Digital pre-digging tool infects Windows computers via EternalBlue and WMI

A newly discovered malware family called CoinMiner is causing many users and companies to secure many problems, making it difficult to prevent or detect the combination of many unique features.

A newly discovered malware family called CoinMiner is causing many users and companies to secure many problems, making it difficult to prevent or detect the combination of many unique features.

Malware - a digital digging tool - uses the NSA EternalBlue vulnerability to infect victims and the WMI toolkit (Windows Management Instrumentation) as a way of running commands on infected systems. In addition, CoinMiner runs on memory (malware without fileless files), uses multiple command classes and control servers to deploy the necessary scenarios to infect victims.

All of this creates a mixture of trouble for older computers, running anti-virus software is no longer suitable for new infection techniques.

Avoid getting infected with CoinMiner by turning off SMBv1

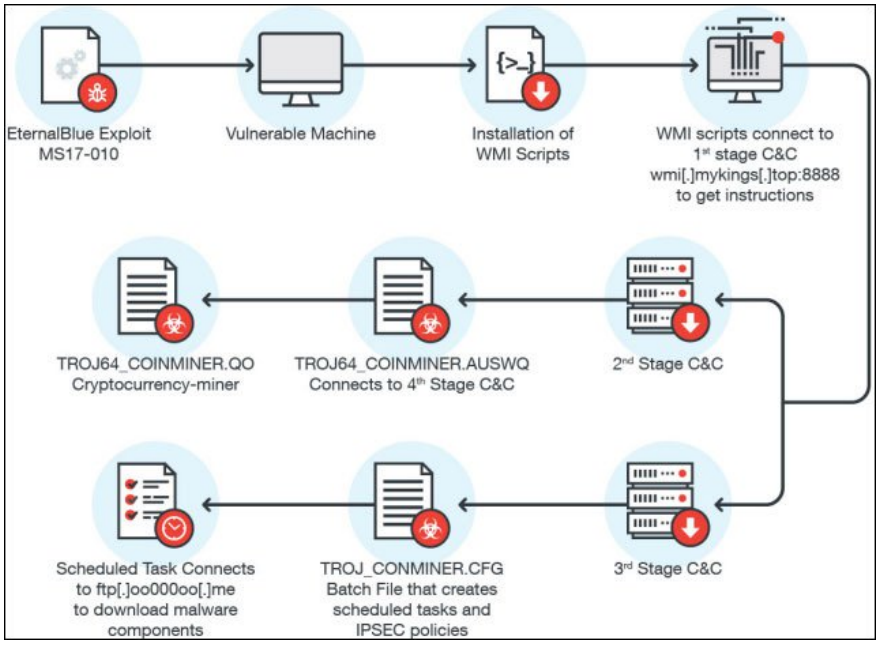
To avoid infection with CoinMiner, there are a number of measures users need to take. The simplest is to prevent the first infection, EternalBlue, a SMB vulnerability developed by the NSA and leaked online by Shadow Brokers hacker group. It is also used in attacks on WannaCry and NotPetya.

Users need to be sure to install Microsoft's MS17-010 security patch or at least turn off the SMBv1 protocol on their machines so that CoinMiner has no way of approaching.

Turn off WMI

In case the above protocol needs to be used to get network interaction, it is still possible to avoid CoinMiner by protecting itself from the second exploit of malware, which is WMI - the toolkit integrated in Windows versions.
.

CoinMiner uses WMI to download scripts and other necessary components to infect computers and then download and run the real CoinMiner binary file.



CoinMiner computer infiltration process

Trend Micro, the company that discovered CoinMiner, recommends turning off WMI on a machine if it is not needed or at least restricting access to WMI to just one admin account, only IT staff.

Instructions on how to turn off SMBv1 and WMI are given at this address *https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3- in-windows-and-windows* and *https://msdn.microsoft.com/en-us/library/aa826517(v=vs.85).aspx* . For more detailed information, Trend Micro also released a detailed step-by-step technical report of CoinMiner. *http://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-miner-uses-wmi-eternalblue-spread-filelessly/*

CoinMiner is not the first digital digging tool to use EternalBlue to attack victims. Adylkuzz is the first malware of its kind, starting to attack shortly after the Shadow Brokers team leaked it on the network. On the other hand, CoinMiner is one of the few less-than-non-program-based virtual money digging tools.