

# SombRAT, Software S0615 | MITRE ATT&CK®

Archived: 2026-04-05 15:24:52 UTC

Enterprise [T1071 .004 Application Layer Protocol: DNS](#)

[SombRAT](#) can communicate over DNS with the C2 server.<sup>[1][2]</sup>

Enterprise [T1560 .003 Archive Collected Data: Archive via Custom Method](#)

[SombRAT](#) has encrypted collected data with AES-256 using a hardcoded key.<sup>[1]</sup>

Enterprise [T1005 Data from Local System](#)

[SombRAT](#) has collected data and files from a compromised host.<sup>[1][3]</sup>

Enterprise [T1074 .001 Data Staged: Local Data Staging](#)

[SombRAT](#) can store harvested data in a custom database under the %TEMP% directory.<sup>[1]</sup>

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

[SombRAT](#) can run `upload` to decrypt and upload files from storage.<sup>[1][3]</sup>

Enterprise [T1568 .002 Dynamic Resolution: Domain Generation Algorithms](#)

[SombRAT](#) can use a custom DGA to generate a subdomain for C2.<sup>[1]</sup>

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

[SombRAT](#) has encrypted its C2 communications with AES.<sup>[1]</sup>

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

[SombRAT](#) can SSL encrypt C2 traffic.<sup>[1][2][3]</sup>

Enterprise [T1041 Exfiltration Over C2 Channel](#)

[SombRAT](#) has uploaded collected data and files from a compromised host to its C2 server.<sup>[1]</sup>

Enterprise [T1083 File and Directory Discovery](#)

[SombRAT](#) can execute `enum` to enumerate files in storage on a compromised system.<sup>[1]</sup>

Enterprise [T1564 .010 Hide Artifacts: Process Argument Spoofing](#)

[SombRAT](#) has the ability to modify its process memory to hide process command-line arguments.<sup>[2]</sup>

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

[SombRAT](#) has the ability to run `cancel` or `closeanddeletestorage` to remove all files from storage and delete the storage temp file on a compromised host.<sup>[1]</sup>

Enterprise [T1105 Ingress Tool Transfer](#)

[SombRAT](#) has the ability to download and execute additional payloads.<sup>[1][2][3]</sup>

Enterprise [T1036 Masquerading](#)

[SombRAT](#) can use a legitimate process name to hide itself.<sup>[3]</sup>

Enterprise [T1106 Native API](#)

[SombRAT](#) has the ability to respawn itself using `ShellExecuteW` and `CreateProcessW`.<sup>[1]</sup>

Enterprise [T1095 Non-Application Layer Protocol](#)

[SombRAT](#) has the ability to use TCP sockets to send data and ICMP to ping the C2 server.<sup>[1][2]</sup>

Enterprise [T1027 Obfuscated Files or Information](#)

[SombRAT](#) can encrypt strings with XOR-based routines and use a custom AES storage format for plugins, configuration, C2 domains, and harvested data.<sup>[1][2][3]</sup>

Enterprise [T1057 Process Discovery](#)

[SombRAT](#) can use the `getprocesslist` command to enumerate processes on a compromised host.<sup>[1][2][3]</sup>

Enterprise [T1055 .001 Process Injection: Dynamic-link Library Injection](#)

[SombRAT](#) can execute `loadfromfile`, `loadfromstorage`, and `loadfrommem` to inject a DLL from disk, storage, or memory respectively.<sup>[1]</sup>

Enterprise [T1090 Proxy](#)

[SombRAT](#) has the ability to use an embedded SOCKS proxy in C2 communications.<sup>[3]</sup>

Enterprise [T1082 System Information Discovery](#)

[SombRAT](#) can execute `getinfo` to enumerate the computer name and OS version of a compromised system.<sup>[1]</sup>

Enterprise [T1033 System Owner/User Discovery](#)

[SombRAT](#) can execute `getinfo` to identify the username on a compromised host.<sup>[1][3]</sup>

Enterprise [T1007 System Service Discovery](#)

[SombRAT](#) can enumerate services on a victim machine.<sup>[1]</sup>

Enterprise [T1124 System Time Discovery](#).

[SombRAT](#) can execute `getinfo` to discover the current time on a compromised host.<sup>[1][3]</sup>

---

Source: <https://attack.mitre.org/software/S0615>