C0018, Campaign C0018 | MITRE ATT&CK®

Archived: 2026-04-05 13:36:28 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

During C0018, the threat actors used HTTP for C2 communications.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

During C0018, the threat actors used encoded PowerShell scripts for execution.[2][1]

Enterprise T1486 Data Encrypted for Impact

During C0018, the threat actors used AvosLocker ransomware to encrypt files on the compromised network.[2][1]

Enterprise T1190 Exploit Public-Facing Application

During C0018, the threat actors exploited VMWare Horizon Unified Access Gateways that were vulnerable to several Log4Shell vulnerabilities, including CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, and CVE-2021-44832.[2]

Enterprise T1105 Ingress Tool Transfer

During C0018, the threat actors downloaded additional tools, such as Mimikatz and Sliver, as well as Cobalt Strike and AvosLocker ransomware onto the victim network.[2][1]

Enterprise T1570 Lateral Tool Transfer

During C0018, the threat actors transferred the SoftPerfect Network Scanner and other tools to machines in the network using AnyDesk and PDQ Deploy.[2][1]

Enterprise T1036 Masquerading

During C0018, AvosLocker was disguised using the victim company name as the filename.[2]

.005 Match Legitimate Resource Name or Location

For C0018, the threat actors renamed a Sliver payload to `vmware_kb.exe`.[2]

Enterprise T1046 Network Service Discovery

During C0018, the threat actors used the SoftPerfect Network Scanner for network scanning.[2]

Enterprise T1571 Non-Standard Port

During C0018, the threat actors opened a variety of ports, including ports 28035, 32467, 41578, and 46892, to establish RDP connections.[1]

Enterprise T1027 .010 Obfuscated Files or Information: Command Obfuscation

During C0018, the threat actors used Base64 to encode their PowerShell scripts.[2][1]

Enterprise T1588 .002 Obtain Capabilities: Tool

For C0018, the threat actors acquired a variety of open source tools, including Mimikatz, Sliver, SoftPerfect Network Scanner, AnyDesk, and PDQ Deploy.[2][1]

Enterprise T1219 .002 Remote Access Tools: Remote Desktop Software

During C0018, the threat actors used AnyDesk to transfer tools between systems.[2][1]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

During C0018, the threat actors opened a variety of ports to establish RDP connections, including ports 28035, 32467, 41578, and 46892.[1]

Enterprise T1072 Software Deployment Tools

During C0018, the threat actors used PDQ Deploy to move AvosLocker and tools across the network.[2]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

During C0018, the threat actors used `rundll32` to run Mimikatz.[1]

Enterprise T1016 System Network Configuration Discovery

During C0018, the threat actors ran `nslookup` and Advanced IP Scanner on the target network.[1]

Enterprise T1033 System Owner/User Discovery

During C0018, the threat actors collected `whoami` information via PowerShell scripts.[1]

Enterprise T1047 Windows Management Instrumentation

During C0018, the threat actors used WMIC to modify administrative settings on both a local and a remote host, likely as part of the first stages for their lateral movement; they also used WMI Provider Host (`wmiprvse.exe`) to execute a variety of encoded PowerShell scripts using the `DownloadString` method.[2][1]
