PROMETHIUM, StrongPity, Group G0056 | MITRE ATT&CK®

Archived: 2026-04-05 18:34:56 UTC

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

PROMETHIUM has used Registry run keys to establish persistence.[3]

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

PROMETHIUM has created new services and modified existing services for persistence.[4]

Enterprise T1587 .002 Develop Capabilities: Code Signing Certificates

PROMETHIUM has created self-signed certificates to sign malicious installers.[4]

.003 Develop Capabilities: Digital Certificates

PROMETHIUM has created self-signed digital certificates for use in HTTPS C2 traffic.[3]

Enterprise T1189 Drive-by Compromise

PROMETHIUM has used watering hole attacks to deliver malicious versions of legitimate installers.[4]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

PROMETHIUM has named services to appear legitimate.[3][4]

.005 Masquerading: Match Legitimate Resource Name or Location

PROMETHIUM has disguised malicious installer files by bundling them with legitimate software installers.[3][4]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

PROMETHIUM has signed code with self-signed certificates.[4]

Enterprise T1205 .001 Traffic Signaling: Port Knocking

PROMETHIUM has used a script that configures the knockd service and firewall to only accept C2 connections from systems that use a specified sequence of knock ports.[4]

Enterprise T1204 .002 User Execution: Malicious File

PROMETHIUM has attempted to get users to execute compromised installation files for legitimate software including compression applications, security software, browsers, file recovery applications, and other tools and utilities.[3][4]

Enterprise T1078 .003 Valid Accounts: Local Accounts

PROMETHIUM has created admin accounts on a compromised host.[4]

Mobile T1517 Access Notifications

During C0033, PROMETHIUM used StrongPity to collect message notifications from 17 applications.[6]

Mobile T1437 .001 Application Layer Protocol: Web Protocols

During C0033, PROMETHIUM used StrongPity to communicate with the C2 server using HTTPS.[6]

Mobile T1532 Archive Collected Data

During C0033, PROMETHIUM used StrongPity to exfiltrate encrypted data to the C2 server.[6]

Mobile T1429 Audio Capture

During C0033, PROMETHIUM used StrongPity to record phone calls.[6]

Mobile T1456 Drive-By Compromise

During C0033, PROMETHIUM distributed StrongPity through the compromised official Syrian E-Gov website.[7]

Mobile T1521 .001 Encrypted Channel: Symmetric Cryptography

During C0033, PROMETHIUM used StrongPity to encrypt C2 communication using AES.[6]

Mobile T1624 .001 Event Triggered Execution: Broadcast Receivers

During C0033, PROMETHIUM used StrongPity to receive the following broadcast events to establish persistence: `BOOT_COMPLETED`, `BATTERY_LOW`, `USER_PRESENT`, `SCREEN_ON`, `SCREEN_OFF`, or `CONNECTIVITY_CHANGE`.[6]

Mobile T1646 Exfiltration Over C2 Channel

During C0033, PROMETHIUM used StrongPity to exfiltrate to the C2 server using HTTPS.[6][7]

Mobile T1420 File and Directory Discovery

During C0033, PROMETHIUM used StrongPity to collect file lists on the victim device.[6]

Mobile T1629 .003 Impair Defenses: Disable or Modify Tools

During C0033, PROMETHIUM used StrongPity to modify permissions on a rooted device and tried to disable the SecurityLogAgent application.[6]

Mobile T1544 Ingress Tool Transfer

During C0033, PROMETHIUM used StrongPity to receive files from the C2 and execute them via the parent application.[6]

Mobile T1430 Location Tracking

During C0033, PROMETHIUM used StrongPity to access the device's location.[6]

Mobile T1655 .001 Masquerading: Match Legitimate Name or Location

During C0033, PROMETHIUM used StrongPity on a compromised website to distribute a malicious version of a legitimate application.[7]

Mobile T1406 Obfuscated Files or Information

During C0033, PROMETHIUM used StrongPity to obfuscate code and strings to evade detection.[6]

Mobile T1636 .002 Protected User Data: Call Log

During C0033, PROMETHIUM used StrongPity to collect call logs.[6]

.003 Protected User Data: Contact List

During C0033, PROMETHIUM used StrongPity to collect the device's contact list.[6]

.004 Protected User Data: SMS Messages

During C0033, PROMETHIUM used StrongPity to collect SMS messages.[6]

Mobile T1418 Software Discovery

During C0033, PROMETHIUM used StrongPity to obtain a list of installed applications.[6]

Mobile T1426 System Information Discovery

During C0033, PROMETHIUM used StrongPity to collect the device's information, such as SIM serial number, SIM serial number, etc.[6]

Mobile T1421 System Network Connections Discovery

During C0033, PROMETHIUM used StrongPity to collect information regarding available Wi-Fi networks.[7]
