SDBbot, Software S0461 | MITRE ATT&CK®

Archived: 2026-04-05 14:26:57 UTC

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

SDBbot has the ability to add a value to the Registry Run key to establish persistence if it detects it is running with regular user privilege. [1][2]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

SDBbot has the ability to use the command shell to execute commands on a compromised host.[1]

Enterprise T1005 Data from Local System

SDBbot has the ability to access the file system on a compromised host.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

SDBbot has the ability to decrypt and decompress its payload to enable code execution.[1][2]

Enterprise T1546 .011 Event Triggered Execution: Application Shimming

SDBbot has the ability to use application shimming for persistence if it detects it is running as admin on Windows XP or 7, by creating a shim database to patch services.exe.[1]

.012 Event Triggered Execution: Image File Execution Options Injection

SDBbot has the ability to use image file execution options for persistence if it detects it is running with admin privileges on a Windows version newer than Windows 7.[1]

Enterprise T1041 Exfiltration Over C2 Channel

SDBbot has sent collected data from a compromised host to its C2 servers.[3]

Enterprise T1083 File and Directory Discovery

SDBbot has the ability to get directory listings or drive information on a compromised host.[1]

Enterprise T1070 Indicator Removal

SDBbot has the ability to clean up and remove data structures from a compromised host.[1]

.004 File Deletion

SDBbot has the ability to delete files from a compromised host.[1]

Enterprise T1105 Ingress Tool Transfer

SDBbot has the ability to download a DLL from C2 to a compromised host.[1]

Enterprise T1095 Non-Application Layer Protocol

SDBbot has the ability to communicate with C2 with TCP over port 443.[1]

Enterprise T1027 Obfuscated Files or Information

SDBbot has the ability to XOR the strings for its installer component with a hardcoded 128 byte key.[1]

.002 Software Packing

SDBbot has used a packed installer file.[2]

Enterprise T1057 Process Discovery

SDBbot can enumerate a list of running processes on a compromised machine.[3]

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

SDBbot has the ability to inject a downloaded DLL into a newly created rundll32.exe process.[1]

Enterprise T1090 Proxy

SDBbot has the ability to use port forwarding to establish a proxy between a target host and C2.[1]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

SDBbot has the ability to use RDP to connect to victim's machines.[1]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

SDBbot has used rundll32.exe to execute DLLs.[3]

Enterprise T1082 System Information Discovery

SDBbot has the ability to identify the OS version, OS bit information and computer name.[1][3]

Enterprise T1614 System Location Discovery

SDBbot can collected the country code of a compromised machine.[3]

Enterprise T1016 System Network Configuration Discovery

SDBbot has the ability to determine the domain name and whether a proxy is configured on a compromised host.[1]

Enterprise T1033 System Owner/User Discovery

SDBbot has the ability to identify the user on a compromised host.[1]

Enterprise T1125 Video Capture

SDBbot has the ability to record video on a compromised host.[1][2]

Source: https://attack.mitre.org/software/S0461