Operation Spalax, Campaign C0005 | MITRE ATT&CK®

Archived: 2026-04-05 16:01:00 UTC

Enterprise T1583 .001 Acquire Infrastructure: Domains

For Operation Spalax, the threat actors registered hundreds of domains using Duck DNS and DNS Exit.[1]

Enterprise T1059 Command and Scripting Interpreter

For Operation Spalax, the threat actors used Nullsoft Scriptable Install System (NSIS) scripts to install malware.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

For Operation Spalax, the threat actors used a variety of packers and droppers to decrypt malicious payloads.[1]

Enterprise T1568 Dynamic Resolution

For Operation Spalax, the threat actors used dynamic DNS services, including Duck DNS and DNS Exit, as part of their C2 infrastructure.[1]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

For Operation Spalax, the threat actors used a variety of packers, including CyaX, to obfuscate malicious executables.[1]

.003 Obfuscated Files or Information: Steganography

For Operation Spalax, the threat actors used packers that read pixel data from images contained in PE files' resource sections and build the next layer of execution from the data.[1]

.013 Obfuscated Files or Information: Encrypted/Encoded File

For Operation Spalax, the threat actors used XOR-encrypted payloads.[1]

Enterprise T1588 .001 Obtain Capabilities: Malware

For Operation Spalax, the threat actors obtained malware, including Remcos, njRAT, and AsyncRAT.[1]

.002 Obtain Capabilities: Tool

For Operation Spalax, the threat actors obtained packers such as CyaX.[1]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

During Operation Spalax, the threat actors sent phishing emails that included a PDF document that in some cases led to the download and execution of malware.[1]

.002 Phishing: Spearphishing Link

During Operation Spalax, the threat actors sent phishing emails to victims that contained a malicious link.[1]

Enterprise T1608 .001 Stage Capabilities: Upload Malware

For Operation Spalax, the threat actors staged malware and malicious files in legitimate hosting services such as OneDrive or MediaFire.[1]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

During Operation Spalax, the threat actors used `rundll32.exe` to execute malicious installers.[1]

Enterprise T1204 .001 User Execution: Malicious Link

During Operation Spalax, the threat actors relied on a victim to click on a malicious link distributed via phishing emails.[1]

.002 User Execution: Malicious File

During Operation Spalax, the threat actors relied on a victim to open a PDF document and click on an embedded malicious link to download malware.[1]

Enterprise T1497 Virtualization/Sandbox Evasion

During Operation Spalax, the threat actors used droppers that would run anti-analysis checks before executing malware on a compromised host.[1]

Enterprise T1102 Web Service

During Operation Spalax, the threat actors used OneDrive and MediaFire to host payloads.[1]
