NotPetya, Software S0368 | MITRE ATT&CK®

Archived: 2026-04-05 18:28:56 UTC

Enterprise T1486 Data Encrypted for Impact

NotPetya encrypts user files and disk structures like the MBR with 2048-bit RSA.[1][2][4]

Enterprise T1210 Exploitation of Remote Services

NotPetya can use two exploits in SMBv1, EternalBlue and EternalRomance, to spread itself to other remote systems on the network.[1][2][4]

Enterprise T1083 File and Directory Discovery

NotPetya searches for files ending with dozens of different file extensions prior to encryption.[4]

Enterprise T1070 .001 Indicator Removal: Clear Windows Event Logs

NotPetya uses `wevtutil` to clear the Windows event logs.[1][4]

Enterprise T1036 Masquerading

NotPetya drops PsExec with the filename dllhost.dat.[1]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

NotPetya contains a modified version of Mimikatz to help gather credentials that are later used for lateral movement.[1][2][5]

Enterprise T1021 .002 Remote Services: SMB/Windows Admin Shares

NotPetya can use PsExec, which interacts with the `ADMIN$` network share to execute commands on remote systems.[1][2][6]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

NotPetya creates a task to reboot the system one hour after infection.[1]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

NotPetya determines if specific antivirus programs are running on an infected host machine.[4]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

NotPetya uses `rundll32.exe` to install itself on remote systems when accessed via PsExec or `wmic`.[1]

Enterprise T1569 .002 System Services: Service Execution

NotPetya can use PsExec to help propagate itself across a network.[1][2]

Enterprise T1529 System Shutdown/Reboot

NotPetya will reboot the system one hour after infection.[1][4]

Enterprise T1078 .003 Valid Accounts: Local Accounts

NotPetya can use valid credentials with PsExec or `wmic` to spread itself to remote systems.[1][2]

Enterprise T1047 Windows Management Instrumentation

NotPetya can use `wmic` to help propagate itself across a network.[1][2]

ICS T0866 Exploitation of Remote Services

NotPetya initially infected IT networks, but by means of an exploit (particularly the SMBv1-targeting MS17-010 vulnerability) spread to industrial networks. [7]

ICS T0867 Lateral Tool Transfer

NotPetya can move laterally through industrial networks by means of the SMB service. [7]

ICS T0828 Loss of Productivity and Revenue

NotPetya disrupted manufacturing facilities supplying vaccines, resulting in a halt of production and the inability to meet demand for specific vaccines. [8]
