Techniques Used

| **Domain** | **ID** | | **Name** | **Use** |
| --- | --- | --- | --- | --- |
| Enterprise | [T1074](https://attack.mitre.org/techniques/T1074) | [.001](https://attack.mitre.org/techniques/T1074/001) | [Data Staged](https://attack.mitre.org/techniques/T1074): [Local Data Staging](https://attack.mitre.org/techniques/T1074/001) | [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) has copied files of interest to the main drive's recycle bin.[[1]](https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/) |
| Enterprise | [T1190](https://attack.mitre.org/techniques/T1190) | | [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190) | [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) has exploited CVE-2020-5902, an F5 BIP-IP vulnerability, to drop a Linux backdoor. [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) has also exploited mis-configured Plesk servers.[[1]](https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/) |
| Enterprise | [T1574](https://attack.mitre.org/techniques/T1574) | [.001](https://attack.mitre.org/techniques/T1574/001) | [Hijack Execution Flow](https://attack.mitre.org/techniques/T1574): [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1574/001) | [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) has executed DLL search order hijacking.[[1]](https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/) |
| Enterprise | [T1105](https://attack.mitre.org/techniques/T1105) | | [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) | [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) has downloaded additional files and tools onto a compromised host.[[1]](https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/) |
| Enterprise | [T1036](https://attack.mitre.org/techniques/T1036) | [.004](https://attack.mitre.org/techniques/T1036/004) | [Masquerading](https://attack.mitre.org/techniques/T1036): [Masquerade Task or Service](https://attack.mitre.org/techniques/T1036/004) | [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) has disguised their backdoor droppers with naming conventions designed to blend into normal operations.[[1]](https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/) |
|  |  | [.005](https://attack.mitre.org/techniques/T1036/005) | [Masquerading](https://attack.mitre.org/techniques/T1036): [Match Legitimate Name or Location](https://attack.mitre.org/techniques/T1036/005) | [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) has dropped implants in folders named for legitimate software.[[1]](https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/) |
| Enterprise | [T1046](https://attack.mitre.org/techniques/T1046) | | [Network Service Discovery](https://attack.mitre.org/techniques/T1046) | [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) has used SMBTouch, a vulnerability scanner, to determine whether a target is vulnerable to EternalBlue malware.[[1]](https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/) |
| Enterprise | [T1095](https://attack.mitre.org/techniques/T1095) | | [Non-Application Layer Protocol](https://attack.mitre.org/techniques/T1095) | [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) has used EarthWorm for network tunneling with a SOCKS5 server and port transfer functionalities.[[1]](https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/) |
| Enterprise | [T1027](https://attack.mitre.org/techniques/T1027) | | [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) | [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) has obfuscated tools and malware it uses with VMProtect.[[1]](https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/) |
| Enterprise | [T1588](https://attack.mitre.org/techniques/T1588) | [.001](https://attack.mitre.org/techniques/T1588/001) | [Obtain Capabilities](https://attack.mitre.org/techniques/T1588): [Malware](https://attack.mitre.org/techniques/T1588/001) | [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) has obtained and used leaked malware, including DoublePulsar, EternalBlue, EternalRocks, and EternalSynergy, in its operations.[[1]](https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/) |
|  |  | [.002](https://attack.mitre.org/techniques/T1588/002) | [Obtain Capabilities](https://attack.mitre.org/techniques/T1588): [Tool](https://attack.mitre.org/techniques/T1588/002) | [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) has obtained a variety of open-source reconnaissance and red team tools for discovery and lateral movement.[[1]](https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/) |
| Enterprise | [T1120](https://attack.mitre.org/techniques/T1120) | | [Peripheral Device Discovery](https://attack.mitre.org/techniques/T1120) | [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) has used an executable to detect removable media, such as USB flash drives.[[1]](https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/) |
| Enterprise | [T1055](https://attack.mitre.org/techniques/T1055) | [.001](https://attack.mitre.org/techniques/T1055/001) | [Process Injection](https://attack.mitre.org/techniques/T1055): [Dynamic-link Library Injection](https://attack.mitre.org/techniques/T1055/001) | [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) has dropped legitimate software onto a compromised host and used it to execute malicious DLLs.[[1]](https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/) |
| Enterprise | [T1505](https://attack.mitre.org/techniques/T1505) | [.003](https://attack.mitre.org/techniques/T1505/003) | [Server Software Component](https://attack.mitre.org/techniques/T1505): [Web Shell](https://attack.mitre.org/techniques/T1505/003) | [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) has used web shells to establish an initial foothold and for lateral movement within a victim's system.[[1]](https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/) |
| Enterprise | [T1049](https://attack.mitre.org/techniques/T1049) | | [System Network Connections Discovery](https://attack.mitre.org/techniques/T1049) | [BackdoorDiplomacy](https://attack.mitre.org/groups/G0135) has used NetCat and PortQry to enumerate network connections and display the status of related TCP and UDP ports.[[1]](https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/) |