BackdoorDiplomacy, Group G0135 | MITRE ATT&CK®

Archived: 2026-04-05 14:17:24 UTC

Enterprise T1074 .001 Data Staged: Local Data Staging

BackdoorDiplomacy has copied files of interest to the main drive's recycle bin.[1]

Enterprise T1190 Exploit Public-Facing Application

BackdoorDiplomacy has exploited CVE-2020-5902, an F5 BIP-IP vulnerability, to drop a Linux backdoor. BackdoorDiplomacy has also exploited mis-configured Plesk servers.[1]

Enterprise T1574 .001 Hijack Execution Flow: DLL

BackdoorDiplomacy has executed DLL search order hijacking.[1]

Enterprise T1105 Ingress Tool Transfer

BackdoorDiplomacy has downloaded additional files and tools onto a compromised host.[1]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

BackdoorDiplomacy has disguised their backdoor droppers with naming conventions designed to blend into normal operations.[1]

.005 Masquerading: Match Legitimate Resource Name or Location

BackdoorDiplomacy has dropped implants in folders named for legitimate software.[1]

Enterprise T1046 Network Service Discovery

BackdoorDiplomacy has used SMBTouch, a vulnerability scanner, to determine whether a target is vulnerable to EternalBlue malware.[1]

Enterprise T1095 Non-Application Layer Protocol

BackdoorDiplomacy has used EarthWorm for network tunneling with a SOCKS5 server and port transfer functionalities.[1]

Enterprise T1027 Obfuscated Files or Information

BackdoorDiplomacy has obfuscated tools and malware it uses with VMProtect.[1]

Enterprise T1588 .001 Obtain Capabilities: Malware

BackdoorDiplomacy has obtained and used leaked malware, including DoublePulsar, EternalBlue, EternalRocks, and EternalSynergy, in its operations.[1]

.002 Obtain Capabilities: Tool

BackdoorDiplomacy has obtained a variety of open-source reconnaissance and red team tools for discovery and lateral movement.[1]

Enterprise T1120 Peripheral Device Discovery

BackdoorDiplomacy has used an executable to detect removable media, such as USB flash drives.[1]

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

BackdoorDiplomacy has dropped legitimate software onto a compromised host and used it to execute malicious DLLs.[1]

Enterprise T1505 .003 Server Software Component: Web Shell

BackdoorDiplomacy has used web shells to establish an initial foothold and for lateral movement within a victim's system.[1]

Enterprise T1049 System Network Connections Discovery

BackdoorDiplomacy has used NetCat and PortQry to enumerate network connections and display the status of related TCP and UDP ports.[1]
