

Volgmer, Software S0180 | MITRE ATT&CK®

Archived: 2026-04-05 15:00:50 UTC

Enterprise [T1059 .003 Command and Scripting Interpreter: Windows Command Shell](#)

[Volgmer](#) can execute commands on the victim's machine.^{[1][2]}

Enterprise [T1543 .003 Create or Modify System Process: Windows Service](#)

[Volgmer](#) installs a copy of itself in a randomly selected service, then overwrites the ServiceDLL entry in the service's Registry entry. Some [Volgmer](#) variants also install .dll files as services with names generated by a list of hard-coded strings.^{[1][2][3]}

Enterprise [T1140 Deobfuscate/Decode Files or Information](#)

[Volgmer](#) deobfuscates its strings and APIs once its executed.^[2]

Enterprise [T1573 .001 Encrypted Channel: Symmetric Cryptography](#)

[Volgmer](#) uses a simple XOR cipher to encrypt traffic and files.^[2]

[.002 Encrypted Channel: Asymmetric Cryptography](#)

Some [Volgmer](#) variants use SSL to encrypt C2 communications.^[1]

Enterprise [T1083 File and Directory Discovery](#)

[Volgmer](#) can list directories on a victim.^[1]

Enterprise [T1070 .004 Indicator Removal: File Deletion](#)

[Volgmer](#) can delete files and itself after infection to avoid analysis.^[2]

Enterprise [T1105 Ingress Tool Transfer](#)

[Volgmer](#) can download remote files and additional payloads to the victim's machine.^{[1][2][3]}

Enterprise [T1036 .004 Masquerading: Masquerade Task or Service](#)

Some [Volgmer](#) variants add new services with display names generated by a list of hard-coded strings such as Application, Background, Security, and Windows, presumably as a way to masquerade as a legitimate service.^{[2][3]}

Enterprise [T1112 Modify Registry](#)

[Volgmer](#) modifies the Registry to store an encoded configuration file in
HKKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Security .^{[2][3]}

Enterprise [T1106 Native API](#)

[Volgmer](#) executes payloads using the Windows API call CreateProcessW().^[2]

Enterprise [T1027 .011 Obfuscated Files or Information: Fileless Storage](#)

[Volgmer](#) stores an encoded configuration file in
HKKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Security .^{[1][3]}

[.013 Obfuscated Files or Information: Encrypted/Encoded File](#)

A [Volgmer](#) variant is encoded using a simple XOR cipher.^[2]

Enterprise [T1057 Process Discovery](#)

[Volgmer](#) can gather a list of processes.^[3]

Enterprise [T1012 Query Registry](#)

[Volgmer](#) checks the system for certain Registry keys.^[2]

Enterprise [T1082 System Information Discovery](#)

[Volgmer](#) can gather system information, the computer name, OS version, drive and serial information from the victim's machine.^{[1][2][3]}

Enterprise [T1016 System Network Configuration Discovery](#)

[Volgmer](#) can gather the IP address from the victim's machine.^[3]

Enterprise [T1049 System Network Connections Discovery](#)

[Volgmer](#) can gather information about TCP connection state.^[3]

Enterprise [T1007 System Service Discovery](#)

[Volgmer](#) queries the system to identify existing services.^[1]

Source: https://attack.mitre.org/software/S0180/