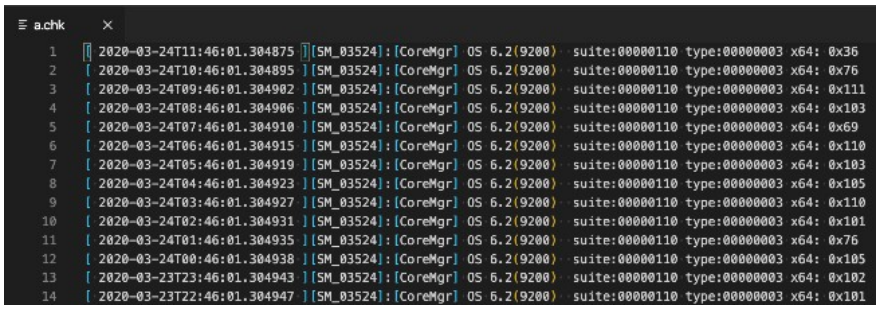
Hide malicious code in Windows logs file to attack computers, new ways of attack by hackers

Hackers are constantly inventing new ways to attack corporate and user computer systems.

Recently, Huntress Labs, a software vendor that detects cyber security threats, has uncovered a sophisticated new hacker script. This attack scenario requires a lot of perseverance, but the results can be huge for hackers.

Specifically, after gaining access to the victim's computer, hackers will use a file called "a.chk" to silently deploy malicious code. This file will be disguised as an error log file for Windows application.

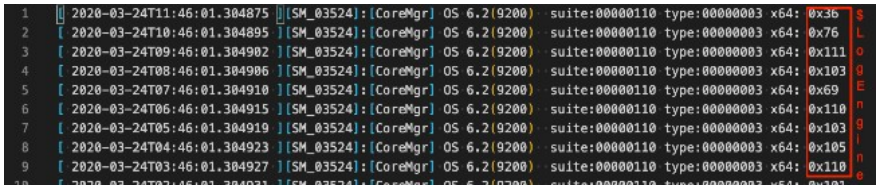


The fake log file is named a.chk
The parameters in this file are normal except for the last column. At a glance, this column looks like it contains hexadecimal values. However, when converting to decimal, this is the number of the characters in the ASCII table. Once decoded, these characters form a script that links to the hacker's control server to help them carry out further actions.

Without careful review, even security experts do not recognize the abnormality of these logs files. The columns and rows are both time and reference markers for the internal version number of Microsoft.

A closer inspection revealed that the hacker had hidden the code to extract the relevant data and build an encrypted payload. The payload is part of a malware, a piece of code that is run on the victim's computer, used to perform certain malicious activities, such as destroying data, sending spam or encrypting data. In addition to the payload, such malware has additional overhead code to spread it, or to avoid being identified.

You can see how the hacker hid the code in the image below, notice the rightmost column:

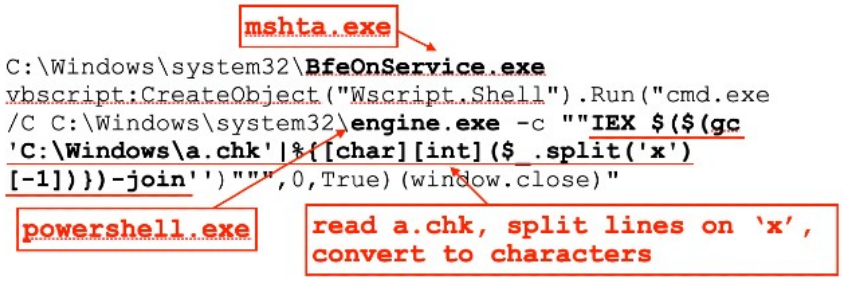


The values ??in the last column can be turned into dangerous codes

According to security expert John Ferrell, vice president of Hunttress Labs, payloads are created by faking Windows scheduled tasks. The two scripts executed in this new attack method are renamed to the same default commands to avoid detection.

The first code is called BfeOnService.exe, a copy of mshta.exe. This code executes VBScript to start PowerShell and run the commands in it.

The second code is named engine.exe, a copy of powershell.exe. This code is responsible for extracting ASCII numbers in the fake logs file and decoding them into other scripts to build the payload.



At launch, the code together creates a payload, collecting information on the victim's computer
Once built, the payload will collect information about the browser, tax-related software, security software and PoS software installed on the victim's computer.

At this time, it is not known which hacker or organization is behind this attack. This is a fairly sophisticated attack method and it shows that hackers are trying to find ways to intrude and steal important information on personal computers and businesses.