

Enumerates physical storage devices • 1 TTPs
Attempts to interact with connected storage/optical drive(s).

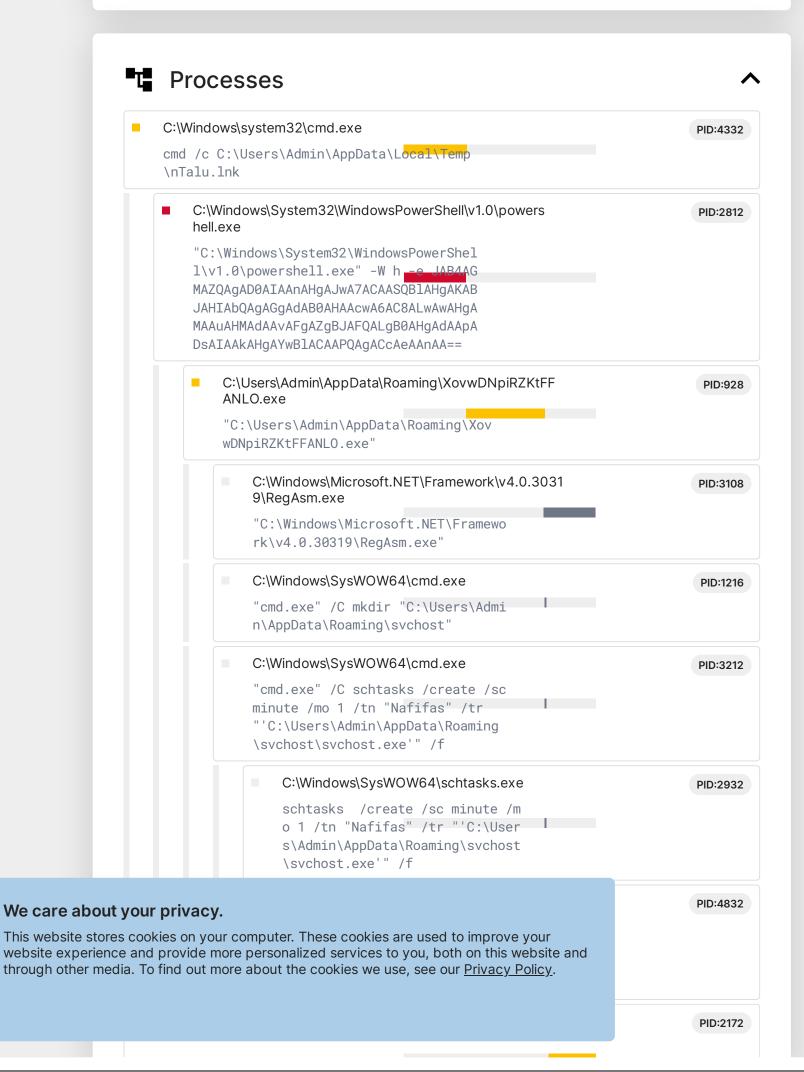
System Location Discovery: System Language Discovery • 1 TTPs 7 IoCs
Attempt gather information about the system language of a victim in order to infer the geographical location of that host.

DISCOVERY

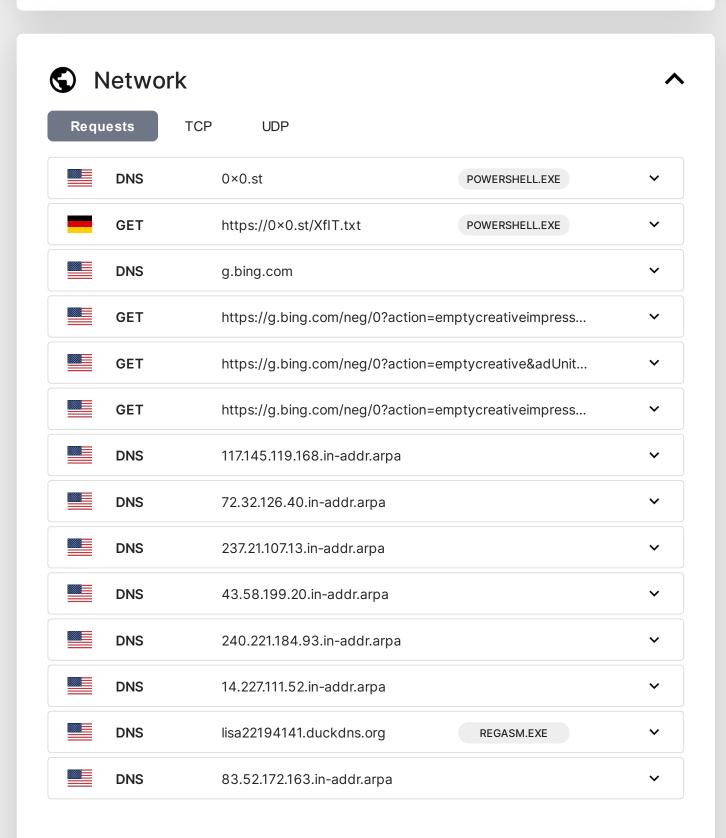
Scheduled Task/Job: Scheduled Task • 1 TTPs 1 IoCs
Schtasks is often used by malware for persistence or to perform post-infection execution.

PERSISTENCE EXECUTION

Suspicious behavior: AddClipboardFormatListener • 1 IoCs
Suspicious use of AdjustPrivilegeToken • 2 IoCs
Suspicious use of SetWindowsHookEx • 1 IoCs
Suspicious use of WriteProcessMemory • 25 IoCs

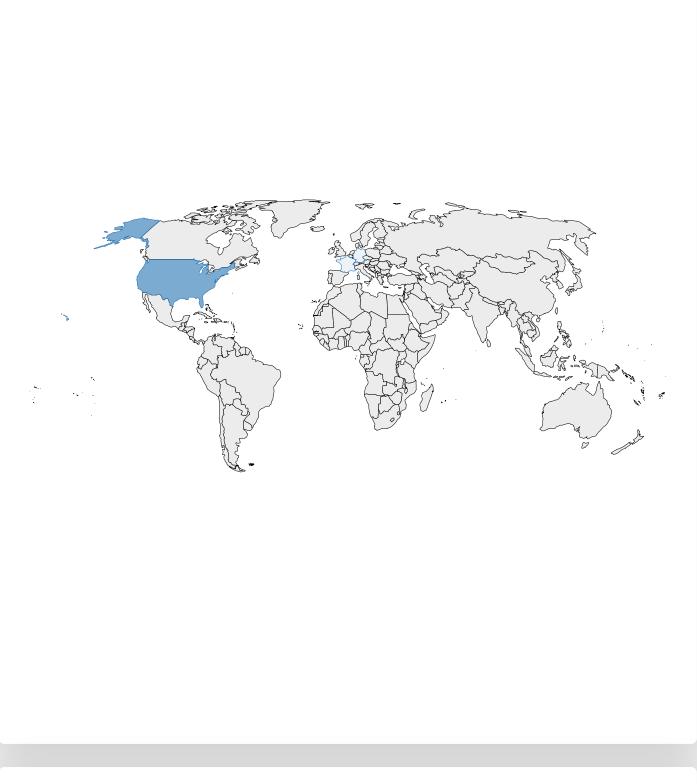


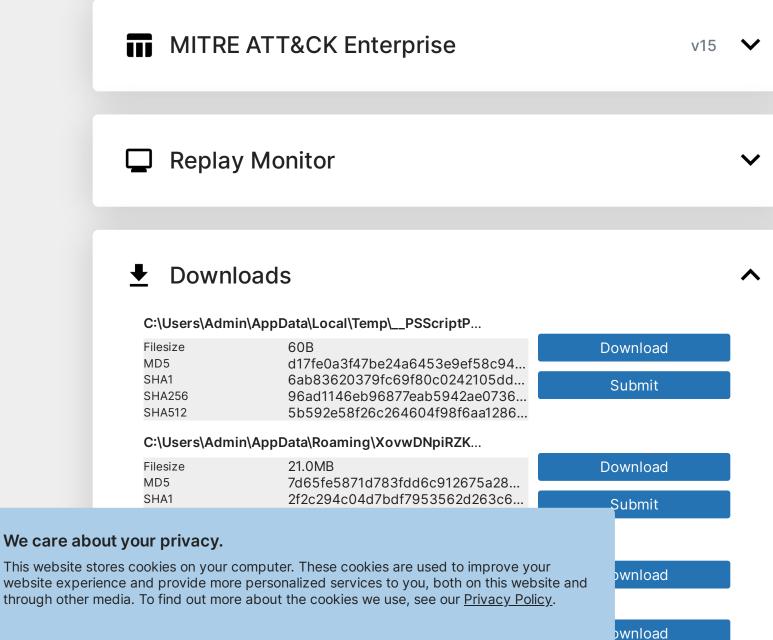
C:\Users\Admin\AppData\Roaming\svchost\s
vchost.exe



We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our <u>Privacy Policy</u>.





memory/2812-8-0×0000016867650000-0×0000...
Filesize 136KB

memory/2812-15-0×00007FFA3D403000-0×000...
Filesize 8KB

memory/2812-16-0×00007FFA3D400000-0×000...
Filesize 0 10.8MB
© 2018-2024

Terms | Privacy

We care about your privacy.

This website stores cookies on your computer. These cookies are used to improve your website experience and provide more personalized services to you, both on this website and through other media. To find out more about the cookies we use, see our <u>Privacy Policy</u>.