Tropic Trooper, Pirate Panda, KeyBoy, Group G0081

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

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Tropic Trooper has used HTTP in communication with the C2.[5][3]

.004 Application Layer Protocol: DNS

Tropic Trooper's backdoor has communicated to the C2 over the DNS protocol.[3]

Enterprise T1119 Automated Collection

Tropic Trooper has collected information automatically using the adversary's USBferry attack.[3]

Enterprise T1020 Automated Exfiltration

Tropic Trooper has used a copy function to automatically exfiltrate sensitive data from air-gapped systems using USB storage.[3]

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

Tropic Trooper has created shortcuts in the Startup folder to establish persistence.[5][3]

.004 Boot or Logon Autostart Execution: Winlogon Helper DLL

Tropic Trooper has created the Registry key `HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell` and sets the value to establish persistence.[2][3]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

Tropic Trooper has used Windows command scripts.[3]

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

Tropic Trooper has installed a service pointing to a malicious DLL dropped to disk.[6]

Enterprise T1132 .001 Data Encoding: Standard Encoding

Tropic Trooper has used base64 encoding to hide command strings delivered from the C2.[3]

Enterprise T1140 Deobfuscate/Decode Files or Information

Tropic Trooper used shellcode with an XOR algorithm to decrypt a payload. Tropic Trooper also decrypted image files which contained a payload.[2][3]

Enterprise T1573 Encrypted Channel

Tropic Trooper has encrypted traffic with the C2 to prevent network detection.[3]

.002 Asymmetric Cryptography

Tropic Trooper has used SSL to connect to C2 servers.[1][3]

Enterprise T1052 .001 Exfiltration Over Physical Medium: Exfiltration over USB

Tropic Trooper has exfiltrated data using USB storage devices.[3]

Enterprise T1203 Exploitation for Client Execution

Tropic Trooper has executed commands through Microsoft security vulnerabilities, including CVE-2017-11882, CVE-2018-0802, and CVE-2012-0158.[1][2]

Enterprise T1083 File and Directory Discovery

Tropic Trooper has monitored files' modified time.[3]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

Tropic Trooper has created a hidden directory under `C:\ProgramData\Apple\Updates\` and `C:\Users\Public\Documents\Flash\`.[1][3]

Enterprise T1574 .001 Hijack Execution Flow: DLL

Tropic Trooper has been known to side-load DLLs using a valid version of a Windows Address Book and Windows Defender executable with one of their tools.[7][5]

Enterprise T1070 .004 Indicator Removal: File Deletion

Tropic Trooper has deleted dropper files on an infected system using command scripts.[3]

Enterprise T1105 Ingress Tool Transfer

Tropic Trooper has used a delivered trojan to download additional files.[3]

Enterprise T1680 Local Storage Discovery

Tropic Trooper has detected a target system’s system volume information.[8][3]

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

Tropic Trooper has hidden payloads in Flash directories and fake installer files.[3]

Enterprise T1106 Native API

Tropic Trooper has used multiple Windows APIs including HttpInitialize, HttpCreateHttpHandle, and HttpAddUrl.[3]

Enterprise T1046 Network Service Discovery

Tropic Trooper used `pr` and an openly available tool to scan for open ports on target systems.[8][3]

Enterprise T1135 Network Share Discovery

Tropic Trooper used `netview` to scan target systems for shared resources.[8]

Enterprise T1027 .003 Obfuscated Files or Information: Steganography

Tropic Trooper has used JPG files with encrypted payloads to mask their backdoor routines and evade detection.[3]

.013 Obfuscated Files or Information: Encrypted/Encoded File

Tropic Trooper has encrypted configuration files.[1][3]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Tropic Trooper sent spearphishing emails that contained malicious Microsoft Office and fake installer file attachments.[2][8][9][5][3]

Enterprise T1057 Process Discovery

Tropic Trooper is capable of enumerating the running processes on the system using `pslist`.[2][3]

Enterprise T1055 .001 Process Injection: Dynamic-link Library Injection

Tropic Trooper has injected a DLL backdoor into dllhost.exe and svchost.exe.[1][3]

Enterprise T1091 Replication Through Removable Media

Tropic Trooper has attempted to transfer USBferry from an infected USB device by copying an Autorun function to the target machine.[3]

Enterprise T1505 .003 Server Software Component: Web Shell

Tropic Trooper has started a web service in the target host and wait for the adversary to connect, acting as a web shell.[3]

Enterprise T1518 Software Discovery

Tropic Trooper's backdoor could list the infected system's installed software.[3]

.001 Security Software Discovery

Tropic Trooper can search for anti-virus software running on the system.[2]

Enterprise T1082 System Information Discovery

Tropic Trooper has detected a target system’s OS version.[8][3]

Enterprise T1016 System Network Configuration Discovery

Tropic Trooper has used scripts to collect the host's network topology.[3]

Enterprise T1049 System Network Connections Discovery

Tropic Trooper has tested if the localhost network is available and other connection capability on an infected system using command scripts.[3]

Enterprise T1033 System Owner/User Discovery

Tropic Trooper used `letmein` to scan for saved usernames on the target system.[8]

Enterprise T1221 Template Injection

Tropic Trooper delivered malicious documents with the XLSX extension, typically used by OpenXML documents, but the file itself was actually an OLE (XLS) document.[2]

Enterprise T1204 .002 User Execution: Malicious File

Tropic Trooper has lured victims into executing malware via malicious e-mail attachments.[5]

Enterprise T1078 .003 Valid Accounts: Local Accounts

Tropic Trooper has used known administrator account credentials to execute the backdoor directly.[3]
