Fox Kitten, UNC757, Parisite, Pioneer Kitten, RUBIDIUM, Lemon Sandstorm, Group G0117

Archived: 2026-04-05 16:35:48 UTC

Enterprise T1087 .001 Account Discovery: Local Account

Fox Kitten has accessed ntuser.dat and UserClass.dat on compromised hosts.[5]

.002 Account Discovery: Domain Account

Fox Kitten has used the Softerra LDAP browser to browse documentation on service accounts.[5]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

Fox Kitten has used 7-Zip to archive data.[5]

Enterprise T1217 Browser Information Discovery

Fox Kitten has used Google Chrome bookmarks to identify internal resources and assets.[5]

Enterprise T1110 Brute Force

Fox Kitten has brute forced RDP credentials.[4]

Enterprise T1059 Command and Scripting Interpreter

Fox Kitten has used a Perl reverse shell to communicate with C2.[4]

.001 PowerShell

Fox Kitten has used PowerShell scripts to access credential data.[5]

.003 Windows Command Shell

Fox Kitten has used cmd.exe likely as a password changing mechanism.[5]

Enterprise T1136 .001 Create Account: Local Account

Fox Kitten has created a local user account with administrator privileges.[4]

Enterprise T1555 .005 Credentials from Password Stores: Password Managers

Fox Kitten has used scripts to access credential information from the KeePass database.[5]

Enterprise T1530 Data from Cloud Storage

Fox Kitten has obtained files from the victim's cloud storage instances.[5]

Enterprise T1213 .005 Data from Information Repositories: Messaging Applications

Fox Kitten has accessed victim security and IT environments and Microsoft Teams to mine valuable information.[5]

Enterprise T1005 Data from Local System

Fox Kitten has searched local system resources to access sensitive documents.[5]

Enterprise T1039 Data from Network Shared Drive

Fox Kitten has searched network shares to access sensitive documents.[5]

Enterprise T1585 Establish Accounts

Fox Kitten has created KeyBase accounts to communicate with ransomware victims.[4][7]

.001 Social Media Accounts

Fox Kitten has used a Twitter account to communicate with ransomware victims.[4]

Enterprise T1546 .008 Event Triggered Execution: Accessibility Features

Fox Kitten has used sticky keys to launch a command prompt.[5]

Enterprise T1190 Exploit Public-Facing Application

Fox Kitten has exploited known vulnerabilities in Fortinet, PulseSecure, and Palo Alto VPN appliances.[1][3][2][5][4]

Enterprise T1210 Exploitation of Remote Services

Fox Kitten has exploited known vulnerabilities in remote services including RDP.[1][2][4]

Enterprise T1083 File and Directory Discovery

Fox Kitten has used WizTree to obtain network files and directory listings.[5]

Enterprise T1105 Ingress Tool Transfer

Fox Kitten has downloaded additional tools including PsExec directly to endpoints.[5]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

Fox Kitten has named the task for a reverse proxy lpupdate to appear legitimate.[5]

.005 Masquerading: Match Legitimate Resource Name or Location

Fox Kitten has named binaries and configuration files svhost and dllhost respectively to appear legitimate.[5]

Enterprise T1046 Network Service Discovery

Fox Kitten has used tools including NMAP to conduct broad scanning to identify open ports.[5][4]

Enterprise T1027 .010 Obfuscated Files or Information: Command Obfuscation

Fox Kitten has base64 encoded scripts to avoid detection.[5]

.013 Obfuscated Files or Information: Encrypted/Encoded File

Fox Kitten has base64 encoded payloads to avoid detection.[5]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

Fox Kitten has used prodump to dump credentials from LSASS.[5]

.003 OS Credential Dumping: NTDS

Fox Kitten has used Volume Shadow Copy to access credential information from NTDS.[5]

Enterprise T1572 Protocol Tunneling

Fox Kitten has used protocol tunneling for communication and RDP activity on compromised hosts through the use of open source tools such as ngrok and custom tool SSHMinion.[2][5][4]

Enterprise T1090 Proxy

Fox Kitten has used the open source reverse proxy tools including FRPC and Go Proxy to establish connections from C2 to local servers.[5][4][7]

Enterprise T1012 Query Registry

Fox Kitten has accessed Registry hives ntuser.dat and UserClass.dat.[5]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

Fox Kitten has used RDP to log in and move laterally in the target environment.[5][4]

.002 Remote Services: SMB/Windows Admin Shares

Fox Kitten has used valid accounts to access SMB shares.[5]

.004 Remote Services: SSH

Fox Kitten has used the PuTTY and Plink tools for lateral movement.[5]

.005 Remote Services: VNC

Fox Kitten has installed TightVNC server and client on compromised servers and endpoints for lateral movement.[5]

Enterprise T1018 Remote System Discovery

Fox Kitten has used Angry IP Scanner to detect remote systems.[5]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Fox Kitten has used Scheduled Tasks for persistence and to load and execute a reverse proxy binary.[5][4]

Enterprise T1505 .003 Server Software Component: Web Shell

Fox Kitten has installed web shells on compromised hosts to maintain access.[5][4]

Enterprise T1552 .001 Unsecured Credentials: Credentials In Files

Fox Kitten has accessed files to gain valid credentials.[5]

Enterprise T1078 Valid Accounts

Fox Kitten has used valid credentials with various services during lateral movement.[5]

Enterprise T1102 Web Service

Fox Kitten has used Amazon Web Services to host C2.[4]
