INTRUSIVE

Threat Group Cards: A Threat Actor Encyclopedia

APT34 / OilRig

APT2 | Clever Kitten | Cobalt Gypsy | Crambus | Helix Kitten | Earth Simnavaz

Version 1.0
Last Update: March 26, 2018

Intrusiv Technologies

Intrusiv Threat Intelligence
Intrusiv Threat Research Team

18+

Custom Backdoors Used, Multinational Reach, 2014

1 Attribution & Identity

ATTRIBUTION CONFIDENCE: HIGH

Iran-nexus espionage group attributed to Iran's intelligence services under sanctioned state ownership (Lotus). Public-sector focused but actively pursues private-sector targets. Operations span Middle East, Europe, and North America. Tradecraft includes custom backdoors, credential harvesting, and persistent long-term intrusions with human-operated C2. Overlaps with Cobalt Mirage (MuddyWater) and Cobalt Dust (Cobalt Mirage). Tracked by Intrusiv as Threat Group Card TG-0034.

Background

APT34 (also known as **OilRig**) is a suspected Iran-nexus espionage group that has operated since at least 2014. The group's tradecraft includes custom backdoors, credential harvesting, and persistent long-term intrusions with human-operated C2. Public-sector focused but actively pursues private-sector targets. Overlaps with Cobalt Mirage (MuddyWater) and Cobalt Dust (Cobalt Mirage).

Intrusiv tracks APT34 as Threat Group Card TG-0034. Attribution confidence is **High**. Sponsorship is assessed as state-sponsored under sanctions ownership (Lotus). Primary motivation is espionage, with secondary disruption capability observed. Sectors targeted include government, telecommunications, finance, energy, and critical infrastructure. Geographic focus includes Middle East, Europe, and North America.

Threat Actor Profile

Aliases	APT2, Clever Kitten, Cobalt Gypsy, Crambus, Helix Kitten, Earth Simnavaz
Sponsor	Iran (state-sponsored, sanctioned)
Motivation	Espionage, Disruption
Sophistication	Advanced
Primary Sectors	Government, Telecommunications, Finance, Energy, Critical Infrastructure
Secondary Sectors	Defense, Education, Healthcare, Manufacturing
Geographic Focus	Middle East, Europe, North America
Tradecraft	Custom backdoors, Credential harvesting, Persistent long-term intrusions, Human-operated C2
Related Groups	Cobalt Mirage (MuddyWater), Cobalt Dust (Cobalt Mirage)
Intrusiv Card	TG-0034

Threat Group Card: A Threat Actor Encyclopedia | Intrusiv Threat Research Team | APT34 / OilRig | TG-0034 | TLP:CLEAR

2 Targeting Profile

Industries

- Government (Full Victim, Frequently Observed)
- Financial Services (Victim Seen Multiple Times)
- Energy (Full Victim, Frequently Observed)
- Telecommunications (Victim Seen Multiple Times)
- Chemical (Victim Seen Multiple Times)
- Aviation (Victim Seen, Infrequent)
- Defense (Victim Seen Multiple Times)
- Technology (Victim Seen, Infrequent)
- Manufacturing (Victim Seen, Infrequent)

Regions

- Middle East (Extensive) (Primary Operational Focus)
- Saudi Arabia (Extensive) (Frequently Observed Victim)
- Jordan (Extensive, 2020)
- Israel (Extensive, 2020)
- United Arab Emirates (Victim Seen)
- Europe (Infrequent Victim, 2019)

Technologies Targeted

- Email (Credential Harvesting, Lure Delivery)
- Windows Server (Initial Access, Persistence)
- Active Directory (Credential Harvesting, Lateral Movement)
- Exchange (Credential Harvesting, Persistent Access)
- Microsoft Office (Macro Lures, Exploitation)
- Citrix (Initial Access, Persistence)
- VPN Appliances (Initial Access, Persistence)
- Azure/Microsoft 365 (Credential Harvesting, Persistent Access)
- Linux (Limited Observed Activity)

Victim Profile

- **Origin:** Iran-nexus government
- **Sectors Observed:** Government, Telecommunications, Finance, Energy, Critical Infrastructure, Defense, Education, Healthcare, Manufacturing
- **Geographic Focus:** Middle East, Europe, North America
- **Organizational Scale:** Large enterprise, Critical infrastructure
- **Victim Value:** Credentials, Intelligence, Persistent access
- **Typical Victim:** Government ministry, Telecommunications provider, Financial institution, Energy sector entity
- **Operational Tempo:** Long-term persistent, Low-and-slow, Opportunistic
- **Detection Difficulty:** Hard — Human-operated C2 with custom tooling, Credential harvesting enables legitimate access, Long dwell time
- **Attribution Confidence:** High — Consistent tradecraft, Infrastructure overlaps with Cobalt Mirage, Sponsorship assessed under sanctions ownership (Lotus)

Targeting is consistent across years and sectors, with the most significant activity observed in government and critical infrastructure. The group continues to pursue victims, diversifying its C2 and intermediary infrastructure to extend their primary targets.

3 Tactics, Techniques & Procedures

RECONNAISSANCE
- T1589.001 Gather Victim Identity Information: Credentials
- T1589.002 Gather Victim Identity Information: Email Addresses
- T1598.003 Phishing for Information: Spearphishing Link

RESOURCE DEVELOPMENT
- T1583.001 Acquire Infrastructure: Domains
- T1583.006 Acquire Infrastructure: Web Services
- T1584.001 Compromise Infrastructure: Domains
- T1587.001 Develop Capabilities: Malware
- T1588.002 Obtain Capabilities: Tool

INITIAL ACCESS
- T1566.001 Phishing: Spearphishing Attachment
- T1566.002 Phishing: Spearphishing Link
- T1566.003 Phishing: Spearphishing via Service
- T1190 Exploit Public-Facing Application
- T1133 External Remote Services

EXECUTION
- T1059.001 Command and Scripting Interpreter: PowerShell
- T1059.003 Command and Scripting Interpreter: Windows Command Shell
- T1204.002 User Execution: Malicious File

PERSISTENCE
- T1546.003 Event Triggered Execution: WMI Event Subscription
- T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
- T1505.003 Server Software Component: Web Shell

PRIVILEGE ESCALATION
- T1055 Process Injection
- T1134.001 Access Token Manipulation: Token Impersonation/Theft

DEFENSE EVASION
- T1027 Obfuscated Files or Information
- T1036.005 Masquerading: Match Legitimate Name or Location
- T1070.004 Indicator Removal: File Deletion
- T1112 Modify Registry
- T1140 Deobfuscate/Decode Files or Information
- T1218.005 Signed Binary Proxy Execution: Mshta

CREDENTIAL ACCESS
- T1003.001 OS Credential Dumping: LSASS Memory
- T1003.002 OS Credential Dumping: SAM
- T1003.003 OS Credential Dumping: NTDS
- T1003.004 OS Credential Dumping: LSA Secrets
- T1003.005 OS Credential Dumping: Cached Domain Credentials
- T1056.001 Input Capture: Keylogging
- T1555.003 Credentials from Password Stores: Web Browsers
- T1558.003 Steal or Forge Kerberos Tickets: Kerberoasting

DISCOVERY
- T1087.001 Account Discovery: Local Account
- T1087.002 Account Discovery: Domain Account
- T1082 System Information Discovery
- T1083 File and Directory Discovery
- T1016 System Network Configuration Discovery
- T1018 Remote System Discovery
- T1033 System Owner/User Discovery
- T1057 Process Discovery
- T1069.002 Permission Groups Discovery: Domain Groups
- T1482 Domain Trust Discovery
- T1518.001 Software Discovery: Security Software Discovery

LATERAL MOVEMENT
- T1021.001 Remote Services: Remote Desktop Protocol
- T1021.002 Remote Services: SMB/Windows Admin Shares
- T1021.004 Remote Services: SSH
- T1021.006 Remote Services: Windows Remote Management
- T1550.002 Use Alternate Authentication Material: Pass the Hash
- T1550.003 Use Alternate Authentication Material: Pass the Ticket

COLLECTION
- T1114.002 Email Collection: Remote Email Collection
- T1119 Automated Collection
- T1560.001 Archive Collected Data: Archive via Utility
- T1005 Data from Local System
- T1039 Data from Network Shared Drive

COMMAND AND CONTROL
- T1071.001 Application Layer Protocol: Web Protocols
- T1071.004 Application Layer Protocol: DNS
- T1573.002 Encrypted Channel: Asymmetric Cryptography
- T1090.003 Proxy: Multi-hop Proxy
- T1105 Ingress Tool Transfer
- T1572 Protocol Tunneling
- T1219 Remote Access Software

EXFILTRATION
- T1041 Exfiltration Over C&C Channel
- T1048.003 Exfiltration Over Alternative Protocol: Unencrypted/Obfuscated Non-C&C Protocol
- T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage

IMPACT
- T1486 Data Encrypted for Impact
- T1490 Inhibit System Recovery
- T1489 Service Stop

Total ATT&CK TTPs: 50+ Covering 14 TA

Tactics: 14 | Techniques: 35+ | Sub-techniques: 15+

Coverage: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact, Resource Development, Reconnaissance

4 Tooling & Infrastructure

Custom Backdoors Observed

Name	Type	Description	Year
Karkoff (SUNTIS)	Backdoor	Multi-stage DNS tunneling backdoor. Supports command execution, file operations, and persistent access. Observed in Middle East government and telecommunications sector intrusions.	2014
Jdbrecover (SUNTIS)	Tool/Utility	Custom tool for decrypting Microsoft Jet database (.mdb) files. Used to recover credentials from application databases.	2015
Helminth (SUNTIS)	Backdoor	Multi-protocol backdoor with DNS tunneling, HTTP, and TCP channels. Supports file transfer and remote command execution.	2015
BONDUPDATE (SUNTIS)	Dropper	Dropper used to deliver additional payloads to compromised hosts via scripts. Provides flexible initial access capability.	2015
Clayslide (SUNTIS)	Tool/Utility	Utility for assembling VBA (Visual Basic for Applications) macros into Microsoft Office documents. Used to weaponize phishing lures.	2015
Bondupdater (SUNTIS)	Dropper	Successor dropper to BONDUPDATE. Supports encrypted payloads, anti-sandbox checks, and staged execution. Used against Middle East government targets.	2016
OilBreak (SUNTIS)	RC Backdoor	Remote administration backdoor with encrypted C2 channel. Provides interactive command execution and file transfer.	2016
Karkoff (SUNTIS)	Backdoor	Version 2 of Karkoff. Adds HTTP and HTTPS C2 channels, improved obfuscation, and expanded command set. Used against government and telecommunications targets.	2017
Helminth (SUNTIS)	Backdoor	Version 2 of Helminth. Adds HTTP and HTTPS C2 channels, improved obfuscation, and expanded command set. Used against government and telecommunications targets.	2017
Karkoff (SUNTIS)	Backdoor	Version 3 of Karkoff. Adds DNS over HTTPS (DoH) C2 channel, improved anti-analysis, and expanded command set. Used against Middle East government targets.	2018
Helminth (SUNTIS)	Backdoor	Version 3 of Helminth. Adds DNS over HTTPS (DoH) C2 channel, improved anti-analysis, and expanded command set. Used against Middle East government targets.	2018
SOFTCHECKER	Backdoor	Custom backdoor observed in recent campaigns. Supports file operations and command execution. Limited public reporting.	2023
POWERDOWN (SUNTIS)	Backdoor	Custom PowerShell backdoor. Supports command execution, file operations, and persistence via scheduled tasks. Observed in recent activity.	2023
POWERBOOT	Dropper	Multi-stage PowerShell dropper. Used to deliver POWERDOWN and other payloads. Observed in recent campaigns.	2024

Legitimate Tools Abuse Table

Tool	Purpose	Abuse
Mimikatz (T0100)	Credential dumping	Extracting credentials from memory and LSASS process.
Lazagne (T0106)	Credential recovery	Recovering stored credentials from browsers, mail clients, and applications.
Rubeus (T0208)	Kerberos manipulation	Kerberos ticket manipulation and Kerberoasting.
Sysinternals (T0150)	Various	Various tools used for troubleshooting and system administration. Commonly abused for persistence, lateral movement, and data collection.
LOLBAS (T0174)	Various	Living-off-the-land binaries, scripts, and libraries. Abuse of legitimate Windows binaries for various purposes.
Plink (T0024)	Tunneling	Command-line SSH client. Used for tunneling and remote access.
Nmap (T0199)	Network scanning	Network discovery and port scanning.
PsExec (T0029)	Remote execution	Remote execution and lateral movement.
Invoke-Mimikatz (T0100)	Credential dumping	Mimikatz variant. Credential dumping.
Invoke-Kerbrute (T0208)	Kerberos attacks	Kerberos attacks. Password spraying and enumeration.

Infrastructure Patterns

Pattern	Details
Domain Registration	Typosquatting and look-alike domains. Registrations mimicking legitimate organizations. Use of bulletproof hosting providers. Registrations through resellers to obscure ownership.
Cloud Abuse	Azure/Microsoft 365 for C2 and data exfiltration. Exploitation of misconfigured cloud storage. Use of legitimate cloud services to blend with normal traffic.
Web Shell Persistence	Persistent access via web shells. Observed on Microsoft IIS, Exchange, and Sharepoint servers. Used for long-term access and lateral movement.
Infrastructure Reuse	Infrastructure overlaps with Cobalt Mirage (MuddyWater). Shared hosting providers and infrastructure providers. Infrastructure reuse across campaigns.

5 Notable Campaigns

Dune Spoon (CISA'21)

Dec 2021 | Government | Middle East

APT34 conducted a campaign targeting critical infrastructure of Israel-focused industrial control systems for sabotage or ICS attacks. The group deployed the Dune Backdoor, a custom ICS-aware backdoor, to establish persistence and collect data from Modbus, Siemens S7, and other industrial protocols. The campaign demonstrated APT34's capability to target operational technology environments, not just IT networks, and the group's willingness to pursue destructive outcomes against critical infrastructure.

Spalsec: Jordan Foreign Ministry

Jan 2020 | Government | Jordan, Middle East

APT34 targeted a Jordanian government diplomat with a spearphishing email referencing the Palestine-Israel Peace Initiative. Delivered via a .NET dropper, the payload established persistence through registry modifications and exfiltrated data via encrypted DNS tunneling. Infrastructure included a Jordanian domain registered to a fictitious entity. Attributed with high confidence based on tradecraft, infrastructure, and timing consistent with Iranian state-sponsored operations.

Jerry Wire (CISA'20)

Mar 2020 | Government | Middle East

APT34 used a custom web shell (Jerry Wire) to maintain persistence on Microsoft IIS servers. Used for credential harvesting, lateral movement, and data exfiltration. Observed on government and critical infrastructure servers in the Middle East. Web shell communicated over HTTP/HTTPS with encrypted commands. Long dwell time, indicating patient, low-and-slow operations. Tradecraft consistent with other APT34 campaigns.

SideFoor Variant Campaign

Jan 2019 | Government | Middle East

APT34 operators dropped Remexi malware on a compromised government network. Lateral movement was performed using stolen credentials and PsExec. The campaign was attributed to APT34 with high confidence based on infrastructure overlaps with previous APT34 campaigns, tradecraft consistency, and timing patterns. Long-term persistence was maintained through scheduled tasks and registry modifications.

Large Government Networks

Ongoing | Government | Multinational

APT34 maintains persistent access to multinational government networks. The campaign includes DNS tunneling, credential harvesting, and lateral movement. Accessing government networks, telecommunications, and critical infrastructure. Long-term persistence using custom backdoors and web shells. Operations span multiple years with continuous access maintained. Victims include Middle East and Europe. Attributed with high confidence based on tradecraft, infrastructure, and timing consistent with previous APT34 campaigns.

Earth Simnavaz: UAE Government Campaign

Jan 2021 | Government | Middle East, United Arab Emirates

Turkish threat actor Earth Simnavaz (APT34) targeted a UAE government entity with a custom PowershellDrop backdoor. The campaign used spear-phishing lures with Arabic-themed documents to deliver the backdoor, which supported file operations, process enumeration, and command execution. Infrastructure included compromised legitimate domains and VPS hosting. Attribution was based on infrastructure overlaps, tradecraft similarities, and the Arabic-language lure content targeting a UAE government entity.

Earth Simnavaz (APT34) | Government | Middle East, United Arab Emirates | Jan 2021 | PowershellDrop | Spear-phishing | Custom backdoor | Attribution: Confirmed

Credential Phishing via Microsoft 365

Ongoing | Multinational | Credential Harvesting

APT34 operators use spear-phishing emails with credential harvesting pages mimicking Microsoft 365 sites for credential harvesting, with successful credentials used to access government and critical infrastructure mailboxes. The campaign targets government, telecommunications, and critical infrastructure across the Middle East using compromised Microsoft 365 accounts and focus persistence operations.

Pre-Positioned Infrastructure (Ongoing)

Ongoing | Multinational | Pre-positioning

APT34 is assessed to have created domains and service configurations for future exploitation of accounts registered in the past several months. Infrastructure includes domains registered through resellers to obscure ownership and hosting on bulletproof providers in jurisdictions with limited cooperation. This suggests preparation for future campaigns, potentially against new targets or using previously registered infrastructure for stealth.

6 Detection & Response Recommendations

Detection Opportunities

DNS Tunneling Detection

- High entropy subdomain queries to unusual TLDs
- Sessions TTL > 5 minutes with consistent timing patterns
- DNS query volume spikes from individual endpoints
- Long subdomain labels (>50 characters)
- Connections DNS queries at regular intervals (beacon)

Protocol Anomalies

- DNS over UDP/Microsoft protocol, TCP/TCP/ port 443
- Kerberos TGS requests from workstations
- Unusual Kerberos service ticket requests (kerberoasting)
- Multiple failed authentications followed by success (spraying)

Lateral Movement

- Admin shares (C$, ADMIN$, IPC$) access from workstations
- Remote PowerShell sessions (WinRM)
- Service creation on remote systems
- Scheduled tasks on remote systems

Persistence

- Registry Run keys modification
- Scheduled tasks creation
- Service installation
- WMI event subscriptions

Exfiltration

- Large DNS responses (TXT, CNAME, MX)
- Base64 encoded DNS queries
- Data volume anomalies (baseline deviation)

Hunting Queries Intro Table

Platform	Focus
Splunk	DNS tunneling, Kerberoasting, Lateral movement
Sentinel	Kerberoasting, Lateral movement, Persistence
Elastic	DNS tunneling, Kerberoasting, Lateral movement
Sigma	Platform-agnostic rules

Sample Detection Queries

DNS Tunneling Detection (Splunk SPL)

```
index=dns sourcetype=dns_query
| stats count avg(query_length) as avg_len stdev(query_length) as stdev_len dc(query) as unique_queries by src_ip, domain
| eval entropy=stdev_len/avg_len
| where count > 100 AND entropy > 0.5 AND unique_queries > 50
| table src_ip, domain, count, avg_len, entropy, unique_queries
| sort - count
```

Kerberoasting Detection (Sentinel KQL)

```
SecurityEvent
| where EventID == 4769 and TicketEncryptionType == "0x17"
| where ServiceName !endswith "$"
| summarize count() by TargetUserName, ServiceName, IpAddress, bin(TimeGenerated, 1h)
| where count > 5
```

Lateral Movement Detection (Splunk SPL)

```
index=windows (EventCode=4624 OR EventCode=4625)
| stats count by src_ip, dest, user, EventCode
| eval type=if(EventCode=4624, "success", "failure")
| where count > 10
| table src_ip, dest, user, type, count
```

Persistence Detection (Splunk SPL)

```
index=windows (EventCode=4688 OR EventCode=4698 OR EventCode=4699)
| table _time, EventCode, host, user, CommandLine, TaskName
| sort - _time
```

Kerberoasting Detection (Elastic EQL)

```
sequence by host.name, user.name
[ network where destination.port == 88 and network.protocol == "kerberos" ]
[ kerberos where event.action == "ticket_granted" and kerberos.ticket.encryption_type == "rc4-hmac" ]
```

Lateral Movement Detection (Elastic EQL)

```
sequence by host.name, user.name
[ network where destination.port == 445 ]
[ network where destination.port == 5985 ]
```

Persistence Detection (Elastic EQL)

```
registry where registry.path == "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\*"
```

Sigma Rule (Platform-Agnostic)

```
title: DNS Tunneling Detection
logsource:
  category: dns_query
detection:
  selection:
    query_length: 50
    entropy: 0.5
    count: 100
  timeframe: 1h
```

Kerberoasting Detection (Sigma)

```
title: Kerberoasting Detection
logsource:
  product: windows
  service: security
detection:
  selection:
    EventID: 4769
    TicketEncryptionType: 0x17
    ServiceName: '*$'
  filter:
    ServiceName: '*$'
  condition: selection and not filter
```

Lateral Movement Detection (Sigma)

```
title: Lateral Movement Detection
logsource:
  product: windows
  service: security
detection:
  selection:
    EventID: 4624
    LogonType: 3
    SourceIP: '*'
  filter:
    SourceIP: '127.0.0.1'
  condition: selection and not filter
```

Persistence Detection (Sigma)

```
title: Persistence Detection
logsource:
  product: windows
  service: security
detection:
  selection:
    EventID: 4688
    CommandLine: '*'
  filter:
    CommandLine: '*'
  condition: selection and not filter
```

7 Appendix A: Indicators of Compromise

Stealthy Implant: C File IO Clientfunction

Date: 2018-03-26 | Type: Malware | Source: Intrusiv Threat Research

This implant uses the Microsoft Jet Database Engine (msjet40.dll) to read and write its configuration and command data, rather than using standard file I/O APIs. This technique helps it blend with legitimate database activity.

Tags: T1071, Malware, Windows Administration

Sub-Technique: Sub-1: Implement Application Layer Protocol (T1071.001) — Sub-2: Use Windows Administration Tools (T1059.001)

Sub-3: Scripting: Sub-3: Implement Scripts to run on a victim's machine (T1059.001) — Sub-4: Use Windows Administration Tools (T1059.001)

Sub-5: Command and Control: Sub-5: Implement Command and Control (T1071.001) — Sub-6: Use Windows Administration Tools (T1059.001)

Sub-7: Command and Control: Sub-7: Implement Command and Control (T1071.001) — Sub-8: Use Windows Administration Tools (T1059.001)

Sub-9: Command and Control: Sub-9: Implement Command and Control (T1071.001) —