile};
    commandLine += L" /C start cmd.exe";
    SysFreeString(targetFile);
    targetFile = SysAllocString(commandLine.c_str());
```

THREAT HUNTING ACTIVITY

Bypass User Account Control (UAC) – Privilege Escalation

Detection can be made on evidences from EventID 4688 in order to detect UAC bypass module execution.

```
Process Information:
        New Process ID:         0x3d44
        New Process Name:       C:\Users\FRANCE~1\AppData\Local\Temp\IDC1.tmp\[1]
bdeunlock.exe
        Token Elevation Type:   %%1937
        Mandatory Label:        Mandatory Label\High Mandatory Level
        Creator Process ID:     0x5f00
        Creator Process Name:   C:\Program Files\Internet Explorer\ieinstal.exe
        Process Command Line:   C:\Users\FRANCE~1\AppData\Local\Temp\IDC1.tmp\[1]
bdeunlock.exe /C start cmd.exe
```

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)