RedDelta Modified PlugX Infection Chain Operations, Campaign C0047

Archived: 2026-04-05 17:15:08 UTC

Enterprise T1583 .001 Acquire Infrastructure: Domains

Mustang Panda registered adversary-controlled domains during RedDelta Modified PlugX Infection Chain Operations that were re-registrations of expired domains.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Mustang Panda used HTTP POST messages for command and control from PlugX installations during RedDelta Modified PlugX Infection Chain Operations.[1]

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

Mustang Panda used Run registry keys with names such as `OneNote Update` to execute legitimate executables that would load through search-order hijacking malicious DLLS to ensure persistence during RedDelta Modified PlugX Infection Chain Operations.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Mustang Panda used LNK files to execute PowerShell commands leading to eventual PlugX installation during RedDelta Modified PlugX Infection Chain Operations.[1]

Enterprise T1480 Execution Guardrails

Mustang Panda included the use of Cloudflare geofencing mechanisms to limit payload download activity during RedDelta Modified PlugX Infection Chain Operations.[1]

Enterprise T1203 Exploitation for Client Execution

Mustang Panda used the GrimResource exploitation technique via specially crafted MSC files for arbitrary code execution during RedDelta Modified PlugX Infection Chain Operations.[1]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

Mustang Panda stored encrypted payloads associated with PlugX installation in hidden directories during RedDelta Modified PlugX Infection Chain Operations.[1]

Enterprise T1574 .001 Hijack Execution Flow: DLL

Mustang Panda used DLL search order hijacking on vulnerable applications to install PlugX payloads during RedDelta Modified PlugX Infection Chain Operations.[1]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

Mustang Panda masqueraded Registry run keys as legitimate-looking service names such as `OneNote Update` during RedDelta Modified PlugX Infection Chain Operations.[1]

Enterprise T1095 Non-Application Layer Protocol

Mustang Panda communicated over TCP 5000 from adversary administrative servers to adversary command and control nodes during RedDelta Modified PlugX Infection Chain Operations.[1]

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

Mustang Panda stored installation payloads as encrypted files in hidden folders during RedDelta Modified PlugX Infection Chain Operations.[1]

Enterprise T1588 .004 Obtain Capabilities: Digital Certificates

Mustang Panda acquired Cloudflare Origin CA TLS certificates during RedDelta Modified PlugX Infection Chain Operations.[1]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Mustang Panda leveraged malicious attachments in spearphishing emails for initial access to victim environments in RedDelta Modified PlugX Infection Chain Operations.[1]

.002 Phishing: Spearphishing Link

Mustang Panda distributed malicious links in phishing emails leading to HTML files that would direct the victim to malicious MSC files if running Windows based on User Agent fingerprinting during RedDelta Modified PlugX Infection Chain Operations.[1]

Enterprise T1090 Proxy

Mustang Panda proxied communication through the Cloudflare CDN service during RedDelta Modified PlugX Infection Chain Operations.[1]

Enterprise T1608 .001 Stage Capabilities: Upload Malware

Mustang Panda staged malware on adversary-controlled domains and cloud storage instances during RedDelta Modified PlugX Infection Chain Operations.[1]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

Mustang Panda used legitimate, signed binaries such as `inkform.exe` or `ExcelRepairToolboxLauncher.exe` for follow-on execution of malicious DLLs through DLL search order hijacking in RedDelta Modified PlugX Infection Chain Operations.[1]

Enterprise T1218 .007 System Binary Proxy Execution: Msiexec

Mustang Panda initial payloads downloaded a Windows Installer MSI file that in turn dropped follow-on files leading to installation of PlugX during RedDelta Modified PlugX Infection Chain Operations.[1]

.014 System Binary Proxy Execution: MMC

Mustang Panda used Microsoft Management Console Snap-In Control files, or MSC files, executed via MMC to run follow-on PowerShell commands during RedDelta Modified PlugX Infection Chain Operations.[1]

Enterprise T1082 System Information Discovery

Mustang Panda captured victim operating system type via User Agent analysis during RedDelta Modified PlugX Infection Chain Operations.[1]

Enterprise T1204 .001 User Execution: Malicious Link

Mustang Panda distributed hyperlinks that would result in an MSC file running a PowerShell command to download and install a remotely-hosted MSI file during RedDelta Modified PlugX Infection Chain Operations.[1]

.002 User Execution: Malicious File

Mustang Panda distributed malicious LNK objects for user execution during RedDelta Modified PlugX Infection Chain Operations.[1]
