Akademia Techniczno-Humanistyczna w Bielsku-Białej
WYDZIAŁ BUDOWY MASZYN I INFORMATYKI
Inżynier XXI wieku
X Inter University Conference „Engineer of XXI Century" – 11 December 2020

ANALYSIS OF "FILELESS" MALWARE AND ATTACKS

let's call a spade a spade!

Basics

01 RAM stored

02 use LoLs

01 Doesn't touch the disk, and does not trigger antivirus file scanning.

02 Is loaded in the context of the legitimate process that executed the scripts.

01 The installation can be actually controlled by a separate program that includes a file.

02 It has own resilience scripts that are written to the operating system registry and restarted when is turned on.

Why it's not fileless?

which is REALLY fileless?

I type

No file activity performed
A compromised device may have malicious code in device firmware, a USB peripheral, or in the firmware of a network card.

II type

Indirect file activity
It doesn't directly write files on the file system, but they can end up using files indirectly (install a malicious PowerShell command within the WMI repository and configure a WMI filter to run the command periodically).

III type

Files required to operate
An initial file may exploit the operating system, the Java/Flash engine, etc. to execute a shellcode and deliver a payload in memory. While the payload is fileless, the initial entry vector is a file.

Out of sight but not invisible

- Keep your software up to date
- Secure possible entry points
- Disable unnecessary functionality
- Behavior monitoring
- Memory scanning
- Boot sector protection

Anna TORCHYLO Andrii BIGDAN Tetiana BABENKO