# C0021, Campaign C0021 | MITRE ATT&CK®

Archived: 2026-04-05 15:25:02 UTC

Enterprise T1583 .001 Acquire Infrastructure: Domains

For C0021, the threat actors registered domains for use in C2.[2]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

During C0021, the threat actors used HTTP for some of their C2 communications.[2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

During C0021, the threat actors used obfuscated PowerShell to extract an encoded payload from within an .LNK file.[2][1]

Enterprise T1584 .001 Compromise Infrastructure: Domains

For C0021, the threat actors used legitimate but compromised domains to host malicious payloads.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

During C0021, the threat actors deobfuscated encoded PowerShell commands including use of the specific string `'FromBase'+0x40+'String'`, in place of `FromBase64String` which is normally used to decode base64.[2][1]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

During C0021, the threat actors used SSL via TCP port 443 for C2 communications.[2]

Enterprise T1105 Ingress Tool Transfer

During C0021, the threat actors downloaded additional tools and files onto victim machines.[1][2]

Enterprise T1095 Non-Application Layer Protocol

During C0021, the threat actors used TCP for some C2 communications.[2]

Enterprise T1027 .009 Obfuscated Files or Information: Embedded Payloads

For C0021, the threat actors embedded a base64-encoded payload within a LNK file.[1]

.010 Obfuscated Files or Information: Command Obfuscation

During C0021, the threat actors used encoded PowerShell commands.[2][1]

Enterprise T1588 .002 Obtain Capabilities: Tool

For C0021, the threat actors used Cobalt Strike configured with a modified variation of the publicly available Pandora Malleable C2 Profile.[2][1]

Enterprise T1566 .002 Phishing: Spearphishing Link

During C0021, the threat actors sent phishing emails with unique malicious links, likely for tracking victim clicks.[2][1]

Enterprise T1608 .001 Stage Capabilities: Upload Malware

For C0021, the threat actors uploaded malware to websites under their control.[2][1]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

During C0021, the threat actors used `rundll32.exe` to execute the Cobalt Strike Beacon loader DLL.[2]

Enterprise T1204 .001 User Execution: Malicious Link

During C0021, the threat actors lured users into clicking a malicious link which led to the download of a ZIP archive containing a malicious .LNK file.[2]

---