SVCReady, Software S1064 | MITRE ATT&CK®

Archived: 2026-04-05 15:56:02 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

SVCReady can communicate with its C2 servers via HTTP.[1]

Enterprise T1059 .005 Command and Scripting Interpreter: Visual Basic

SVCReady has used VBA macros to execute shellcode.[1]

Enterprise T1005 Data from Local System

SVCReady can collect data from an infected host.[1]

Enterprise T1546 .015 Event Triggered Execution: Component Object Model Hijacking

SVCReady has created the `HKEY_CURRENT_USER\Software\Classes\CLSID\{E6D34FFC-AD32-4d6a-934C-D387FA873A19}` Registry key for persistence.[1]

Enterprise T1041 Exfiltration Over C2 Channel

SVCReady can send collected data in JSON format to its C2 server.[1]

Enterprise T1105 Ingress Tool Transfer

SVCReady has the ability to download additional tools such as the RedLine Stealer to an infected host.[1]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

SVCReady has named a task `RecoveryExTask` as part of its persistence activity.[1]

Enterprise T1106 Native API

SVCReady can use Windows API calls to gather information from an infected host.[1]

Enterprise T1027 Obfuscated Files or Information

SVCReady can encrypt victim data with an RC4 cipher.[1]

Enterprise T1120 Peripheral Device Discovery

SVCReady can check for the number of devices plugged into an infected host.[1]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

SVCReady has been distributed via spearphishing campaigns containing malicious Mircrosoft Word documents.[1]

Enterprise T1057 Process Discovery

SVCReady can collect a list of running processes from an infected host.[1]

Enterprise T1012 Query Registry

SVCReady can search for the `HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System` Registry key to gather system information.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

SVCReady can create a scheduled task named `RecoveryExTask` to gain persistence.[1]

Enterprise T1113 Screen Capture

SVCReady can take a screenshot from an infected host.[1]

Enterprise T1518 Software Discovery

SVCReady can collect a list of installed software from an infected host.[1]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

SVCReady has used `rundll32.exe` for execution.[1]

Enterprise T1082 System Information Discovery

SVCReady has the ability to collect information such as computer name, computer manufacturer, BIOS, operating system, and firmware, including through the use of `systeminfo.exe`.[1]

Enterprise T1033 System Owner/User Discovery

SVCReady can collect the username from an infected host.[1]

Enterprise T1124 System Time Discovery

SVCReady can collect time zone information.[1]

Enterprise T1204 .002 User Execution: Malicious File

SVCReady has relied on users clicking a malicious attachment delivered through spearphishing.[1]

Enterprise T1497 .001 Virtualization/Sandbox Evasion: System Checks

SVCReady has the ability to determine if its runtime environment is virtualized.[1]

.003 Virtualization/Sandbox Evasion: Time Based Checks

SVCReady can enter a sleep stage for 30 minutes to evade detection.[1]

Enterprise T1047 Windows Management Instrumentation

SVCReady can use `WMI` queries to detect the presence of a virtual machine environment.[1]
