Epic, Software S0091 | MITRE ATT&CK®

Archived: 2026-04-05 12:47:28 UTC

Enterprise T1087 .001 Account Discovery: Local Account

Epic gathers a list of all user accounts, privilege classes, and time of last logon.[2]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Epic uses HTTP and HTTPS for C2 communications.[1][2]

Enterprise T1560 Archive Collected Data

Epic encrypts collected data using a public key framework before sending it over the C2 channel.[1] Some variants encrypt the collected data with AES and encode it with base64 before transmitting it to the C2 server.[2]

.002 Archive via Library

Epic compresses the collected data with bzip2 before sending it to the C2 server.[2]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Epic encrypts commands from the C2 server using a hardcoded key.[1]

Enterprise T1083 File and Directory Discovery

Epic recursively searches for all .doc files on the system and collects a directory listing of the Desktop, %TEMP%, and %WINDOWS%\Temp directories.[1][2]

Enterprise T1070 .004 Indicator Removal: File Deletion

Epic has a command to delete a file from the machine.[2]

Enterprise T1680 Local Storage Discovery

Epic collects disk space information.[2]

Enterprise T1027 Obfuscated Files or Information

Epic heavily obfuscates its code to make analysis more difficult.[1]

Enterprise T1069 .001 Permission Groups Discovery: Local Groups

Epic gathers information on local group names.[2]

Enterprise T1057 Process Discovery

Epic uses the `tasklist /v` command to obtain a list of processes.[1][2]

Enterprise T1055 .011 Process Injection: Extra Window Memory Injection

Epic has overwritten the function pointer in the extra window memory of Explorer's Shell_TrayWnd in order to execute malicious code in the context of the explorer.exe process.[3]

Enterprise T1012 Query Registry

Epic uses the `rem reg query` command to obtain values from Registry keys.[1]

Enterprise T1018 Remote System Discovery

Epic uses the `net view` command on the victim's machine.[1]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

Epic searches for anti-malware services running on the victim's machine and terminates itself if it finds them.[1]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

Turla has used valid digital certificates from Sysprint AG to sign its Epic dropper.[1]

Enterprise T1082 System Information Discovery

Epic collects the OS version, hardware information, computer name, available system memory status, and system and user language settings.[2]

Enterprise T1016 System Network Configuration Discovery

Epic uses the `nbtstat -n` and `nbtstat -s` commands on the victim's machine.[1]

Enterprise T1049 System Network Connections Discovery

Epic uses the `net use` , `net session` , and `netstat` commands to gather information on network connections. [1][2]

Enterprise T1033 System Owner/User Discovery

Epic collects the user name from the victim's machine.[2]

Enterprise T1007 System Service Discovery

Epic uses the `tasklist /svc` command to list the services on the system.[1]

Enterprise T1124 System Time Discovery

Epic uses the `net time` command to get the system time from the machine and collect the current date and time zone information.[1]

Source: https://attack.mitre.org/software/S0091/