BBSRAT, Software S0127 | MITRE ATT&CK®

Archived: 2026-04-05 18:12:34 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	BBSRAT uses GET and POST requests over HTTP or HTTPS for command and control to obtain commands and send ZLIB compressed data back to the C2 server.[1]
Enterprise	T1560	.002	Archive Collected Data: Archive via Library	BBSRAT can compress data with ZLIB prior to sending it back to the C2 server.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	BBSRAT has been loaded through DLL side-loading of a legitimate Citrix executable that is set to persist through the Registry Run key location `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ssonsvr.exe`
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	BBSRAT can modify service configurations.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	BBSRAT uses Expand to decompress a CAB file into executable content.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	BBSRAT uses a custom encryption algorithm on data sent back to the C2 server over HTTP.[1]
Enterprise	T1546	.015	Event Triggered Execution: Component Object Model Hijacking	BBSRAT has been seen persisting via COM hijacking through replacement of the COM object for MruPidlList `{42aedc87-2188-41fd-b9a3-0c966feabec1}` or Microsoft WBEM New Event Subsystem `{F3130CDB-AA52-4C3A-AB32-85FFC23AF9C1}` depending on the system's CPU architecture.[1]
Enterprise	T1083		File and Directory Discovery	BBSRAT can list file and directory information.[1]

Domain	ID		Name	Use
Enterprise	T1574	.001	Hijack Execution Flow: DLL	DLL side-loading has been used to execute BBSRAT through a legitimate Citrix executable, ssonsvr.exe. The Citrix executable was dropped along with BBSRAT by the dropper.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	BBSRAT can delete files and directories.[1]
Enterprise	T1057		Process Discovery	BBSRAT can list running processes.[1]
Enterprise	T1055	.012	Process Injection: Process Hollowing	BBSRAT has been seen loaded into msiexec.exe through process hollowing to hide its execution.[1]
Enterprise	T1007		System Service Discovery	BBSRAT can query service configuration information.[1]
Enterprise	T1569	.002	System Services: Service Execution	BBSRAT can start, stop, or delete services.[1]
