New “CleverSoar” Installer Targets Chinese and Vietnamese Users

By Natalie Zargarov

Published: 2024-11-27 · Archived: 2026-04-06 01:26:59 UTC

CleverSoar Installer Used to Deploy Nidhogg Rootkit and Winos4.0 Framework Against Targeted Users

In early November, Rapid7 Labs identified a new, highly evasive malware installer, 'CleverSoar,' targeting Chinese and Vietnamese-speaking victims. CleverSoar is designed to deploy and protect multiple malicious components within a campaign, including the advanced Winos4.0 framework and the Nidhogg rootkit. These tools enable capabilities such as keystroke logging, data exfiltration, security bypasses, and covert system control, suggesting that the campaign is part of a potentially prolonged espionage effort. Rapid7 Labs’ findings indicate a sophisticated and persistent threat, likely focused on data capture and extended surveillance.

Distribution

While the majority of CleverSoar installer-related binaries were detected in November 2024, we discovered that the initial version of these files was uploaded to VirusTotal in late July of this year. The malware distribution begins with a .msi installer package, which extracts the files and subsequently executes the CleverSoar installer.

Victimology

The CleverSoar installer, as detailed in the Technical Analysis section, checks the user’s language settings to verify if they are set to Chinese or Vietnamese. If the language is not recognized, the installer terminates, effectively preventing infection. This behavior strongly suggests that the threat actor is primarily targeting victims in these regions. Based on the folder names generated by the malicious .msi files (e.g., Wegame, Installer), we infer that the .msi installer is being distributed as fake software or gaming-related applications.

Attribution

Rapid7 Labs was unable to attribute the installer to a specific known threat actor. However, due to similarities in campaign characteristics, we suspect with medium confidence that the same threat actor may be responsible for both the ValleyRAT campaign and the new campaign, both reported by Fortinet this year. The techniques employed in the CleverSoar installer suggest that the threat actor possesses advanced skills and a comprehensive understanding of Windows protocols and security products.

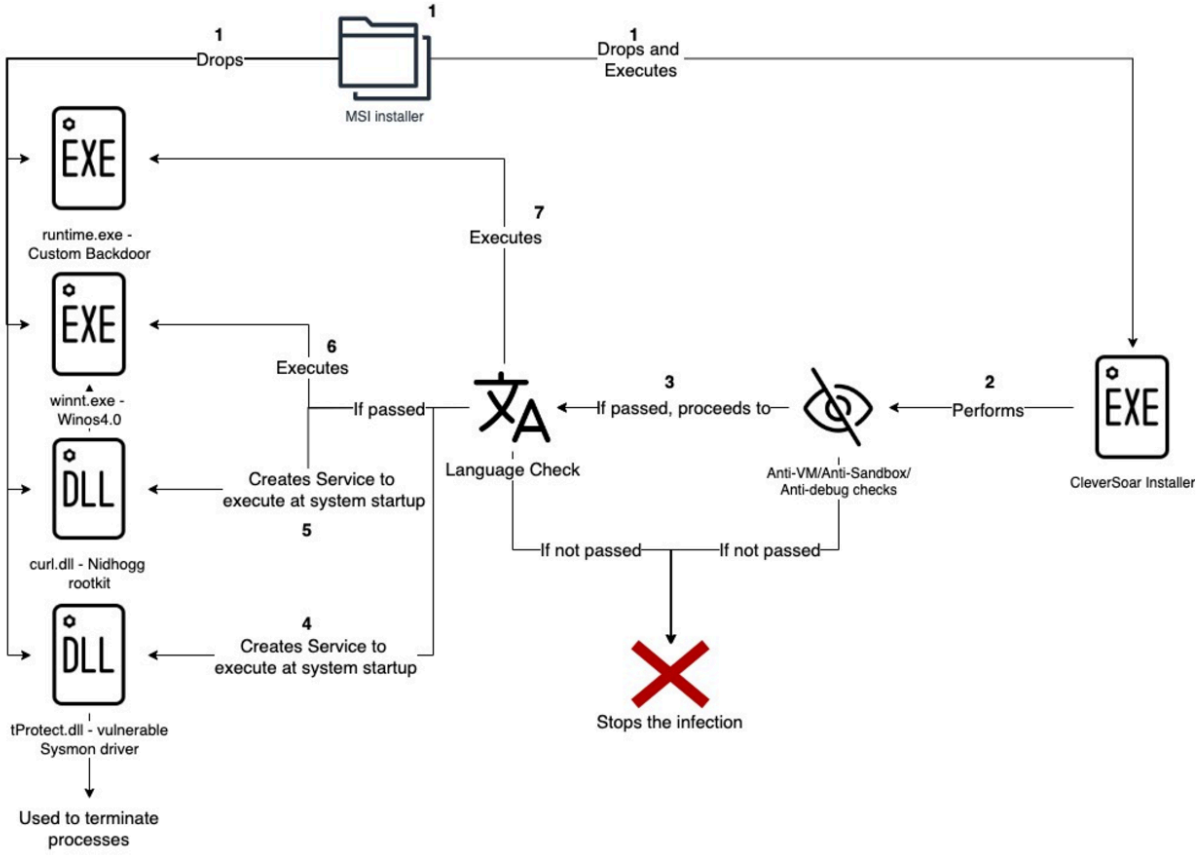
Rapid7 Customers

InsightIDR and Managed Detection and Response (MDR) customers have existing detection coverage through Rapid7's expansive library of detection rules. Rapid7 recommends installing the Insight Agent on all applicable

hosts to ensure visibility into suspicious processes and proper detection coverage. The following rule will alert on a wide range of malicious hashes tied to behavior in this blog: Suspicious Process - Malicious Hash On Asset.

Technical Analysis

This technical analysis will cover the CleverSoar installer used to evasively deploy the **Nidhogg** rootkit, **Winos4.0** framework and the custom backdoor (T1105). The installer is also responsible for disabling security solutions (T1562.001) and making sure to infect only machines with Chinese or Vietnamese system languages (T1614.001).



File Information:

File name	Update.exe
MD5	207836bd04f8086b704d742194061439
Sha1	0e501e4581610c7618466e071c28691eb8680ab1
Sha256	f70b34e2b1716528a3c3fffdbfc008003b9685f1a4da2e5a6052612de92b0c68

Given our high confidence that the malicious files were dropped by a .msi package (T1218.007), which in our case creates a 'WindowsNT' folder under the 'C:\Program Files (x86)' directory, we also assume that the same .msi package is responsible for dropping all the payloads listed below and executing the 'Update.exe' binary.

The installer begins by verifying the existence of the 'C:\cs' folder.It subsequently checks if the process is elevated by executing 'GetTokenInformation' and passing 'TokenElevation' (0x14) as a TokenInformationClass (T1134). If the process is not elevated, the malware will utilize the 'runas' operation of 'ShellExecuteA' to execute the process with Administrator privileges (T1134.002).

Subsequently, it proceeds to a series of evasion techniques, commencing with a rarely employed one.

Firmware Table Anti-VM

The malware retrieves a raw SMBIOS firmware table by invoking 'GetSystemFirmwareTable' and verifying a specific value presence. In our instance, the installer checks for 'QEMU' (indicating a free string open-sourced emulator) presence in the returned buffer (T1497.001). This technique is a sophisticated Anti-VM method as certain memory regions utilized by the operating system contain distinctive artifacts when the operating system is executed within a virtual environment. Notably, this technique has been previously employed by the Raspberry Robin malware, but in a slightly different way.

Windows Defender Emulator

The installer employs the 'LdrGetDllHandleEx' and 'RtlImageDirectoryEntryToData' functions to ascertain the state of Windows Defender’s emulator (T1497.001). Additionally, it utilizes the 'NtIsProcessInJob' and 'NtCompressKey' functions for the same purpose. These three anti-emulation techniques are publicly available in the UACME open-source project. Upon successful completion of these anti-emulation checks, the installer logs that defender checks were successfully bypassed and proceeds to the subsequent check.

Windows 10 or Windows 11

Initially, the installer verifies the operating system version by invoking the 'GetVersionExW' function (T1082). To identify whether the malware is executing on the Windows 10 operating system or Windows 11, the presence of the 'C:\Windows\System32\Taskbar.dll' file is checked, as this file can only be found on Windows 11 operating systems.

3rd Party DLL Injection Prevention

The CleverSoar installer modifies the processes mitigation policy to include the restriction 'Signatures restricted (Microsoft only)' (T1543). This action prevents non-Microsoft-signed binaries from being injected into the affected process. By implementing this technique, Anti-Virus and EDR solutions that employ userland hooking cannot inject their DLLs into the running process.

Timing Anti-Debug

The installer also executes timing anti-debug checks by invoking the 'GetTickCount64' function twice and measuring the delay between instructions and their execution (T1622).

Simple Anti-Debug check

The CleverSoar installer employs the 'IsDebuggerPresent' API call to ascertain whether the process is currently undergoing debugging (T1622).

Anti-Sandbox/Anti-VM Username Check

Upon the successful completion of all preceding checks, the malware retrieves the current username and subsequently compares it to the following (T1497.001):

'CurrentUser, Sandbox, Emily, HAPUBWS, Hone Lee, IT-ADMIN, Johnaon, Miller, miloza, Peter Wilson, timmy, sand box**,** malware, maltest, test user, virus, John Doe, 9ZaXj, WALKER, vbccsb_*, vbccsb.'

While most of these usernames are well known for being used by sandboxes and emulator solutions, two of them seem to be misspelled: 'Hone Lee' instead of 'Hong Lee' and 'Johnaon' instead of 'Johnson'.

```
Stack[000024F4]:000000F4BA71F2AF db    0
Stack[000024F4]:000000F4BA71F2B0 aHoneLee db 'Hone Lee',0
```

There are two possible reasons for this misspell, first, the threat actor typed those names manually, and the second one might be, the threat actor found that those are more recent names used by sandboxes.

Once the username check bypass is successfully executed, the malware proceeds to complete the evasion phase and initiates its malicious actions.

Malicious Activity

Upon successful completion of all environmental checks, the installer proceeds to the system language verification. This process involves retrieving the language identifier (ID) for the user interface language and verifying if that ID corresponds to one of the Chinese language IDs (0x804, 0xC04, 0x1404, 0x1004) or the Vietnamese ID (0x42A). If the language ID does not match any of these identifiers, the malware terminates its execution (T1614.001).

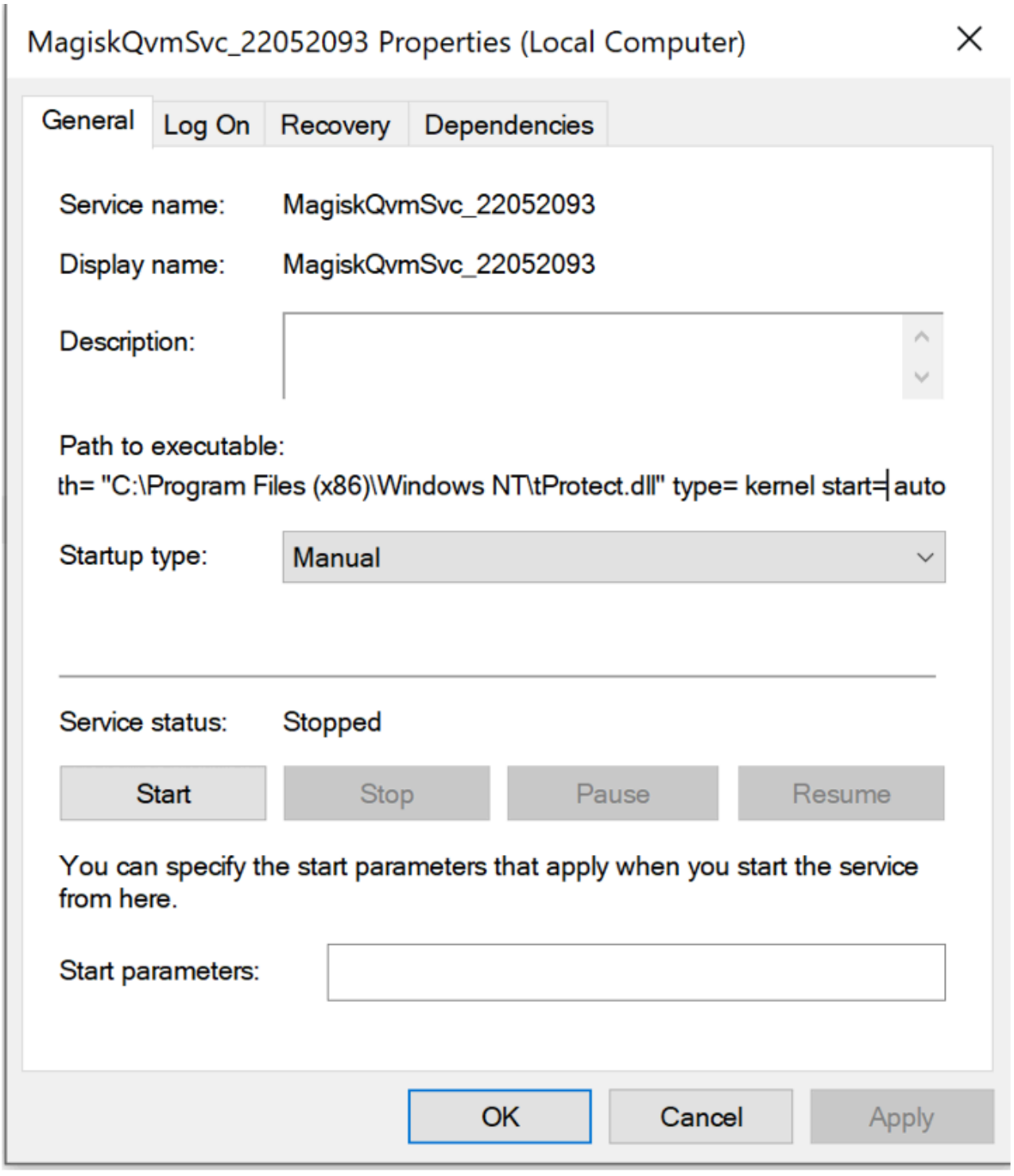
This observation suggests a potential threat actor’s intention to target only endpoints within these two countries.

Subsequently, the installer creates the 'HKCU\SOFTWARE\Magisk' (T1112) registry key and searches for the 'ring3_username' value under it. If the value is not present, the malware retrieves the user name that the 'explorer.exe' process is running as and sets the 'ring3_username' value.

The installer verifies if virtualization is enabled in the firmware and made available by the operating system by calling 'IsProcessorFeaturePresent' with 0x15 (PF_VIRT_FIRMWARE_ENABLED) and creates the 'INIT.dat' file in the 'C:\Program Files (x86)\Windows NT' directory. Next, it enumerates processes and checks if one of 'ZhuDongFangYu.exe', 'QHActiveDefense.exe', 'HipsTray.exe', or 'HipsDaemon.exe' is running (T1518.001). The first two processes belong to 360 Total Security (Chinese Anti-Virus Software), and the last two belong to HeroBravo System Diagnostics. If one of these processes is discovered, the installer proceeds to adjust 'Se_Debug_Privilege' to the running process (T1134), enumerates running processes once again, searches for 'lsass.exe' and writes into that process (T1055). Unfortunately, we were unable to retrieve the written payload due

to an unhandled runtime error. It is noteworthy that during our investigation, we identified several installer versions, and most of them encountered unhandled runtime errors and could not execute.

Upon successful completion of the preceding checks, the installer proceeds to verify the existence of the 'CleverSoarInst' service. If the service is not detected, the installer opens a named '\\.\pipe\ntsvcs' pipe, which is linked to the RPC protocol, to establish a temporary service responsible for creating the 'CleverSoar' service (T1569.002). This temporary service will only execute once, executing the following command: 'cmd /c start sc create CleverSoar' displayname= CleverSoar binPath= “C:\Program Files (x86)\Windows NT\tProtect.dll” type= kernel start= auto'.

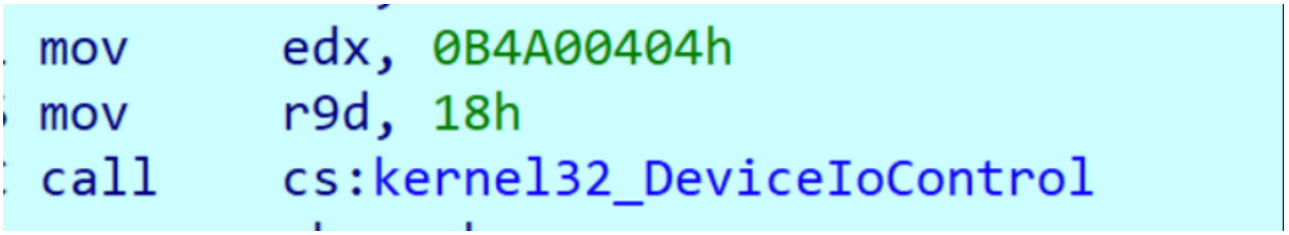


This command will create a new 'CleverSoar' service that will commence executing a driver at the system's startup. The DLL specified within this service is one of the previously dropped files and is, in fact, a vulnerable Sysmon driver commonly employed by threat actors to disable security software. The installer initiates the 'CleverSoar' service and establishes a named '\\.\TfSysMon' pipe connection. Subsequently, it enumerates the currently running processes once more (T1057), searching for any instances that contain one of the following strings:

Security Product	**String**
Bkav Pro	bka, blu
Windows Security	sechealthui, security, smartscreen, msmpeng, mssecess, mpcmdrun, defender
360 Total Security	360, zhudongfangyu, dsmain, qhactive, wdswfsafe, softmgr, 360se, 360chrome, 360zip
Kingsoft	ksafe, kwatch, kxecenter, kislive, kxetray, kxemain, kxewsc, kscan, kxescore, xdict
Huorong Internet Security	wsctrlsvc, usysdiag, hrsword
HeroBravo System Diagnostics	hips
Kaspersky	kav, avp, kis
2345 Security Guard	2345
Tencent	qqpc
McAfee	mcshield, mcapexe, mfemms
Avira	avira, sentryeye
Eset	eset, boothelper, efwd, egui, ekrn.exe, eguiproxy.exe
Elastic Security	elastic, agentbeat.exe, apm-server.exe
Rising Anti-Virus	ravmond.exe, rsmain.exe, rstray, rsmgrsvc
Monitoring and debugging tools	dbg, pchunter, hacker, monitor, wireshark
Other	lenovo, calc.exe, regedit
Unknown	remotectrlaid, superki, mfeavsv, 52pojie, kl_, watchdog

If one of the listed processes is discovered, the installer employs the 'DeviceIoControl' API call, specifying the process ID and the '0B4A00404h' IoControl code. Upon our examination of the Sysmon driver, this action results

in the termination of the identified process (T1489).



Subsequently, CleverSoar installer enumerates the files present in the folder generated by the malware and modifies their attributes by adding 0x6 (FILE_ATTRIBUTE_HIDDEN + FILE_ATTRIBUTE_SYSTEM). This modification is intended to evade file detection mechanisms (T1564.001).

The next phase involves the installation of a rootkit by creating a service which will run a rootkit dll in system startup. The installer initiates a verification process to ascertain the presence of a service named 'Nidhogg.' If the service is not already in existence, it proceeds to execute the command 'sc create Nidhogg displayname= Nidhogg binPath= “C:\Program Files (x86)\Windows NT\curl.dll” type= kernel start= auto' to create a new 'Nidhogg' service (T1543.003). The service will execute an open-sourced Nidhogg rootkit at system startup (T1014).

CleverSoar employs a persistence mechanism by executing a scheduled task upon user login (T1053). This task is initiated by dropping a .xml file into the user’s temporary folder, which contains a scheduled task XML file. By utilizing the same RPC service method previously mentioned, the installer constructs a service responsible for executing a command that creates the scheduled task with the 'Corp' name. The created task is concealed by modifying the 'Index' value under 'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Corp' registry key to 0 (T1564).

After persistence set, the installer turns the Windows firewall off by executing the 'netsh advfirewall set allprofiles state off' command (T1562.004).

The malware now proceeds to the next stages of execution. Firstly, it checks if the 'winnt.exe' binary exists within the malware-created folder. In the event of its presence, the installer executes a command to create a scheduled task that will execute the binary once and immediately delete the scheduled task. The task responsible for executing the 'winnt.exe' is named 'PayloadTask1'. If the binary is not present in the folder, the installer will persistently enumerate the folder and search for it. Based on our analysis of the 'winnt.exe' binary, it appears to be a Winos4.0 command-and-control (C2) framework implant that has recently been covered in Trend Micro’s report.

The installer executes the same process with the 'runtime.exe' binary. The task responsible for executing this binary is designated as 'PayloadTask2'. Based on our investigation, 'runtime.exe' appears to be a custom backdoor, facilitating communication with the C2 server via a proprietary protocol.

By the time of the investigation the C2 server was already down and Rapid7 Labs could not continue the further analysis of interaction between the C2 server and the malware.

Conclusion

The CleverSoar campaign highlights an advanced and targeted threat, employing sophisticated evasion techniques and highly customized malware components like the Winos4.0 framework and Nidhogg rootkit. The campaign's selective targeting of Chinese and Vietnamese-speaking users, along with its layered anti-detection measures, points to a persistent espionage effort by a capable threat actor. While currently aimed at individual users, this campaign's tactics and tools demonstrate a level of sophistication that could easily extend to organizational targets. Organizations in the affected regions should take notice of the TTPs of this actor and monitor suspicious activity.

IOCs

F70b34e2b1716528a3c3fffdbfc008003b9685f1a4da2e5a6052612de92b0c68	**CleverSoar installer**
156.224.26.7	Winos4.0 C2
8848.twilight.zip	Backdoor C2

References

- https://github.com/BlackSnufkin/BYOVD/tree/main/TfSysMon-Killer
- https://www.ired.team/offensive-security/defense-evasion/preventing-3rd-party-dlls-from-injecting-into-your-processes

---