This New Fileless Malware Hides Shellcode in Windows Event Logs

thehackernews.com/2022/05/this-new-fileless-malware-hides.html

May 6, 2022

A new malicious campaign has been spotted taking advantage of Windows event logs to stash chunks of shellcode for the first time in the wild.

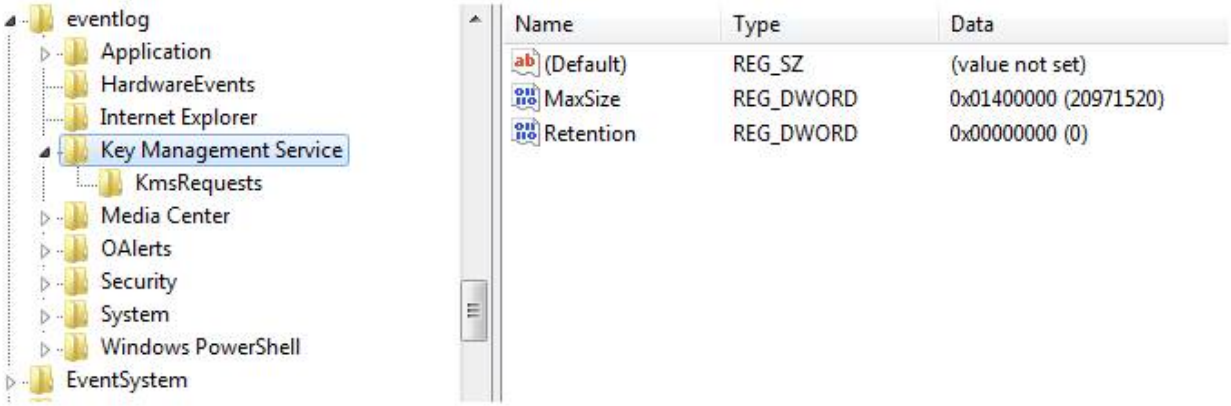
"It allows the 'fileless' last stage trojan to be hidden from plain sight in the file system," Kaspersky researcher Denis Legezo said in a technical write-up published this week.

The stealthy infection process, not attributed to a known actor, is believed to have commenced in September 2021 when the intended targets were lured into downloading compressed .RAR files containing Cobalt Strike and Silent Break.

"The spreading of the Cobalt Strike module was achieved by persuading the target to download the link to the .RAR on the legitimate site file.io, and run it themselves," Legezo explained.

The adversary simulation software modules are then used as a launchpad to inject code into Windows system processes or trusted applications.

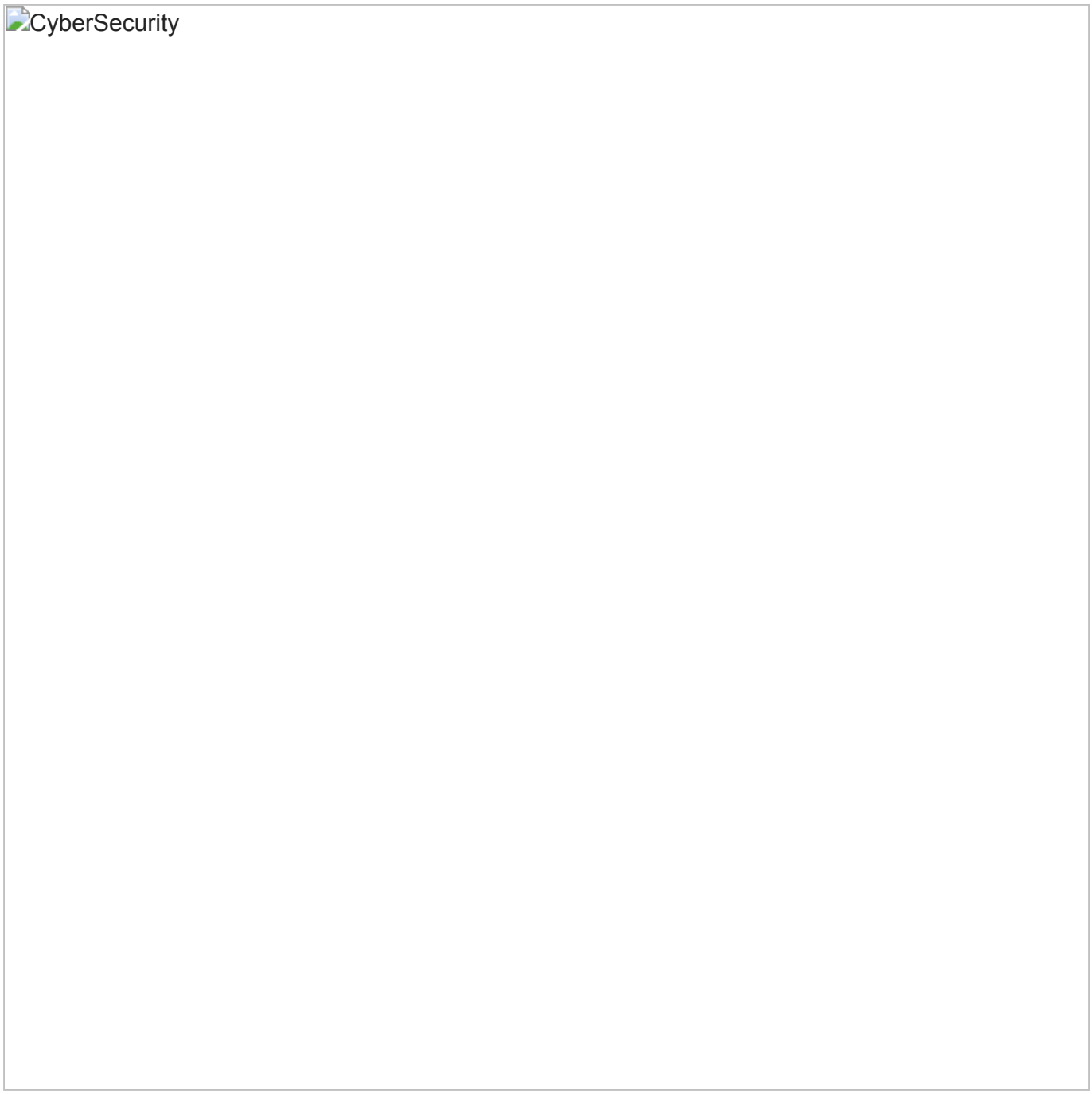
Also notable is the use of anti-detection wrappers as part of the toolset, suggesting an attempt on the part of the operators to fly under the radar.



One of the key methods is to keep encrypted shellcode containing the next-stage malware as 8KB pieces in event logs, a never-before-seen technique in real-world attacks, that's then combined and executed.

Anti-detection technique	Usage
Several compilers	The same AES256 CBC decryption could be done with Go and C++ modules
Whitelisted launchers	Autorunned copy of WerFault.exe maps the launcher into process address space
Digital certificate	15 files are signed with "Fast Invest" certificate. We didn't observe any legitimate files signed with it
Patch logging exports of ntdll.dll	To be more stealthy, Go droppers patch logging-related API functions like EtwEventWriteFull in self-address space with empty functionality
Keep shellcode in event logs	This is the main innovation we observed in this campaign. Encrypted shellcode with the next stager is divided into 8 KB blocks and saved in the binary part of event logs
C2 web domain mimicking	Actor registered a web domain name with ERP in use title

The final payload is a set of trojans that employ two different communication mechanisms — HTTP with RC4 encryption and unencrypted with named pipes — which allow it to run arbitrary commands, download files from a URL, escalate privileges, and take screenshots.



Another indicator of the threat actor's evasion tactics is the use of information gleaned from initial reconnaissance to develop succeeding stages of the attack chain, including the use of a remote server that mimics legitimate software used by the victim.

"The actor behind this campaign is quite capable," Legezo said. "The code is quite unique, with no similarities to known malware."

The disclosure comes as Sysdig researchers demonstrated a way to compromise read-only containers with fileless malware that's executed in-memory by leveraging a critical flaw in Redis servers.

SHARE

SHARE

windows malware, windows security