Blue Mockingbird, Group G0108 | MITRE ATT&CK®

Archived: 2026-04-05 14:35:49 UTC

Enterprise T1134 Access Token Manipulation

Blue Mockingbird has used JuicyPotato to abuse the `SeImpersonate` token privilege to escalate from web application pool accounts to NT Authority\SYSTEM.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Blue Mockingbird has used PowerShell reverse TCP shells to issue interactive commands over a network connection.[1]

.003 Command and Scripting Interpreter: Windows Command Shell

Blue Mockingbird has used batch script files to automate execution and deployment of payloads.[1]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

Blue Mockingbird has made their XMRIG payloads persistent as a Windows Service.[1]

Enterprise T1546 .003 Event Triggered Execution: Windows Management Instrumentation Event Subscription

Blue Mockingbird has used mofcomp.exe to establish WMI Event Subscription persistence mechanisms configured from a *.mof file.[1]

Enterprise T1190 Exploit Public-Facing Application

Blue Mockingbird has gained initial access by exploiting CVE-2019-18935, a vulnerability within Telerik UI for ASP.NET AJAX.[1]

Enterprise T1574 .012 Hijack Execution Flow: COR_PROFILER

Blue Mockingbird has used wmic.exe and Windows Registry modifications to set the COR_PROFILER environment variable to execute a malicious DLL whenever a process loads the .NET CLR.[1]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

Blue Mockingbird has masqueraded their XMRIG payload name by naming it wercplsupporte.dll after the legitimate wercplsupport.dll file.[1]

Enterprise T1112 Modify Registry

Blue Mockingbird has used Windows Registry modifications to specify a DLL payload.[1]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

Blue Mockingbird has obfuscated the wallet address in the payload binary.[1]

Enterprise T1588 .002 Obtain Capabilities: Tool

Blue Mockingbird has obtained and used tools such as Mimikatz.[1]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

Blue Mockingbird has used Mimikatz to retrieve credentials from LSASS memory.[1]

Enterprise T1090 Proxy

Blue Mockingbird has used FRP, ssf, and Venom to establish SOCKS proxy connections.[1]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

Blue Mockingbird has used Remote Desktop to log on to servers interactively and manually copy files to remote hosts.[1]

.002 Remote Services: SMB/Windows Admin Shares

Blue Mockingbird has used Windows Explorer to manually copy malicious files to remote hosts over SMB.[1]

Enterprise T1496 .001 Resource Hijacking: Compute Hijacking

Blue Mockingbird has used XMRIG to mine cryptocurrency on victim systems.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Blue Mockingbird has used Windows Scheduled Tasks to establish persistence on local and remote hosts.[1]

Enterprise T1218 .010 System Binary Proxy Execution: Regsvr32

Blue Mockingbird has executed custom-compiled XMRIG miner DLLs using regsvr32.exe.[1]

.011 System Binary Proxy Execution: Rundll32

Blue Mockingbird has executed custom-compiled XMRIG miner DLLs using rundll32.exe.[1]

Enterprise T1082 System Information Discovery

Blue Mockingbird has collected hardware details for the victim's system, including CPU and memory information.[1]

Enterprise T1569 .002 System Services: Service Execution

Blue Mockingbird has executed custom-compiled XMRIG miner DLLs by configuring them to execute via the "wercplsupport" service.[1]

Enterprise T1047 Windows Management Instrumentation

Blue Mockingbird has used wmic.exe to set environment variables.[1]
