Remsec, Software S0125 | MITRE ATT&CK®

Archived: 2026-04-05 18:45:04 UTC

Enterprise T1087 .001 Account Discovery: Local Account

Remsec can obtain a list of users.[3]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Remsec is capable of using HTTP and HTTPS for C2.[4][5][3]

.003 Application Layer Protocol: Mail Protocols

Remsec is capable of using SMTP for C2.[4][5][3][6]

.004 Application Layer Protocol: DNS

Remsec is capable of using DNS for C2.[4][5][3]

Enterprise T1059 .011 Command and Scripting Interpreter: Lua

Remsec can use modules written in Lua for execution.[7]

Enterprise T1025 Data from Removable Media

Remsec has a package that collects documents from any inserted USB sticks.[3]

Enterprise T1652 Device Driver Discovery

Remsec has a plugin to detect active drivers of some security products.[3]

Enterprise T1048 .003 Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol

Remsec can exfiltrate data via a DNS tunnel or email, separately from its C2 channel.[5]

Enterprise T1052 .001 Exfiltration Over Physical Medium: Exfiltration over USB

Remsec contains a module to move data from airgapped networks to Internet-connected systems by using a removable USB device.[5]

Enterprise T1068 Exploitation for Privilege Escalation

Remsec has a plugin to drop and execute vulnerable Outpost Sandbox or avast! Virtualization drivers in order to gain kernel mode privileges.[3]

Enterprise T1083 File and Directory Discovery

Remsec is capable of listing contents of folders on the victim. Remsec also searches for custom network encryption software on victims.[4][5][3]

Enterprise T1562 .004 Impair Defenses: Disable or Modify System Firewall

Remsec can add or remove applications or ports on the Windows firewall or disable it entirely.[3]

Enterprise T1070 .004 Indicator Removal: File Deletion

Remsec is capable of deleting files on the victim. It also securely removes itself after collecting and exfiltrating data.[4][5][3]

Enterprise T1105 Ingress Tool Transfer

Remsec contains a network loader to receive executable modules from remote attackers and run them on the local victim. It can also upload and download files over HTTP and HTTPS.[4][3]

Enterprise T1056 .001 Input Capture: Keylogging

Remsec contains a keylogger component.[4][3]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

The Remsec loader implements itself with the name Security Support Provider, a legitimate Windows function. Various Remsec .exe files mimic legitimate file names used by Microsoft, Symantec, Kaspersky, Hewlett-Packard, and VMWare. Remsec also disguised malicious modules using similar filenames as custom network encryption software on victims.[8][5]

Enterprise T1556 .002 Modify Authentication Process: Password Filter DLL

Remsec harvests plain-text credentials as a password filter registered on domain controllers.[5]

Enterprise T1046 Network Service Discovery

Remsec has a plugin that can perform ARP scanning as well as port scanning.[3]

Enterprise T1095 Non-Application Layer Protocol

Remsec is capable of using ICMP, TCP, and UDP for C2.[4][5]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

Some data in Remsec is encrypted using RC5 in CBC mode, AES-CBC with a hardcoded key, RC4, or Salsa20. Some data is also base64-encoded.[4][3]

Enterprise T1003 .002 OS Credential Dumping: Security Account Manager

Remsec can dump the SAM database.[3]

Enterprise T1057 Process Discovery

Remsec can obtain a process list from the victim.[3]

Enterprise T1055 .001 Process Injection: Dynamic-link Library Injection

Remsec can perform DLL injection.[3]

Enterprise T1018 Remote System Discovery

Remsec can ping or traceroute a remote host.[3]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Remsec schedules the execution one of its modules by creating a new scheduler task.[3]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

Remsec has a plugin detect security products via active drivers.[3]

Enterprise T1082 System Information Discovery

Remsec can obtain the OS version information, computer name, processor architecture, machine role, and OS edition.[3]

Enterprise T1016 System Network Configuration Discovery

Remsec can obtain information about network configuration, including the routing table, ARP cache, and DNS cache.[3]

Enterprise T1049 System Network Connections Discovery

Remsec can obtain a list of active connections and open ports.[3]

Enterprise T1033 System Owner/User Discovery

Remsec can obtain information about the current user.[3]
