INTRUVENT

COMPREHENSIVE THREAT HUNTING GUIDE

VPN Exploitation & Pre-Positioned Access Detection

Hunting for Lemon Sandstorm (Pioneer Kitten / Fox Kitten) in Enterprise VPN and Network Appliance Environments

Version 1.0
Published March 11, 2026
Trigger Event Operation Epic Fury / Iran Conflict Escalation
Classification TLP:CLEAR
Total Hunt Time 4–5 Hours
Target Sectors Energy, Water, Defense, Healthcare, Manufacturing

Intruvent Technologies
INT-THG-2026-LEMONSANDSTORM-VPN-v1.0

Table of Contents

Overview

Executive Summary 3
MITRE ATT&CK Mapping 4

Hunt Modules

Module 1: VPN Appliance Vulnerability Audit 5
Module 2: Pulse Secure / Ivanti Connect Secure Exploitation Detection 6
Module 3: Fortinet FortiOS Exploitation Detection 7
Module 4: Palo Alto PAN-OS and Check Point Exploitation Detection 8
Module 5: Web Shell Detection on Edge Devices 9
Module 6: Credential Harvesting and Lateral Movement 10
Module 7: Tunneling Tool Detection (Chisel, ngrok, ligolo) 11
Module 8: Known C2 Infrastructure Detection 12
Module 9: Ransomware Precursor Activity 13
Module 10: OT/ICS Network Boundary Monitoring 14

Appendices

Appendix A: Indicators of Compromise 15
Appendix B: Detection Rules 18
Appendix C: References 21

1 Executive Summary

AT A GLANCE

THREAT ACTOR
Lemon Sandstorm / Pioneer Kitten / Fox Kitten (Iran)

PRIMARY TARGETS
VPN Appliances, Network Gateways, Critical Infrastructure

TRIGGER EVENT
Operation Epic Fury (Feb 28, 2026)

TARGET SECTORS
Energy, Water, Defense, Healthcare, Manufacturing

PRIMARY TTP
T1190 Exploit Public-Facing Application (VPN/Firewall)

BUSINESS IMPACT
Pre-positioned ICS/SCADA access, ransomware, data theft

Lemon Sandstorm (tracked by CrowdStrike as **Pioneer Kitten**, by ClearSky as **Fox Kitten**, by Dragos as **Parisite**, and by Secureworks as **COBALT FOXGLOVE**) is an Iranian threat actor that has exploited VPN and network appliance vulnerabilities since at least 2017. According to a joint CISA/FBI/DC3 advisory (AA24-241A, August 2024), the group operates as both a state-sponsored access provider and a ransomware affiliate, partnering with ALPHV/BlackCat, NoEscape, and Ransomhouse to monetize compromised networks.

A Fortinet FortiGuard Incident Response investigation published in May 2025 documented a two-year intrusion (May 2023 to February 2025) into a Middle East critical national infrastructure entity. The group deployed eight custom malware tools, targeted the restricted OT network, and demonstrated the ability to maintain persistent access despite multiple containment attempts. Dragos confirmed this actor (as Parisite) hands off compromised IT access to the Pyroxene threat group for IT-to-OT traversal.

With the escalation of the Iran-US conflict following Operation Epic Fury on February 28, 2026, Lemon Sandstorm's pre-positioned access inside Western critical infrastructure represents an immediate threat. This guide provides **10 hunt modules** designed to detect VPN exploitation, web shell persistence, tunneling tools, C2 communications, ransomware precursors, and OT boundary exposure. Total estimated hunt time is **5.5 hours** (including analysis and documentation).

Threat Overview

Lemon Sandstorm has compromised over 200 organizations since 2017, with a pronounced focus on VPN infrastructure. CrowdStrike assesses the group as a "contract element operating in support of the Iranian government" rather than a direct government unit, explaining its dual espionage and monetization model. The group operates through the front company Danesh Novin Sahand (registration ID: 14007585836) and uses the online monikers "Br0k3r" and "xplfinder" for access brokering on underground forums (source: CISA AA24-241A).

The group's operational signature is rapid adoption of newly disclosed VPN vulnerabilities, sometimes integrating exploits within hours of public disclosure. Target vendors include Pulse Secure/Ivanti, Fortinet, Palo Alto Networks, Citrix, F5, and Check Point. After initial access, the group deploys web shells, creates local accounts with trailing dollar signs to evade enumeration, and establishes persistent tunneling through tools such as Ngrok, Ligolo, Chisel, and custom SSH utilities.

In February 2025, the group relaunched Pay2Key ransomware as "Pay2Key.I2P" on the I2P anonymity network, offering an 80% profit share for attacks against US and Israeli targets. According to Morphisec, the updated ransomware incorporates Mimic/ELENOR-Corp capabilities, and achieved 51+ ransom payouts in its first four months of operation.

KEY CHARACTERISTICS

- Iranian state-sponsored contractor
- VPN exploitation specialist (since 2017)
- 14 CVEs across 7 edge vendors
- 8+ custom malware families
- Ransomware affiliate (ALPHV, NoEscape)
- Pay2Key.I2P RaaS operator
- Access broker ("Br0k3r" persona)
- OT/ICS pre-positioning capability
- Parisite-Pyroxene handoff model
- Web shell persistence on appliances

2 MITRE ATT&CK Mapping

The following techniques have been observed in Lemon Sandstorm / Pioneer Kitten campaigns, sourced from MITRE ATT&CK G0117, CISA AA24-241A, CISA AA20-259A, and Fortinet FortiGuard IR (May 2025):

`T1190` PRIMARY
Exploit Public-Facing Application
Core technique: exploitation of VPN/firewall CVEs in Pulse Secure, Fortinet, Palo Alto, Citrix, F5, Check Point, and Ivanti products

`T1133`
External Remote Services
Compromised SSL VPN credentials used for persistent remote access to target networks

`T1505.003`
Web Shell
UpdateChecker.aspx, RecShell, DropShell, China Chopper, netscaler.php deployed on compromised appliances

`T1136.001`
Create Local Account
Accounts with trailing dollar signs (sqladmin$) and deceptive names (John McCain, IIS_Admin) for persistence

`T1572`
Protocol Tunneling
Ngrok, SSHMinion, Ligolo, Chisel, FRP, Plink used for outbound tunneling and proxy operations

`T1003.001`
LSASS Memory Credential Dumping
CredInterceptor and Mimikatz used to harvest credentials from LSASS process memory

`T1078`
Valid Accounts
Stolen VPN and domain credentials for initial and persistent access; "kharpedar" password pattern since 2017

`T1021.004`
Remote Services: SSH
PuTTY, Plink, SSHMinion for SSH-based lateral movement and tunneling

`T1219`
Remote Access Software
AnyDesk, MeshCentral Agent deployed for persistent remote access

`T1102`
Web Service
AWS-hosted C2; Google Docs for HXLibrary config retrieval; Discord for NeoExpressRAT C2

`T1657`
Financial Theft
Ransomware affiliate operations (ALPHV, NoEscape, Ransomhouse) and Pay2Key.I2P RaaS platform

`T1053.005`
Scheduled Task
SpaceAgentTaskMgrSHR and random eight-character service names for persistence

3 Hunt Modules

1 VPN Appliance Vulnerability Audit

Duration: 35 min Priority: CRITICAL

Objective: Inventory all VPN and network gateway appliances, identify unpatched instances vulnerable to CVEs exploited by Lemon Sandstorm, and prioritize remediation.

Background

Lemon Sandstorm's primary initial access vector is exploitation of VPN and network appliance vulnerabilities. According to CISA AA24-241A and ClearSky, the group has exploited 14 known CVEs across Pulse Secure/Ivanti, Fortinet, Palo Alto Networks, Citrix, F5, and Check Point products. Secureworks notes the group integrates new exploits within hours of public disclosure. The first step in any hunt is confirming your VPN infrastructure is patched against all known exploited vulnerabilities.

Prerequisites

- Complete asset inventory of all VPN concentrators, SSL VPN gateways, and firewall appliances
- Access to vulnerability management platform (Qualys, Tenable, Rapid7)
- Current firmware/software version documentation for each appliance

CVE Reference Table: Lemon Sandstorm Exploited Vulnerabilities

CVE	Product	Type	First Exploited	Source

`CVE-2019-11510`	Pulse Secure VPN	Arbitrary file read	2019	CISA AA20-259A
`CVE-2019-11539`	Pulse Secure VPN	Remote code execution	2019	CISA AA20-259A
`CVE-2024-21887`	Ivanti Connect Secure	Command injection	2024	CISA AA24-241A
`CVE-2018-13379`	Fortinet FortiOS SSL VPN	Path traversal	2019	ClearSky
`CVE-2019-1579`	Palo Alto GlobalProtect	Remote code execution	2019	ClearSky
`CVE-2024-3400`	Palo Alto PAN-OS	Command injection	April 2024	CISA AA24-241A
`CVE-2024-24919`	Check Point Security Gateways	Information disclosure	July 2024	CISA AA24-241A
`CVE-2019-19781`	Citrix ADC/NetScaler	Directory traversal / RCE	2019	CISA AA20-259A
`CVE-2023-3519`	Citrix NetScaler ADC	Remote code execution	2023	CISA AA24-241A
`CVE-2020-5902`	F5 BIG-IP	Remote code execution	2020	CISA AA20-259A
`CVE-2022-1388`	F5 BIG-IP	Authentication bypass / RCE	2022	CISA AA24-241A

Hunt Procedure: Vulnerability Scan Correlation

INVESTIGATION AID

KQL (MICROSOFT SENTINEL)

```
// Query vulnerability assessment data for Lemon Sandstorm-targeted CVEs
// Requires vulnerability assessment connector (Qualys, Tenable, etc.)
let LemonCVEs = dynamic([
    "CVE-2019-11510", "CVE-2019-11539", "CVE-2024-21887",
    "CVE-2018-13379", "CVE-2019-1579", "CVE-2024-3400",
    "CVE-2024-24919", "CVE-2019-19781", "CVE-2023-3519",
    "CVE-2020-5902", "CVE-2022-1388"
]);
DeviceTvmSoftwareVulnerabilities
| where CveId in (LemonCVEs)
| project DeviceName, CveId, SoftwareName, SoftwareVersion,
    VulnerabilitySeverityLevel
| sort by VulnerabilitySeverityLevel desc
```

☐ Verify all VPN appliances are running patched firmware versions that address the CVEs listed above

☐ Cross-reference vulnerability scan results against the CVE table; any unpatched instance requires emergency patching

☐ Check for end-of-life appliances that no longer receive security updates

☐ Confirm that vendor-recommended integrity checks have been run on all Pulse Secure/Ivanti and Citrix appliances

Critical Finding Indicator

Any unpatched VPN appliance running a version vulnerable to the CVEs above should be treated as potentially compromised. Patching alone is insufficient if exploitation already occurred; proceed to Modules 2-5 for post-exploitation indicators.

2 Pulse Secure/Ivanti Connect Secure Exploitation Hunt

Duration: 30 min Priority: **CRITICAL**

Objective: Detect indicators of Lemon Sandstorm exploitation on Pulse Secure and Ivanti Connect Secure appliances, including file artifacts, unauthorized admin sessions, and credential extraction.

Background

Pulse Secure / Ivanti Connect Secure VPNs have been a primary target for Lemon Sandstorm since 2019. CVE-2019-11510 allows unauthenticated arbitrary file reads, enabling extraction of plaintext credentials. CVE-2024-21887 enables command injection on Ivanti Connect Secure. CISA AA20-259A confirmed exploitation of both Pulse Secure CVEs, and Censys identified Ivanti Connect Secure instances in Fox Kitten infrastructure patterns.

Prerequisites

- SSH or console access to Pulse Secure / Ivanti Connect Secure appliance
- VPN authentication logs forwarded to SIEM
- CISA Integrity Checker Tool for Ivanti (if available)

Hunt Procedure: Detect CVE-2019-11510 Exploitation Artifacts

BLOCKING SAFE

BASH (PULSE SECURE APPLIANCE)

```
# Check web server logs for CVE-2019-11510 exploitation attempts
# Look for unauthenticated file read patterns
grep -E "dana-na.*\.\./\.\./\.\." /var/log/httpd/access_log
grep -E "/dana/html5acc/guacamole/" /var/log/httpd/access_log
# Check for credential file access
grep -E "/data/runtime/mtmp/lmdb/dataa/" /var/log/httpd/access_log
```

Hunt Procedure: Suspicious VPN Authentication Patterns

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect VPN authentication from known Lemon Sandstorm infrastructure ASNs
// AS14061 (DigitalOcean) and AS16509 (AWS) identified by Censys analysis
// WARNING: These ASNs serve millions of legitimate users. Alert only.
Syslog
| where SyslogMessage has_any ("PulseSecure", "Ivanti", "VPN")
| where SyslogMessage has "authentication"
| extend SourceIP = extract(@"(\d+\.\d+\.\d+\.\d+)", 1, SyslogMessage)
| where isnotempty(SourceIP)
| project TimeGenerated, SourceIP, SyslogMessage, Computer
| sort by TimeGenerated desc
```

Hunt Procedure: Ivanti Integrity Check

INVESTIGATION AID

BASH (IVANTI CONNECT SECURE APPLIANCE)

```
# Run CISA-recommended Integrity Checker Tool
# Download from: https://www.cisa.gov/ivanti-integrity-checker
# Verify no unauthorized files in web directories
find /home/webserver/ -name "*.php" -newer /etc/issue -ls
find /home/webserver/ -name "*.cgi" -newer /etc/issue -ls
# Check for unauthorized crontab entries
crontab -l
cat /etc/crontab
```

> **Critical Finding Indicator**
>
> Any unauthorized files in web-accessible directories, evidence of credential file access in logs, or unexplained administrator sessions warrant immediate escalation. Lemon Sandstorm commonly extracts VPN credentials within hours of initial exploitation.

3 Fortinet FortiOS Exploitation Detection

Duration: 30 min Priority: **CRITICAL**

Objective: Detect exploitation of Fortinet FortiOS SSL VPN vulnerabilities and identify post-exploitation artifacts consistent with Lemon Sandstorm tradecraft.

Background

CVE-2018-13379 allows unauthenticated attackers to download FortiOS system files, including plaintext VPN session credentials. ClearSky documented Lemon Sandstorm exploitation of this CVE as part of the original Fox Kitten campaign. The Fortinet FortiGuard IR report (May 2025) confirmed that the Middle East CNI intrusion began with compromised SSL VPN credentials, and the actors deployed phishing domains impersonating Fortinet (login.forticloud[.]online, fortigate.forticloud[.]online) for credential harvesting.

Prerequisites

- Access to FortiGate appliance CLI or FortiAnalyzer logs
- FortiOS version documentation for all FortiGate appliances
- DNS query logs or proxy logs for phishing domain detection

Hunt Procedure: CVE-2018-13379 Exploitation Artifacts

BLOCKING SAFE

BASH (FORTIGATE CLI)

```
# Check FortiGate logs for path traversal exploitation attempts
# CVE-2018-13379 targets /remote/fgt_lang?lang=../../
execute log filter category event
execute log filter field msg "lang" "fgt_lang"
execute log display
# Verify current FortiOS version is patched
get system status | grep Version
```

Hunt Procedure: Fortinet Phishing Domain Detection

BLOCKING SAFE

KQL (MICROSOFT SENTINEL)

```
// Detect DNS queries to known Lemon Sandstorm phishing domains
// Source: CISA Advisory AA24-241A (Aug 2024)
let PhishingDomains = dynamic([
    "login.forticloud.online", "fortigate.forticloud.online",
    "cloud.sophos.one"
]);
DnsEvents
| where Name has_any (PhishingDomains)
| project TimeGenerated, ClientIP, Name, QueryType
| sort by TimeGenerated desc
```

Hunt Procedure: Anomalous FortiGate Admin Sessions

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect FortiGate admin logins from unexpected sources
Syslog
| where SyslogMessage has "FortiGate" or SyslogMessage has "fortinet"
| where SyslogMessage has_any ("login", "admin", "authentication")
| where SyslogMessage has "success"
| project TimeGenerated, Computer, SyslogMessage
| sort by TimeGenerated desc
```

Fortinet Credential Harvesting

The phishing domains login.forticloud[.]online and fortigate.forticloud[.]online impersonate legitimate Fortinet services. If DNS queries to these domains are found, the targeted user's credentials should be considered compromised. Immediately reset the affected account and review all VPN sessions associated with those credentials.

4 PAN-OS and Check Point Gateway Exploitation Hunt

Duration: 25 min Priority: HIGH

Objective: Detect exploitation of Palo Alto Networks PAN-OS (CVE-2024-3400, CVE-2019-1579) and Check Point Security Gateways (CVE-2024-24919) by Lemon Sandstorm.

Background

CISA AA24-241A confirmed that Lemon Sandstorm conducted mass scanning for CVE-2024-3400 (PAN-OS command injection) in April 2024 and scanned for CVE-2024-24919 (Check Point information disclosure) in July 2024. CVE-2019-1579 (Palo Alto GlobalProtect RCE) has been in the group's arsenal since 2019 per ClearSky's Fox Kitten report. These are high-value targets because compromising a perimeter firewall provides broad network visibility and lateral movement opportunities.

Hunt Procedure: PAN-OS CVE-2024-3400 Exploitation Detection

DETECTION ONLY

BASH (PAN-OS CLI)

```
# Check for CVE-2024-3400 exploitation indicators
# Look for suspicious files in GlobalProtect directories
find /opt/panlogs/tmp/ -name "*.css" -exec ls -la {} \;
# Check running processes for unexpected shells
ps aux | grep -E "(sh|bash|python)" | grep -v grep
# Verify PAN-OS version is patched
show system info | match version
```

Hunt Procedure: Check Point CVE-2024-24919 Exploitation

DETECTION ONLY

BASH (CHECK POINT GAIA CLI)

```
# CVE-2024-24919 allows reading arbitrary files from the gateway
# Check for exploitation attempts in SmartConsole logs
grep -i "information disclosure" /var/log/messages
# Verify hotfix is applied
cpinfo -y fw1 | grep -i hotfix
# Check for unauthorized local user creation
cat /etc/passwd | grep -v "nologin\|false"
```

Hunt Procedure: Scanning Activity from Known Infrastructure

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect scanning from IPs matching Lemon Sandstorm infrastructure patterns
// Censys identified common geolocations: London, Stockholm, Frankfurt, Tel Aviv, LA
// Common ASNs: AS14061 (DigitalOcean), AS16509 (AWS)
// WARNING: These ASNs serve millions of legitimate users. Alert only.
CommonSecurityLog
| where DeviceVendor has_any ("PaloAlto", "CheckPoint", "Palo Alto")
| where Activity has_any ("scan", "probe", "vulnerability", "exploit")
| summarize AttemptCount=count(), DistinctPorts=dcount(DestinationPort)
    by SourceIP, bin(TimeGenerated, 1h)
| where AttemptCount > 50
| sort by AttemptCount desc
```

Triage Guidance

For PAN-OS: verify that the GlobalProtect portal and gateway are running patched versions. CVE-2024-3400 is a critical command injection that enables unauthenticated RCE. For Check Point: CVE-2024-24919 enables reading the /etc/shadow file, allowing offline password cracking. If your gateway was running a vulnerable version, treat all local passwords as compromised.

5 Web Shell Detection on Edge Devices

Duration: 35 min Priority: CRITICAL

Objective: Detect web shells deployed by Lemon Sandstorm on compromised VPN appliances, IIS servers, and Citrix Netscaler devices.

Background

Web shell deployment is a hallmark of Lemon Sandstorm persistence. The Fortinet FortiGuard IR report documented UpdateChecker.aspx (a heavily obfuscated ASPX shell with three command modules), RecShell (reconnaissance), and DropShell (file upload). CISA AA24-241A identified PHP web shells on Citrix Netscaler devices at paths including /netscaler/logon/sanpdebug.php, /netscaler/logon/LogonPoint/uiareas/ui_style.php, and /var/vpn/themes/imgs/. The group also uses China Chopper, a well-known one-line web shell.

Hunt Procedure: Known Web Shell File Names

BLOCKING SAFE

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect known Lemon Sandstorm web shell filenames
// Source: Fortinet FortiGuard IR (May 2025); CISA AA24-241A
let KnownWebShells = dynamic([
    "UpdateChecker.aspx", "RecShell", "DropShell",
    "netscaler.php", "ctxHeaderLogon.php", "netscaler.1",
    "sanpdebug.php", "ui_style.php"
]);
DeviceFileEvents
| where FileName in~ (KnownWebShells)
| project Timestamp, DeviceName, FileName, FolderPath, SHA256,
    InitiatingProcessFileName
| sort by Timestamp desc
```

Hunt Procedure: Web Shell in Known Deployment Paths

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect file creation in known Lemon Sandstorm web shell directories
// Source: CISA AA24-241A
DeviceFileEvents
| where ActionType == "FileCreated"
| where FolderPath has_any (
    "/var/vpn/themes/imgs/",
    "/netscaler/logon/LogonPoint/uiareas/",
    "/netscaler/logon/",
    "/xui/common/images/",
    "inetpub\\wwwroot",
    "\\Windows\\ADFS\\"
)
| where FileName endswith_any (".aspx", ".php", ".jsp", ".ashx", ".asmx")
| project Timestamp, DeviceName, FileName, FolderPath,
    InitiatingProcessFileName, SHA256
| sort by Timestamp desc
```

Hunt Procedure: IIS Worker Process Spawning Shells

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect suspicious child processes spawned by IIS (w3wp.exe)
// Indicates active web shell usage
DeviceProcessEvents
| where InitiatingProcessFileName =~ "w3wp.exe"
| where FileName in~ ("cmd.exe", "powershell.exe", "certutil.exe",
    "whoami.exe", "net.exe", "net1.exe", "systeminfo.exe",
    "ipconfig.exe", "bitsadmin.exe")
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
    InitiatingProcessCommandLine
| sort by Timestamp desc
```

Hunt Procedure: Citrix Netscaler File System Audit

INVESTIGATION AID

BASH (CITRIX NETSCALER CLI)

```
# Search for unauthorized PHP/ASPX files on Citrix appliance
# Source: CISA AA24-241A web shell paths
find /var/vpn/themes/imgs/ -name "*.php" -ls
find /netscaler/logon/ -name "*.php" -newer /nsconfig/ns.conf -ls
find /var/nslog/ -name "*.php" -ls
# Check for unauthorized cron jobs
crontab -l
ls -la /var/spool/cron/
```

> **Critical Finding Indicator**
>
> Any ASPX or PHP file in VPN appliance web directories that cannot be traced to a legitimate vendor update warrants immediate isolation of the appliance. The UpdateChecker.aspx web shell uses heavy obfuscation (nested loops, junk functions, encryption, Unicode encoding) that may bypass basic file content scanning.

6 Credential Harvesting and Lateral Movement

Duration: 30 min Priority: **HIGH**

Objective: Detect credential harvesting tools and lateral movement techniques consistent with Lemon Sandstorm post-exploitation tradecraft.

Background

After gaining initial access through VPN exploitation, Lemon Sandstorm harvests credentials using CredInterceptor (a custom DLL targeting LSASS), Mimikatz, and KeePass database extraction (T1555.005). The group creates local accounts with names designed to blend in: sqladmin$, adfsservice, IIS_Admin, iis-admin, and "John McCain" (source: CISA AA24-241A). The trailing dollar sign on sqladmin$ hides the account from standard user enumeration. For lateral movement, the group uses RDP, SMB, SSH (via Plink), and PsExec.

Hunt Procedure: Detect Lemon Sandstorm Persistence Accounts

BLOCKING SAFE

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect known Lemon Sandstorm persistence account names
// Source: CISA Advisory AA24-241A (Aug 2024)
let SuspiciousAccounts = dynamic([
    "sqladmin$", "adfsservice", "IIS_Admin", "iis-admin", "John McCain"
]);
DeviceEvents
| where ActionType == "UserAccountCreated"
| where AccountName in~ (SuspiciousAccounts)
| project Timestamp, DeviceName, AccountName, InitiatingProcessFileName,
    InitiatingProcessAccountName
| sort by Timestamp desc
```

Hunt Procedure: Hidden Account Detection (Dollar Sign Suffix)

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect local account creation with trailing dollar sign
// Dollar sign accounts are hidden from 'net user' enumeration
DeviceEvents
| where ActionType == "UserAccountCreated"
| where AccountName endswith "$"
| where AccountName !endswith "$$" // Exclude machine accounts
| project Timestamp, DeviceName, AccountName,
    InitiatingProcessFileName, InitiatingProcessCommandLine
| sort by Timestamp desc
```

Hunt Procedure: LSASS Credential Access Detection

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect processes accessing LSASS memory (credential dumping)
// CredInterceptor and Mimikatz both target LSASS
DeviceProcessEvents
| where FileName in~ ("procdump.exe", "procdump64.exe", "mimikatz.exe")
    or ProcessCommandLine has_any ("sekurlsa", "lsass", "minidump")
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

Hunt Procedure: ADFS DLL Side-Loading

BLOCKING SAFE

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect malicious DLL at known Lemon Sandstorm side-loading path
// Source: CISA AA24-241A
DeviceFileEvents
| where FolderPath has "\\Windows\\ADFS\\"
| where FileName =~ "version.dll"
| project Timestamp, DeviceName, FileName, FolderPath, SHA256,
    InitiatingProcessFileName, ActionType
| sort by Timestamp desc
```

Hunt Procedure: Scheduled Task Persistence

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect known Lemon Sandstorm scheduled task name
// Source: CISA AA24-241A
DeviceProcessEvents
| where FileName =~ "schtasks.exe"
| where ProcessCommandLine has_any ("SpaceAgentTaskMgrSHR", "Spaceport")
| project Timestamp, DeviceName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
```

Hunt Procedure: "kharpedar" Password Pattern

BLOCKING SAFE

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Hunt for "kharpedar" password string in command lines
// Used with variations since 2017 (source: Secureworks COBALT FOXGLOVE)
DeviceProcessEvents
| where ProcessCommandLine has "kharpedar"
| project Timestamp, DeviceName, FileName, ProcessCommandLine, AccountName
```

Critical Finding Indicator

The "kharpedar" password string is a unique operational fingerprint for Lemon Sandstorm, documented by Secureworks since 2017. Any match is a high-confidence indicator. Similarly, any account named "sqladmin$" with a trailing dollar sign should trigger immediate investigation.

7 Tunneling Tool Detection (Chisel, ngrok, ligolo)

Duration: 25 min Priority: HIGH

Objective: Detect tunneling and proxy tools used by Lemon Sandstorm for outbound C2 communications, lateral movement, and network pivoting.

Background

Protocol tunneling is a defining characteristic of Lemon Sandstorm. CrowdStrike originally tracked this actor as "TunnelMaster" before renaming it to Pioneer Kitten. The group uses Ngrok for creating random subdomains as C2 channels, Ligolo/Ligolo-ng for proxy operations, Chisel for TCP/UDP tunneling over HTTP, FRP (Fast Reverse Proxy) for exposing internal services, Plink for SSH tunneling, and custom tools SSHMinion and POWSSHNET. The Fortinet report confirmed use of Plink and Ngrok during the Middle East CNI intrusion.

Hunt Procedure: Tunneling Tool Process Detection

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect execution of known tunneling tools
// Source: MITRE ATT&CK G0117; Secureworks; Fortinet
DeviceProcessEvents
| where FileName in~ ("ngrok.exe", "chisel.exe", "ligolo.exe",
    "ligolo-agent.exe", "ligolo-proxy.exe",
    "frpc.exe", "frps.exe", "plink.exe",
    "gost.exe", "iox.exe")
    or ProcessCommandLine has_any ("ngrok", "chisel", "ligolo",
    "frpc", "frps", "SSHMinion", "POWSSHNET")
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

Hunt Procedure: Ngrok Domain Connections

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect network connections to ngrok infrastructure
DeviceNetworkEvents
| where RemoteUrl has_any ("ngrok.io", "ngrok.com", "ngrok-free.app",
    "tunnel.us.ngrok.com", "tunnel.eu.ngrok.com")
| project Timestamp, DeviceName, InitiatingProcessFileName,
    RemoteUrl, RemoteIP, RemotePort
| sort by Timestamp desc
```

Hunt Procedure: SSH Tunneling via Plink

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect Plink SSH tunneling (common Lemon Sandstorm lateral movement tool)
DeviceProcessEvents
| where FileName =~ "plink.exe"
    or (ProcessCommandLine has "plink" and ProcessCommandLine has_any ("-R", "-L", "-D", "-ssh"))
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

> **Ngrok Legitimate Usage Caveat**
>
> Some organizations use Ngrok for legitimate development and testing purposes. Before blocking, verify with development teams whether Ngrok is sanctioned. However, Ngrok usage on production servers or from unexpected user accounts is a high-priority finding.

8 Known C2 Infrastructure Detection

Duration: 25 min Priority: MEDIUM

Objective: Detect network connections to known Lemon Sandstorm C2 domains and IP addresses documented in CISA advisories and vendor research.

Background

Lemon Sandstorm operates C2 infrastructure across multiple cloud providers. The Fortinet FortiGuard IR report identified apps.gist.githubapp[.]net and gupdate[.]net as active C2 domains during the Middle East CNI intrusion. CISA AA24-241A published 12 IP addresses across DigitalOcean (AS14061) and AWS (AS16509). Censys infrastructure analysis revealed additional IOCs including self-signed certificates with anomalous names (futureenergy.us, next-finance.mil).

Hunt Procedure: Known C2 Domain Detection

BLOCKING SAFE

KQL (MICROSOFT SENTINEL)

```
// Detect DNS queries or connections to known C2 domains
// Source: Fortinet FortiGuard IR (May 2025); CISA AA24-241A
let C2Domains = dynamic([
    "apps.gist.githubapp.net", "githubapp.net",
    "api.gupdate.net", "gupdate.net",
    "login.forticloud.online", "fortigate.forticloud.online",
    "cloud.sophos.one"
]);
DnsEvents
| where Name has_any (C2Domains)
| project TimeGenerated, ClientIP, Name, QueryType
| sort by TimeGenerated desc
```

Hunt Procedure: Known C2 IP Detection

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect connections to known Lemon Sandstorm infrastructure IPs
// Source: CISA Advisory AA24-241A (Aug 2024)
// WARNING: These are cloud provider IPs. See blocking guidance in Appendix A.
let C2IPs = dynamic([
    "138.68.90.19", "167.99.202.130", "78.141.238.182",
    "51.16.51.81", "51.20.138.134", "134.209.30.220",
    "13.53.124.246", "18.134.0.66", "193.149.190.248",
    "45.76.65.42", "206.71.148.78", "193.149.187.41"
]);
CommonSecurityLog
| where DestinationIP in (C2IPs) or SourceIP in (C2IPs)
| project TimeGenerated, SourceIP, DestinationIP,
    DestinationPort, DeviceVendor, Activity
| sort by TimeGenerated desc
```

Hunt Procedure: Catbox File Hosting Connections

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect connections to files.catbox.moe (used for payload delivery)
// Source: CISA AA24-241A
// WARNING: Legitimate file hosting service. Do NOT block the domain.
// Monitor for connections in context of other indicators.
DnsEvents
| where Name has "catbox.moe"
| project TimeGenerated, ClientIP, Name, QueryType
| sort by TimeGenerated desc
```

> **Cloud Infrastructure Caveat**
>
> All 12 IP addresses from CISA AA24-241A belong to cloud providers (DigitalOcean, AWS, Vultr). Blocking these IPs or ranges will disrupt legitimate cloud services. These indicators are suitable for detection and alerting only. Cross-reference any matches with other indicators from this guide before escalating.

9 Ransomware Precursor Indicators

Duration: 25 min Priority: **MEDIUM**

Objective: Detect ransomware precursor tools and behaviors associated with Lemon Sandstorm's ransomware affiliate operations, including SystemBC, remote management tool abuse, and data staging for exfiltration.

Background

Lemon Sandstorm operates as a ransomware affiliate with ALPHV/BlackCat, NoEscape, and Ransomhouse (source: CISA AA24-241A). The Fortinet report documented deployment of SystemBC (a known ransomware precursor proxy backdoor) and MeshCentral Agent in December 2024 during the Middle East CNI intrusion. SystemBC was loaded via DarkLoadLibrary, an open-source in-memory loader. The group also operates its own Pay2Key.I2P ransomware-as-a-service platform, which achieved 51+ payouts in its first four months (source: Morphisec, July 2025). The group sells access via a Tor site using the "Br0k3r" persona, advertising domain administrator credentials, Active Directory hashes, DNS zone files, and domain trust mappings.

Hunt Procedure: SystemBC Detection

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect SystemBC proxy backdoor indicators
// SystemBC creates SOCKS5 proxy connections
DeviceNetworkEvents
| where InitiatingProcessFileName !in~ ("chrome.exe", "msedge.exe",
    "firefox.exe", "svchost.exe")
| where RemotePort in (1080, 4443, 4444, 5555)
| summarize ConnectionCount=count(),
    DistinctRemoteIPs=dcount(RemoteIP)
    by InitiatingProcessFileName, DeviceName, bin(Timestamp, 1h)
| where ConnectionCount > 10
| sort by ConnectionCount desc
```

Hunt Procedure: Unauthorized Remote Management Tools

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect MeshCentral Agent and AnyDesk (used by Lemon Sandstorm)
// Source: Fortinet FortiGuard IR; CISA AA24-241A
DeviceProcessEvents
| where FileName in~ ("MeshAgent.exe", "MeshAgent64.exe",
    "AnyDesk.exe", "anydesk.exe")
    or ProcessCommandLine has_any ("meshcentral", "anydesk")
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

Hunt Procedure: Data Staging and Archive Creation

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect 7-Zip or RAR archiving of large datasets (data staging)
// Lemon Sandstorm uses 7-Zip for data archiving (T1560.001)
DeviceProcessEvents
| where FileName in~ ("7z.exe", "7za.exe", "rar.exe", "WinRAR.exe")
| where ProcessCommandLine has_any ("-p", "password")
    or (FileName in~ ("7z.exe", "7za.exe") and ProcessCommandLine has " a ")
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

Hunt Procedure: Volume Shadow Copy Deletion

DETECTION ONLY

KQL (MICROSOFT DEFENDER FOR ENDPOINT)

```
// Detect shadow copy deletion (ransomware pre-step)
DeviceProcessEvents
| where ProcessCommandLine has_any (
    "vssadmin delete shadows",
    "wmic shadowcopy delete",
    "bcdedit /set {default} recoveryenabled no",
    "wbadmin delete catalog"
)
| project Timestamp, DeviceName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

Ransomware Deployment Window

If SystemBC, unauthorized RMM tools, data staging, or shadow copy deletion are detected, the organization may be in the pre-deployment phase of a ransomware attack. Immediately isolate affected endpoints, revoke compromised credentials, and engage incident response. Lemon Sandstorm actively participates in locking down networks and devising extortion strategies alongside ransomware partners (source: CISA AA24-241A).

10 OT/ICS Network Boundary Assessment

Duration: 30 min Priority: **MEDIUM**

Objective: Assess the security boundary between IT and OT/ICS networks, identify potential traversal paths exploitable by Lemon Sandstorm and the Pyroxene threat group, and verify segmentation controls.

Background

The Fortinet FortiGuard IR report confirmed that Lemon Sandstorm's primary objective in the Middle East CNI intrusion was the restricted OT network. While Fortinet assessed "no evidence that the adversary penetrated the OT network," the two-year persistence indicated pre-positioning for future access. Dragos identified a formalized handoff model: Parisite (Lemon Sandstorm) provides initial IT access, then Pyroxene specializes in IT-to-OT traversal. Pyroxene targets aviation, aerospace, defense, and maritime sectors across the US, Western Europe, Israel, and UAE (source: Dragos 2026 Year in Review). With Operation Epic Fury escalating the Iran-US conflict, activation of pre-positioned OT access is a realistic near-term scenario.

Hunt Procedure: IT-to-OT Network Traffic Analysis

INVESTIGATION AID

KQL (MICROSOFT SENTINEL)

```
// Detect IT network traffic crossing into OT/ICS network segments
// Requires proper network segmentation and firewall logging
// Replace CIDR ranges below with your actual OT network ranges
CommonSecurityLog
| where ipv4_is_in_any_range(DestinationIP, "10.100.0.0/16", "172.20.0.0/16")
| where not(ipv4_is_in_any_range(SourceIP, "10.100.0.0/16", "172.20.0.0/16")) // IT to OT
| where DeviceAction != "Deny"
| summarize ConnectionCount=count(),
    DistinctSources=dcount(SourceIP),
    DistinctPorts=dcount(DestinationPort)
    by DestinationIP, bin(TimeGenerated, 1d)
| where ConnectionCount > 10
| sort by ConnectionCount desc
```

Hunt Procedure: OT Protocol Detection on IT Networks

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect OT/ICS protocol traffic on IT network segments
// Presence of these protocols on IT segments indicates boundary violation
CommonSecurityLog
| where DestinationPort in (
    502,    // Modbus
    102,    // S7comm (Siemens)
    44818,  // EtherNet/IP (CIP)
    20000,  // DNP3
    4840,   // OPC UA
    2222    // EtherCAT
)
| project TimeGenerated, SourceIP, DestinationIP,
    DestinationPort, DeviceVendor, Activity
| sort by TimeGenerated desc
```

Hunt Procedure: ZKTeco BioTime Exploitation

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect exploitation of ZKTeco BioTime (physical access control)
// Lemon Sandstorm exploited CVE-2023-38950/51/52 in Phase 4
// Source: Fortinet FortiGuard IR (May 2025)
CommonSecurityLog
| where DestinationPort in (80, 443, 8080, 8443)
| where RequestURL has_any ("biotime", "ZKTeco", "zkaccess")
| project TimeGenerated, SourceIP, DestinationIP,
    RequestURL, DeviceAction
| sort by TimeGenerated desc
```

Manual Review Checklist

- ☐ Verify that IT and OT networks are properly segmented with a demilitarized zone (DMZ) between them
- ☐ Confirm that firewall rules between IT and OT segments follow a default-deny policy
- ☐ Audit all jump servers and bastion hosts that bridge IT and OT environments
- ☐ Verify that remote access to OT systems requires separate credentials from IT domain accounts
- ☐ Check that ZKTeco BioTime physical access systems are patched against CVE-2023-38950/51/52
- ☐ Confirm that OT network monitoring (e.g., Dragos, Claroty, Nozomi) is operational and alerting

OT/ICS Impact Warning

Lemon Sandstorm's documented Parisite-Pyroxene handoff model creates a direct pipeline from IT compromise to OT impact. The Fortinet report confirmed OT was the primary target of the two-year Middle East CNI intrusion. Organizations in the energy, water, manufacturing, and defense sectors should treat any IT compromise by this actor as a precursor to potential OT operations. Coordinate with OT security teams and ICS-CERT immediately.

A Appendix A: Indicators of Compromise

Blocking Guidance: 3-Tier IOC Classification

Tier 1: Block (High Confidence)

C2 domains (apps.gist.githubapp[.]net, gupdate[.]net, api.gupdate[.]net, githubapp[.]net): Confirmed Lemon Sandstorm C2 infrastructure documented by Fortinet FortiGuard IR and CISA. Safe to add to DNS sinkhole and firewall deny rules.

Phishing domains (login.forticloud[.]online, fortigate.forticloud[.]online, cloud.sophos[.]one): Confirmed credential harvesting domains. Safe to block at DNS and web proxy level.

Known web shell filenames and the "kharpedar" password pattern: Safe for file-based detection and EDR blocking rules.

Tier 2: Alert / Monitor (Shared Infrastructure)

CISA AA24-241A IP addresses (138.68.90.19, 167.99.202.130, etc.): These belong to DigitalOcean (AS14061), AWS (AS16509), and Vultr cloud providers. Blocking cloud provider IP ranges will disrupt legitimate services. Deploy as detection/alerting queries only. Require analyst review before action. Do NOT block at network level.

files.catbox[.]moe: Legitimate file hosting service also used by non-malicious actors. Do NOT block the domain. Monitor for connections in context of other indicators.

Tunneling tool domains (ngrok.io, ngrok.com): Ngrok is a legitimate development tool used by many organizations. Blocking requires coordination with development teams. Alert on unexpected usage only.

Self-signed certificates (futureenergy.us, next-finance.mil): Monitor for these certificate names in TLS inspection logs. These are infrastructure patterns, not blocklist candidates.

Tier 3: Investigate (Unconfirmed)

Cloud provider IPs matching Censys infrastructure patterns: Censys identified 38,862 potentially malicious hosts matching Fox Kitten patterns across DigitalOcean and AWS. These require individual investigation before any action. Many will be legitimate services.

Historical IPs (193.149.190.248, 45.76.65.42, 206.71.148.78, 193.149.187.41): Older infrastructure from CISA AA24-241A. May have been reassigned to legitimate users. Verify current assignment before any blocking action.

Network Indicators (C2 IPs)

Indicator	Provider	Context	Source	Tier
`138.68.90.19`	DigitalOcean	Active through Aug 2024	CISA AA24-241A	Alert
`167.99.202.130`	DigitalOcean	Active through Aug 2024	CISA AA24-241A	Alert
`78.141.238.182`	Cloud/VPS	Active through Aug 2024	CISA AA24-241A	Alert
`51.16.51.81`	AWS	Active through Aug 2024	CISA AA24-241A	Alert
`51.20.138.134`	AWS	Active through Aug 2024	CISA AA24-241A	Alert
`134.209.30.220`	DigitalOcean	Active through Aug 2024	CISA AA24-241A	Alert
`13.53.124.246`	AWS	Active through Aug 2024	CISA AA24-241A	Alert
`18.134.0.66`	AWS	Historical	CISA AA24-241A	Investigate
`193.149.190.248`	VPS	Historical	CISA AA24-241A	Investigate
`45.76.65.42`	Vultr	Historical	CISA AA24-241A	Investigate

`206.71.148.78`	VPS	Historical	CISA AA24-241A	Investigate
`193.149.187.41`	VPS	Historical	CISA AA24-241A	Investigate

All IP addresses above belong to cloud and VPS providers. Blocking cloud provider IP ranges may disrupt legitimate integrations and services. **Recommend monitoring and contextual analysis only.** Cross-reference matches with other Lemon Sandstorm indicators before escalating.

C2 Domains

Indicator	Context	Source	Tier
`apps.gist.githubapp[.]net`	Active C2 (Middle East CNI intrusion)	Fortinet FortiGuard IR; Censys	Block
`githubapp[.]net`	C2 parent domain	CISA AA24-241A; Censys	Block
`api.gupdate[.]net`	C2 domain (active since Apr 2024)	CISA AA24-241A; Censys; Fortinet	Block
`gupdate[.]net`	C2 parent domain	Fortinet FortiGuard IR	Block
`login.forticloud[.]online`	Credential harvesting (Fortinet impersonation)	CISA AA24-241A	Block
`fortigate.forticloud[.]online`	Credential harvesting (Fortinet impersonation)	CISA AA24-241A	Block
`cloud.sophos[.]one`	Credential harvesting (Sophos impersonation)	CISA AA24-241A	Block
`files.catbox[.]moe`	Payload delivery / exfiltration	CISA AA24-241A	Alert

Web Shell Indicators

Filename	Type	Deployment Path	Source
`UpdateChecker.aspx`	ASPX (obfuscated, 3 modules)	IIS web directories	Fortinet FortiGuard IR
`RecShell`	Web shell (recon)	External-facing servers	Fortinet FortiGuard IR
`DropShell`	Web shell (file upload)	External-facing servers	Fortinet FortiGuard IR
`netscaler.php`	PHP web shell	Citrix Netscaler	CISA AA24-241A
`ctxHeaderLogon.php`	PHP web shell	Citrix Netscaler	CISA AA24-241A
`sanpdebug.php`	PHP web shell	`/netscaler/logon/`	CISA AA24-241A
`ui_style.php`	PHP web shell	`/netscaler/logon/LogonPoint/uiareas/`	CISA AA24-241A
`netscaler.1`	Web shell	Citrix Netscaler	CISA AA24-241A
`China Chopper`	One-line web shell	Various	MITRE ATT&CK G0117

Persistence Indicators

Type	Indicator	Context	Source
Account	`sqladmin$`	Hidden local account (trailing $)	CISA AA24-241A
Account	`adfsservice`	Local persistence account	CISA AA24-241A
Account	`IIS_Admin`	Local persistence account	CISA AA24-241A
Account	`iis-admin`	Local persistence account	CISA AA24-241A
Account	`John McCain`	Deceptive account name	CISA AA24-241A
Password	`kharpedar`	Operational fingerprint since 2017	Secureworks
Sched Task	`SpaceAgentTaskMgrSHR`	Persistence task (Windows\Spaceport\)	CISA AA24-241A
File Path	`C:\Windows\ADFS\version.dll`	DLL side-loading location	CISA AA24-241A
File Path	`/var/vpn/themes/imgs/`	Web shell dir (Citrix)	CISA AA24-241A
File Path	`/xui/common/images/`	Web shell deployment dir	CISA AA24-241A

CVE Reference Table

CVE	Product	Type	First Exploited	Source
`CVE-2019-11510`	Pulse Secure VPN	Arbitrary file read	2019	CISA AA20-259A
`CVE-2019-11539`	Pulse Secure VPN	RCE	2019	CISA AA20-259A
`CVE-2024-21887`	Ivanti Connect Secure	Command injection	2024	CISA AA24-241A
`CVE-2018-13379`	Fortinet FortiOS SSL VPN	Path traversal	2019	ClearSky
`CVE-2019-1579`	Palo Alto GlobalProtect	RCE	2019	ClearSky
`CVE-2024-3400`	Palo Alto PAN-OS	Command injection	Apr 2024	CISA AA24-241A
`CVE-2024-24919`	Check Point Gateways	Info disclosure	Jul 2024	CISA AA24-241A
`CVE-2019-19781`	Citrix ADC/NetScaler	Dir traversal / RCE	2019	CISA AA20-259A

`CVE-2023-3519`	Citrix NetScaler ADC	RCE	2023	CISA AA24-241A
`CVE-2020-5902`	F5 BIG-IP	RCE	2020	CISA AA20-259A
`CVE-2022-1388`	F5 BIG-IP	Auth bypass / RCE	2022	CISA AA24-241A
`CVE-2023-38950`	ZKTeco BioTime	Exploitation	Dec 2024	Fortinet
`CVE-2023-38951`	ZKTeco BioTime	Exploitation	Dec 2024	Fortinet
`CVE-2023-38952`	ZKTeco BioTime	Exploitation	Dec 2024	Fortinet

B Appendix B: Detection Rules

KQL Detection Rules

Lemon Sandstorm C2 Domain Detection KQL

BLOCKING SAFE

MICROSOFT SENTINEL

```
// RULE: Detect DNS queries to confirmed Lemon Sandstorm C2 domains
// Source: Fortinet FortiGuard IR; CISA AA24-241A; Censys
let C2Domains = dynamic([
    "apps.gist.githubapp.net", "githubapp.net",
    "api.gupdate.net", "gupdate.net",
    "login.forticloud.online", "fortigate.forticloud.online",
    "cloud.sophos.one"
]);
DnsEvents
| where Name has_any (C2Domains)
| extend AlertSeverity = "High"
| project TimeGenerated, ClientIP, Name, QueryType, AlertSeverity
| sort by TimeGenerated desc
```

VPN Appliance Web Shell Detection KQL

BLOCKING SAFE

MICROSOFT DEFENDER FOR ENDPOINT

```
// RULE: Detect known Lemon Sandstorm web shell files
let WebShellNames = dynamic([
    "UpdateChecker.aspx", "netscaler.php", "ctxHeaderLogon.php",
    "sanpdebug.php", "ui_style.php", "netscaler.1"
]);
let WebShellPaths = dynamic([
    "/var/vpn/themes/imgs/", "/netscaler/logon/",
    "/xui/common/images/", "\\Windows\\ADFS\\"
]);
DeviceFileEvents
| where FileName in~ (WebShellNames)
    or (FolderPath has_any (WebShellPaths)
        and FileName endswith_any (".aspx", ".php", ".jsp"))
| project Timestamp, DeviceName, FileName, FolderPath, SHA256
| sort by Timestamp desc
```

Tunneling Tool Execution Detection KQL

DETECTION ONLY

MICROSOFT DEFENDER FOR ENDPOINT

```
// RULE: Detect execution of tunneling tools used by Lemon Sandstorm
DeviceProcessEvents
| where FileName in~ ("ngrok.exe", "chisel.exe", "ligolo.exe",
    "ligolo-agent.exe", "frpc.exe", "frps.exe", "plink.exe",
    "gost.exe", "iox.exe")
    or ProcessCommandLine has_any ("ngrok", "chisel", "ligolo",
    "SSHMinion", "POWSSHNET")
| extend AlertSeverity = case(
    FileName in~ ("ngrok.exe", "chisel.exe", "ligolo.exe"), "High",
    "Medium")
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
    AccountName, AlertSeverity
| sort by Timestamp desc
```

Hidden Account Creation (Dollar Sign Suffix) KQL

DETECTION ONLY

MICROSOFT DEFENDER FOR ENDPOINT

```
// RULE: Detect local account creation with trailing dollar sign
// Lemon Sandstorm creates sqladmin$ to hide from enumeration
DeviceEvents
| where ActionType == "UserAccountCreated"
| where AccountName endswith "$"
| where AccountName !endswith "$$"
| extend AlertSeverity = "High"
| project Timestamp, DeviceName, AccountName,
    InitiatingProcessFileName, AlertSeverity
```

IIS Web Shell Activity

KQL

DETECTION ONLY

MICROSOFT DEFENDER FOR ENDPOINT

```
// RULE: Detect IIS worker process spawning suspicious child processes
DeviceProcessEvents
| where InitiatingProcessFileName =~ "w3wp.exe"
| where FileName in~ ("cmd.exe", "powershell.exe", "certutil.exe",
    "bitsadmin.exe", "net.exe", "whoami.exe", "systeminfo.exe")
| extend AlertSeverity = case(
    FileName in~ ("certutil.exe", "bitsadmin.exe"), "High",
    "Medium")
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
    AlertSeverity
| sort by Timestamp desc
```

Sigma Rule: Lemon Sandstorm Tunneling Tool Execution

Sigma Rule Disclaimer

This Sigma rule requires conversion to your SIEM's native query language using sigmac or pySigma. Test thoroughly in a non-production environment before deployment. Adjust for environment-specific false positives.

DETECTION ONLY

SIGMA (YAML)

```
title: Lemon Sandstorm Tunneling Tool Execution
id: b3c4d5e6-f7a8-9012-bcde-1e40a52a0d01
status: experimental
description: |
    Detects execution of tunneling tools associated with
    Lemon Sandstorm / Pioneer Kitten (T1572). Includes Ngrok,
    Chisel, Ligolo, FRP, Plink, SSHMinion, and POWSSHNET.
references:
    - https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a
    - https://attack.mitre.org/groups/G0117/
    - https://www.crowdstrike.com/en-us/blog/who-is-pioneer-kitten/
author: Intruvent Technologies
date: 2026-03-11
tags:
    - attack.command-and-control
    - attack.t1572
    - attack.t1090
logsource:
    category: process_creation
    product: windows
detection:
    selection_filename:
        Image|endswith:
            - '\ngrok.exe'
            - '\chisel.exe'
            - '\ligolo.exe'
            - '\ligolo-agent.exe'
            - '\ligolo-proxy.exe'
            - '\frpc.exe'
            - '\frps.exe'
            - '\plink.exe'
            - '\gost.exe'
            - '\iox.exe'
    selection_cmdline:
        CommandLine|contains:
            - 'SSHMinion'
            - 'POWSSHNET'
            - 'ngrok tcp'
            - 'chisel client'
            - 'ligolo'
    condition: selection_filename or selection_cmdline
falsepositives:
    - Legitimate use of Ngrok by development teams
    - Legitimate use of Plink for SSH administration
    - Penetration testing activities
level: high
```

YARA Rule: Lemon Sandstorm Web Shell Patterns

BLOCKING SAFE

YARA

```
rule LemonSandstorm_WebShell_Indicators {
    meta:
        description = "Detects Lemon Sandstorm web shell patterns on VPN appliances and IIS servers"
        author = "Intruvent Technologies"
        date = "2026-03-11"
        reference = "Fortinet FortiGuard IR (May 2025); CISA AA24-241A"
        tlp = "TLP:CLEAR"

    strings:
        $ws1 = "UpdateChecker" ascii wide
        $ws2 = "RecShell" ascii wide
        $ws3 = "DropShell" ascii wide
        $ws4 = "sanpdebug" ascii wide
        $ws5 = "ctxHeaderLogon" ascii wide

        $path1 = "/var/vpn/themes/imgs/" ascii
        $path2 = "/netscaler/logon/LogonPoint/uiareas/" ascii
        $path3 = "/xui/common/images/" ascii

        $pwd = "kharpedar" ascii wide nocase

        $cmd1 = "CommandShell" ascii wide
        $cmd2 = "FileManager" ascii wide
        $obf1 = "Unicode" ascii wide

    condition:
        (any of ($ws*) and filesize < 1MB) or
        ($pwd) or
        (any of ($path*) and filesize < 500KB) or
        (any of ($ws*) and $cmd1 and $cmd2)
}
```

YARA Rule: Lemon Sandstorm Custom Malware (HanifNet)

BLOCKING SAFE

YARA

```
rule LemonSandstorm_HanifNet_Backdoor {
    meta:
        description = "Detects HanifNet backdoor (.NET) used by Lemon Sandstorm"
        author = "Intruvent Technologies"
        date = "2026-03-11"
        reference = "Fortinet FortiGuard IR (May 2025)"
        tlp = "TLP:CLEAR"

    strings:
        $dotnet = "mscoree.dll" ascii
        $name = "masf.exe" ascii wide nocase
        $arg2 = ".config" ascii
        $xml = "XmlDocument" ascii wide
        $http = "HttpWebRequest" ascii wide

    condition:
        uint16(0) == 0x5A4D and
        $dotnet and
        ($name or ($arg2 and $xml and $http and filesize < 2MB))
}
```

C Appendix C: References

Government Advisories

[1] **CISA/FBI/DC3** - "Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations" (Advisory AA24-241A, August 28, 2024)
cisa.gov

[2] **CISA/FBI** - "Iran-Based Threat Actor Exploits VPN Vulnerabilities" (Advisory AA20-259A, September 15, 2020)
cisa.gov

[3] **FBI IC3** - "Iran-based Cyber Actors Enabling Ransomware Attacks on U.S. Organizations" (August 28, 2024)
ic3.gov

Vendor Threat Intelligence (Primary)

[4] **Fortinet FortiGuard IR** - "Investigating Iranian Intrusion into Strategic Middle East Critical National Infrastructure" (May 2025)
fortinet.com

[5] **Fortinet FortiGuard IR** - Full PDF Report (May 2025)
fortinet.com

[6] **CrowdStrike** - "PIONEER KITTEN: Targets & Methods" (September 2020)
crowdstrike.com

[7] **CrowdStrike** - "Pioneer Kitten Adversary Profile"
crowdstrike.com

[8] **Secureworks** - "COBALT FOXGLOVE Threat Profile"
secureworks.com

[9] **ClearSky** - "Fox Kitten Campaign" (February 2020)
clearskysec.com

[10] **ClearSky** - "Pay2Kitten: Fox Kitten 2 / Pay2Key Ransomware Campaign" (December 2020)
clearskysec.com

[11] **Dragos** - "2026 Year in Review: New OT Threats and Ransomware"
dragos.com

[12] **Morphisec** - "Pay2Key's Resurgence: Iranian Cyber Warfare Targets the West" (July 2025)
morphisec.com

[13] **Censys** - "Analysis of Fox Kitten Infrastructure Reveals Unique Host Patterns and Potentially New IOCs" (September 2024)
censys.com

[14] **MITRE ATT&CK** - "Fox Kitten, Group G0117"
attack.mitre.org

[15] **Microsoft** - "Microsoft Digital Defense Report 2025"
microsoft.com

Investigative Journalism

[16] **The Hacker News** - "Iranian Hackers Maintain 2-Year Access to Middle East CNI via VPN Flaws and Malware" (May 3, 2025)
thehackernews.com

[17] **Dark Reading** - "Lemon Sandstorm Reveals Risks to Middle East Infrastructure" (May 2025)
darkreading.com

[18] **The Register** - "Iranian ransomware crew reemerges, promises big bucks for attacks on US or Israel" (July 9, 2025)
theregister.com

[19] **Bleeping Computer** - "Iranian hackers act as brokers selling critical infrastructure access" (August 28, 2024)
bleepingcomputer.com

Industry Reports (2026 Iran Conflict Context)

[20] **Palo Alto Unit 42** - "Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran"
unit42.paloaltonetworks.com

[21] **CloudSEK** - "A Threat Actor Landscape Assessment of ICS/OT Targeting in the 2026 Iran-US Conflict"
cloudsek.com

[22] **BeyondTrust** - "Threat Advisory: Iran-Aligned Cyber Actors Respond to Operation Epic Fury"
beyondtrust.com

[23] **Proofpoint** - "Iran conflict drives heightened espionage activity against Middle East targets" (March 2026)
proofpoint.com

[24] **AttackIQ** - "Defending Against Iranian Cyber Threats in the Wake of Operation Epic Fury" (March 5, 2026)
attackiq.com

[25] **SecurityWeek** - "3 Threat Groups Started Targeting ICS/OT in 2025: Dragos" (February 2026)
securityweek.com

[26] **Cybersecurity Dive** - "US entities face heightened cyber risk related to Iran war" (March 2026)
cybersecuritydive.com

OSINT & Analyst Research

[27] **Picus Security** - "Pioneer Kitten: Iranian Threat Actors Facilitate Ransomware Attacks Against U.S. Organizations"
picussecurity.com

[28] **Huntress** - "Fox Kitten Threat Actor Profile"
huntress.com

[29] **Malpedia** - "Fox Kitten"
malpedia.caad.fkie.fraunhofer.de

[30] **HHS Cybersecurity** - "Iranian Threat Actors & Healthcare" (November 3, 2022)
hhs.gov

[31] **FDD** - "Pioneer Kitten: A New Iranian Cyber Threat Group Emerges" (September 16, 2020)
fdd.org

[32] **Trellix** - "The Iranian Cyber Capability"
trellix.com

[33] **Flashpoint** - "Escalation in the Middle East: Tracking Operation Epic Fury Across Military and Cyber Domains" (March 2026)
flashpoint.io

NEED HELP IMPLEMENTING THESE DETECTIONS?

Our threat hunting team can deploy, tune, and operationalize these detection rules in your environment.

- ✓ Detection rule deployment and tuning
- ✓ Managed threat hunting operations
- ✓ Incident response retainer

Contact Our Team

or

Automate continuous detection with BRACE, our sector-specific threat intelligence platform. **See BRACE plans →**