HUNTER — Iranian Threat Actor Coverage

Following our initial threat hunting initiative and in response to ongoing regional developments, our team has expanded coverage to include additional Iranian state-aligned threat actors, as well as new and updated tactics, techniques, and procedures (TTPs). This expansion reflects continued analysis and intelligence review, resulting in refinements to existing Hunt Packages and the development of new hypotheses to address evolving adversary behavior.

The newly developed Hunt Packages will be made available in the Hunter platform as soon as possible and will be accessible through the existing threat actor search links and filters. Together, these updates are designed to capture emerging behavioral patterns and enhance coverage across multiple stages of adversary operations.

MANGO SANDSTORM

(MuddyWater, Static Kitten, TEMP.Zagros, TA450)

- Hiding Files and Directories
- Mock Trusted Directories for DLL Sideloading
- Potentially Injected Process Command Execution
- Prohibited Applications Spawning cmd.exe or powershell.exe
- Potential DLL Sideloading Utilizing DAT File
- Obfuscated PowerShell Execution String — Potential Malware Execution
- CURL/WGET Download and Execute — Potential Payload Download Followed by Execution
- Microsoft Office Parent of Suspicious LOLB
- DLL and EXE File Written in Same Directory in Short Period — Potential DLL Write for DLL Side Loading
- Powershell Encoded Command Execution
- Titan Reporting
  - https://titan.intel471.com/report/inforep/805ebbf60a526fe8d94fccf15b7ed01f

- https://titan.intel471.com/report/geopol/intelligence_bulletin/0aaa86e3b974379849a42d069869d551
- https://titan.intel471.com/report/geopol/threat_brief/ca78bffa401da3b12b7297fd6ed5e378
- https://titan.intel471.com/report/fintel/660167cd88d8249928c27e24f7a43dd9

HAZEL SANDSTORM

(OilRig, Helix Kitten, APT34, TA452, Evasive Serpens, Cobalt Gypsy)

- Powershell Aliasing — Potential Detection Bypass — ScriptBlock
- Powershell Aliasing — Potential Detection Bypass
- MsiExec Executing MSI File From Zip — Potential Malware Execution
- Certutil.exe Encoding/Decoding Flags — Attempt to Encode or Decode Data/Files
- WMIC Windows Internal Discovery and Enumeration
- CURL/WGET Download and Execute — Potential Payload Download Followed by Execution
- Multiple DNS Queries Originating from the Same Source Port — Potential DNS Tunneling
- Excessive Volume of Unique DNS Queries — Potential DNS Tunneling
- Scheduled Task Created
- Titan Reporting
  - https://titan.intel471.com/report/geopol/profile_report/b74a9869f4387baf67c56aee-a0ff586d
  - https://titan.intel471.com/report/geopol/intelligence_summary/2666d1244bc-08d75ac7378cdea50034f
  - https://titan.intel471.com/report/geopol/threat_brief/339e3ee6fe5f11c-ca172d824d6261d41
  - https://titan.intel471.com/report/geopol/intelligence_bulletin/0aaa86e-3b974379849a42d069869d551
  - https://titan.intel471.com/report/geopol/threat_brief/ca78bffa401da3b12b7297fd-6ed5e378
  - https://titan.intel471.com/report/inforep/ed6abd2a0b6481ab703ca99be5fb911d

LEMON SANDSTORM

(Pioneer Kitten, Parasite, UNC757)

- Generic Web Directory Traversal
- Citrix ADC (Netscaler) Path Traversal Exploit (CVE-2019-19781)
- Uniquely Named Driver Writes With FileNames Between 4 – 10 Characters
- File Created in Driver Directory Followed by Service Creation — Potential Malware Installation

- CURL/WGET Activity associated with IP Geolocation Services
- Remote Interactive Connections from Unexpected Locations
- Potential Ngrok Tunnel for Exfiltration — Command Line
- Usage of chmod to Enable Execution — Potential Payload Staging
- Titan Reporting
  - https://titan.intel471.com/report/geopol/intelligence_summary/2666d1244bc-08d75ac7378cdea50034f

MINT SANDSTORM

(Charming Kitten, APT35, TA453, Newscaster, APT42)

- Windows Defender Tampering - Possible Malware Activity
- WScript Executing VBS From Temp Folder Locations - Potential Malware
- Methods for Downloading Files with PowerShell
- Powershell Encoded Command Execution
- Command Obfuscation Attempt — Use of Variable String Replacement
- CURL/WGET Download and Execute — Potential Payload Download Followed by Execution
- Titan Reporting
  - https://titan.intel471.com/report/geopol/threat_brief/339e3ee6fe5f11c-ca172d824d6261d41
  - https://titan.intel471.com/report/geopol/intelligence_summary/2666d1244bc-08d75ac7378cdea50034f
  - https://titan.intel471.com/report/geopol/threat_brief/4362811f13918d-40012ba9a2e8eae4c4
  - https://titan.intel471.com/report/geopol/intelligence_bulletin/0aaa86e-3b974379849a42d069869d551
  - https://titan.intel471.com/report/geopol/intelligence_summary/c72d63e28f1773339ef6b3916eff0a84
  - https://titan.intel471.com/report/geopol/threat_brief/ca78bffa401da3b12b7297fd-6ed5e378

COTTON SANDSTORM

(Haywire Kitten, Vice Leaker)

- Process Loading or Writing DLL in User Temp Directory — Potential Meterpreter Privilege Escalation
- TITAN Reporting
  - https://titan.intel471.com/report/geopol/threat_brief/2d5332f34bff0f200dbb-63841fc8a2c2

- https://titan.intel471.com/report/geopol/intelligence_summary/c3cb2ff-73fa91392284a7dbf070fcd6f
- https://titan.intel471.com/report/geopol/intelligence_bulletin/0aaa86e-3b974379849a42d069869d551

CRIMSON SANDSTORM

(Imperial Kitten, APT35, TA456, Tortoiseshell)

- WMIC Windows Internal Discovery and Enumeration
- Autorun or ASEP Registry Key Modification
- TITAN Reporting
  - https://titan.intel471.com/report/inforep/8de6790f70f0fb7d48cd494baa9100e7
  - https://titan.intel471.com/report/inforep/44c335c8302734c691f72f8825cdf1bc
  - https://titan.intel471.com/report/fintel/266fc945730e702422b9475cf137dbba

PINK SANDSTORM

(Spectral Kitten, BlackShadow, Agrius, Deadwood, SharpBoys, DEV-0022)

- Single Character Process On Endpoint
- Wevtutil Cleared Log
- Suspect Child Process to IIS Worker Process (w3wp.exe) - Potential Exploitation
- Attempted Credential Dump From Registry Via Reg.exe
- Single-Character Named Files Used for Execution
- Suspicious Scheduled Task Created - Execution Details Contains Scripting Reference
- TITAN Reporting
  - https://titan.intel471.com/report/inforep/8de6790f70f0fb7d48cd494baa9100e7
  - https://titan.intel471.com/report/geopol/intelligence_summary/5d98d493da6b-5c4ff527d73b6e046486
  - https://titan.intel471.com/report/inforep/ed00723cba39944010c808d8c4c26f43
  - https://titan.intel471.com/report/fintel/4066e610e26f185852d8a9574598e5a2
  - https://titan.intel471.com/report/breach_alert/b293e236b0c28fd62d88ed9fd-f0edd62

RED SANDSTORM

(Banished Kitten, Dune, Void Manticore, Storm-0842, DEV-0842)

- Ping Count Activity
- Suspicious bcdedit Activity - Potential Ransomware
- Shadow Copies Deletion Using Operating Systems Utilities
- TITAN Reporting

- https://titan.intel471.com/report/inforep/ed6abd2a0b6481ab703ca99be5fb911d
- https://titan.intel471.com/report/fintel/0f30801aa88f295adf4979134ad54bdd

MARIGOLD SANDSTORM

(Vengeful Kitten, Moses Staff, DEV-500)

- Masquerading Process Outside of Native Directory
- Executing SysWOW64 Directory Executables for Masquerading
- Environmentally Unique ASPX File Written to wwwroot Directory - Potential Webshell Installation
- Dump LSASS via comsvcs DLL
- Copying Files From Native Windows Directory for Masquerading
- Executing System32 Directory Executables for Masquerading
- TITAN Reporting
  - https://titan.intel471.com/report/geopol/intelligence_bulletin/0aaa86e-3b974379849a42d069869d551
  - https://titan.intel471.com/report/geopol/threat_brief/ca78bffa401da3b12b7297fd-6ed5e378
  - https://titan.intel471.com/report/fintel/4f64eea95d86249ca9f6a335fec23b25

BURGUNDY SANDSTORM

(Remix Kitten, APT39, Chafer)

- Double File Extension -—Potential Malware Execution
- Autorun or ASEP Registry Key Modification