Shamoon, Software S0140 | MITRE ATT&CK®

Archived: 2026-04-05 12:45:46 UTC

Enterprise T1548 .002 Abuse Elevation Control Mechanism: Bypass User Account Control

Shamoon attempts to disable UAC remote restrictions by modifying the Registry.[2]

Enterprise T1134 .001 Access Token Manipulation: Token Impersonation/Theft

Shamoon can impersonate tokens using `LogonUser`, `ImpersonateLoggedOnUser`, and `ImpersonateNamedPipeClient`.[6]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Shamoon has used HTTP for C2.[2]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

Shamoon creates a new service named "ntssrv" to execute the payload. Newer versions create the "MaintenaceSrv" and "hdv_725x" services.[2][3]

Enterprise T1485 Data Destruction

Shamoon attempts to overwrite operating system files and disk structures with image files.[4][5][2] In a later variant, randomly generated data was used for data overwrites.[3][6]

Enterprise T1486 Data Encrypted for Impact

Shamoon has an operational mode for encrypting data instead of overwriting it.[2][3]

Enterprise T1140 Deobfuscate/Decode Files or Information

Shamoon decrypts ciphertext using an XOR cipher and a base64-encoded string.[3]

Enterprise T1561 .002 Disk Wipe: Disk Structure Wipe

Shamoon has been seen overwriting features of disk structure such as the MBR.[4][5][2][3]

Enterprise T1070 .006 Indicator Removal: Timestomp

Shamoon can change the modified time for files to evade forensic detection.[6]

Enterprise T1105 Ingress Tool Transfer

Shamoon can download an executable to run on the victim.[2]

Enterprise T1570 Lateral Tool Transfer

Shamoon attempts to copy itself to remote machines on the network.[2]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

Shamoon creates a new service named "ntssrv" that attempts to appear legitimate; the service's display name is "Microsoft Network Realtime Inspection Service" and its description is "Helps guard against time change attempts targeting known and newly discovered vulnerabilities in network time protocols." Newer versions create the "MaintenaceSrv" service, which misspells the word "maintenance."[2][6]

Enterprise T1112 Modify Registry

Once Shamoon has access to a network share, it enables the RemoteRegistry service on the target system. It will then connect to the system with RegConnectRegistryW and modify the Registry to disable UAC remote restrictions by setting `SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy` to 1.[5][2][6]

Enterprise T1027 Obfuscated Files or Information

Shamoon contains base64-encoded strings.[2]

Enterprise T1012 Query Registry

Shamoon queries several Registry keys to identify hard disk partitions to overwrite.[2]

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

Shamoon accesses network share(s), enables share access to the target device, copies an executable payload to the target system, and uses a Scheduled Task/Job to execute the malware.[5]

Enterprise T1018 Remote System Discovery

Shamoon scans the C-class subnet of the IPs on the victim's interfaces.[5]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Shamoon copies an executable payload to the target system by using SMB/Windows Admin Shares and then scheduling an unnamed task to execute the malware.[5][2]

Enterprise T1082 System Information Discovery

Shamoon obtains the victim's operating system version and keyboard layout and sends the information to the C2 server.[2][3]

Enterprise T1016 System Network Configuration Discovery

Shamoon obtains the target's IP address and local network segment.[2][6]

Enterprise T1569 .002 System Services: Service Execution

Shamoon creates a new service named "ntssrv" to execute the payload. Shamoon can also spread via PsExec.[2][7]

Enterprise T1529 System Shutdown/Reboot

Shamoon will reboot the infected system once the wiping functionality has been completed.[3][6]

Enterprise T1124 System Time Discovery

Shamoon obtains the system time and will only activate if it is greater than a preset date.[2][3]

Enterprise T1078 .002 Valid Accounts: Domain Accounts

If Shamoon cannot access shares using current privileges, it attempts access using hard coded, domain-specific credentials gathered earlier in the intrusion.[5][3]
