INTRUVENT

THREAT ACTOR INTELLIGENCE PROFILE

APT33

IRGC Cloud Espionage and Destructive Operations Group / Peach Sandstorm / Refined Kitten

Version 1.0
Last Updated March 18, 2026
Classification TLP:CLEAR
Attribution Confidence HIGH

Intruvent Technologies
INT-TAP-2026-APT33-v1.0

13+

Years of Continuous Espionage Operations Since 2013

Password spraying at scale against cloud infrastructure | Custom backdoors deployed across energy, defense, satellite, and government sectors

1 Attribution & Identity

ATTRIBUTION CONFIDENCE: HIGH

APT33 is assessed with high confidence to be an offensive cyber operations group operating on behalf of Iran's Islamic Revolutionary Guard Corps (IRGC). FireEye (now Mandiant) first publicly attributed the group in September 2017, linking it to operations targeting aviation and energy sectors since 2013. Microsoft, Symantec, CrowdStrike, and Dragos have independently confirmed attribution. The group is tracked by MITRE as G0064. The developer handle "xman_1365_x" appears in PDB paths of TURNEDUP backdoor samples, providing a personnel-level attribution signal. According to FireEye, the actor may have ties to the Nasr Institute, an organization linked to IRGC cyber operations.

Background

APT33 is an Iranian state-sponsored threat group that has conducted espionage and destructive operations since at least 2013. The group targets organizations in the energy, aviation, defense, and government sectors, with primary focus on Saudi Arabia, the United States, South Korea, Israel, and the United Arab Emirates.

APT33's operational profile has evolved significantly over its 13-year history. Early operations (2013-2017) focused on spearphishing with malicious HTA files and custom backdoors (TURNEDUP, DROPSHOT, StoneDrill). Starting in 2023, the group shifted to large-scale password spray campaigns against Azure AD and Microsoft 365 environments, using compromised education sector accounts to establish fraudulent Azure subscriptions for command-and-control infrastructure. This cloud-first approach represents a significant operational evolution from traditional endpoint-based intrusions.

The group maintains links to destructive capability through its association with the StoneDrill wiper (also known as SHAPESHIFT), which shares code with the Shamoon wiper family. While direct APT33 attribution for Shamoon attacks remains contested among vendors, the group's access to wiper technology signals a dual espionage-and-destruction mandate consistent with IRGC tasking.

Known Aliases

`APT33 (Mandiant/FireEye)` `Peach Sandstorm (Microsoft)` `Refined Kitten (CrowdStrike)` `Elfin (Symantec)` `Magnallium (Dragos)` `HOLMIUM (Microsoft, legacy)` `G0064 (MITRE)`

QUICK FACTS

- **Origin:** Iran (IRGC)
- **Active Since:** 2013 (earliest observed)
- **Motivation:** Nation-state espionage; destructive capability
- **Sophistication:** High
- **Last Observed:** July 2024 (Tickler backdoor)
- **Sponsor:** IRGC (Islamic Revolutionary Guard Corps)
- **Signature TTP:** Cloud password spraying + custom backdoors
- **Custom Tools:** Tickler, FalseFont, POWERTON, TURNEDUP, StoneDrill

> *"APT33 has shown particular interest in organizations in the aviation sector involved in both military and commercial capabilities, as well as organizations in the energy sector with ties to petrochemical production."*
>
> FireEye (Mandiant), "APT33: New Insights into Iranian Cyber Espionage Group" (September 2017)

2 Targeting Profile

Industries

- **Energy / Petrochemical** (primary, since 2013)
- **Aviation / Aerospace** (primary, since 2013)
- **Defense Industrial Base** (FalseFont, 2023)
- **Satellite / Space** (2023-2024 campaigns)
- **Government** (federal and state, US and UAE)
- **Communications Equipment** (Tickler, 2024)
- **Oil and Gas** (Tickler, 2024)
- **Higher Education** (infrastructure procurement)
- **Pharmaceutical** (2023 password spray)

Regions

- **Saudi Arabia** (primary, energy sector)
- **United States** (defense, government, energy)
- **South Korea** (energy, petrochemical)
- **Israel** (defense, government)
- **United Arab Emirates** (government, oil/gas)
- **Australia** (education, defense; 2024)

Technologies Targeted

- **Azure AD / Entra ID** (password spraying)
- **Microsoft 365** (credential theft)
- **Azure Subscriptions** (C2 infrastructure)
- **Outlook Web Access** (email harvesting)
- **VPN Gateways** (initial access)
- **Windows Endpoints** (backdoor deployment)
- **Active Directory** (AD snapshots for lateral movement)

Cloud Infrastructure as Operational Platform

APT33 has developed a distinctive operational pattern: compromise education sector accounts with low-cost password spraying, use those accounts to create fraudulent Azure for Students subscriptions, and then repurpose the resulting cloud infrastructure as C2 servers for attacks against high-value defense and energy targets. This approach provides the group with legitimate-looking cloud infrastructure that blends with normal Azure traffic. (Source: Microsoft, August 2024)

3 Tactics, Techniques & Procedures

The following MITRE ATT&CK techniques are documented for APT33 (G0064) from the Intruvent Golden CTI Database, MITRE ATT&CK, and Microsoft Threat Intelligence:

INITIAL ACCESS

- `T1566.001` Spearphishing Attachment
- `T1566.002` Spearphishing Link
- `T1078` Valid Accounts
- `T1078.004` Cloud Accounts KEY

CREDENTIAL ACCESS

- `T1110.003` Password Spraying KEY
- `T1003.001` LSASS Memory (Mimikatz)
- `T1003.004` LSA Secrets
- `T1003.005` Cached Domain Credentials
- `T1552.001` Credentials in Files
- `T1552.006` Group Policy Preferences
- `T1555` Credentials from Password Stores
- `T1555.003` Credentials from Web Browsers

EXECUTION

- `T1059.001` PowerShell
- `T1059.005` Visual Basic
- `T1204.001` Malicious Link
- `T1204.002` Malicious File
- `T1203` Exploitation for Client Execution

PERSISTENCE

- `T1053.005` Scheduled Task
- `T1547.001` Registry Run Keys
- `T1546.003` WMI Event Subscription

DEFENSE EVASION

- `T1027.013` Encrypted/Encoded File
- `T1588.002` Obtain Capabilities: Tool

DISCOVERY

- `T1040` Network Sniffing

COLLECTION & EXFILTRATION

- `T1560.001` Archive via Utility
- `T1048.003` Exfiltration Over Unencrypted Protocol

COMMAND AND CONTROL

- `T1071.001` Web Protocols (HTTP/HTTPS)
- `T1105` Ingress Tool Transfer
- `T1132.001` Standard Encoding
- `T1571` Non-Standard Port
- `T1573.001` Encrypted Channel: Symmetric

IMPACT

- `T1068` Exploitation for Privilege Escalation

Operational Evolution: From Spearphishing to Cloud Abuse

APT33's early campaigns (2013-2019) relied heavily on spearphishing with HTA file attachments and custom backdoors. Starting in 2023, the group pivoted to large-scale password spray campaigns against Azure AD and Microsoft 365 environments. This shift reflects a broader Iranian APT trend toward cloud-focused initial access, allowing the group to bypass traditional endpoint security controls and establish persistent access through legitimate cloud accounts. (Sources: FireEye 2017, Microsoft 2023, Microsoft 2024)

4 Tooling & Infrastructure

Custom Malware Arsenal

Tool	Type	Description	First Seen
TURNEDUP (S0199)	Backdoor	Non-public backdoor that can download/upload files, report system information, and create a reverse shell. Dropped by DROPSHOT. PDB paths contain the handle "xman_1365_x."	2013
DROPSHOT	Dropper	Dropper that delivers TURNEDUP and SHAPESHIFT/StoneDrill. Contains Farsi language artifacts in the binary, supporting Iranian origin.	2016
StoneDrill / SHAPESHIFT (S0380)	Backdoor / Wiper	Dual-purpose tool: backdoor component downloads additional files, wiper component clears the master boot record. Shares code with the Shamoon wiper family. Contains Farsi language artifacts.	2017
POWERTON (S0371)	Backdoor (PowerShell)	PowerShell-based implant using encrypted C2 communications. Supports multiple persistence mechanisms and credential dumping. Delivered via macro-enabled documents.	2018
FalseFont	Backdoor	Custom backdoor targeting the Defense Industrial Base sector. Provides remote access, file launch capabilities, and C2 data exfiltration. First observed November 2023.	Nov 2023
Tickler	Backdoor (multi-stage)	Custom multi-stage backdoor deployed in 2024 campaigns. First stage collects network information and sends it to C2 via HTTP POST. Second stage (sold.dll) adds Trojan dropper functionality, downloads payloads from Azure-hosted C2, enables persistence via batch scripts, and uses DLL sideloading.	Apr 2024
DEADWOOD / Detbosit (S1134)	Wiper	Wiper malware. Links to 2019 Saudi Arabian attacks. Shared across multiple Iranian threat groups.	2019

Open-Source and Dual-Use Tools

Tool	Purpose	Source
Mimikatz (S0002)	LSASS memory dumping for credential harvesting	MITRE G0064; Symantec (2019)
LaZagne (S0349)	Password recovery from local stores (browsers, email clients, databases)	MITRE G0064
Ruler (S0358)	Exchange/Outlook abuse for persistence and command execution via mail rules	MITRE G0064
Empire (S0363)	PowerShell post-exploitation framework for C2 and lateral movement	MITRE G0064
PoshC2 (S0378)	C2 framework used in post-compromise operations	MITRE G0064
PowerSploit (S0194)	PowerShell offensive module collection for privilege escalation and credential access	MITRE G0064
Pupy (S0192)	Cross-platform RAT used for remote access	MITRE G0064
NanoCore (S0336)	Commodity RAT used in early campaigns for remote access and surveillance	MITRE G0064
NETWIRE (S0198)	Commodity RAT used in spearphishing campaigns for remote access	MITRE G0064
AutoIt backdoor (S0129)	AutoIt-scripted backdoor for persistent access	MITRE G0064
AnyDesk / RMM Tools	Remote monitoring and management tools installed post-compromise for persistent access	Microsoft (2024)

Infrastructure

Category	Details	Source
Cloud C2	Fraudulent Azure subscriptions created using compromised education sector accounts (Azure for Students). Attacker-controlled Azure tenants serve as Tickler C2 infrastructure. Outlook email addresses used to register new Azure tenants.	Microsoft (Aug 2024)
Initial Access	Large-scale password spray campaigns targeting Azure AD/Entra ID, Microsoft 365, and Outlook Web Access. Spearphishing with HTA files in earlier campaigns. Job-themed lures for defense and aerospace targets.	FireEye (2017); Microsoft (2023, 2024)
Spearphishing Lures	Recruitment-themed lures targeting aviation and energy sector employees. "Network Security.zip" archive containing Tickler alongside legitimate PDF decoy documents.	FireEye (2017); Microsoft (2024)
Domain Registration	Registered domains mimicking Saudi Arabian aviation and Western energy companies for credential harvesting pages.	FireEye (2017)
Post-Compromise	Active Directory snapshot collection for offline analysis. SMB lateral movement. Installation of RMM tools (AnyDesk and similar) for persistent access.	Microsoft (2023, 2024)

5 Notable Campaigns

Aviation and Energy Sector Espionage

2013-2017

Saudi Arabia · United States · South Korea · Aviation · Energy

APT33's foundational campaign. The group targeted organizations in the aviation and energy sectors across Saudi Arabia, the United States, and South Korea using spearphishing emails with recruitment-themed lures. The group registered domains mimicking Saudi Arabian aviation companies and Western energy firms to host credential harvesting pages. Custom malware including TURNEDUP, DROPSHOT, and StoneDrill was deployed via HTA file attachments. FireEye's September 2017 report was the first public attribution of this activity to Iran. (Source: FireEye, Sept 2017)

StoneDrill / Shamoon Connection

2017-2018

Saudi Arabia · Energy · Destructive

Kaspersky identified StoneDrill in 2017 and documented code overlap with the Shamoon 2 wiper. APT33's DROPSHOT dropper delivered StoneDrill, establishing a link between the espionage group and destructive wiper capability. Direct attribution of Shamoon wiper attacks to APT33 remains contested; Booz Allen Hamilton and other vendors have noted they cannot independently verify APT33 directly executed Shamoon wiping operations. The connection may indicate shared resources or tooling within IRGC-affiliated groups. (Sources: Kaspersky 2017; Booz Allen Hamilton; FireEye 2017)

Attribution Note

The direct link between APT33 and Shamoon wiper operations is not confirmed by all vendors. The association is based on shared code between StoneDrill and Shamoon 2. Some researchers assess that APT33 provides initial access that is then handed off to a separate team for destructive operations.

Symantec "Elfin" Campaign Tracking

2016-2019

Saudi Arabia · United States · Multiple Sectors

Symantec tracked APT33 under the name "Elfin" and documented attacks against at least 50 organizations in Saudi Arabia, the United States, and other countries between 2016 and 2019. Targets included government, research, chemical, engineering, manufacturing, consulting, finance, and telecommunications organizations. Symantec observed the use of commodity RATs (NanoCore, NETWIRE) alongside custom tools (TURNEDUP, POWERTON), and noted the group's exploitation of a WinRAR vulnerability (CVE-2018-20250) shortly after proof-of-concept code became available. (Source: Symantec, March 2019)

Password Spray Campaign (Feb-Jul 2023)

Feb-Jul 2023

United States · Satellite · Defense · Pharmaceutical

Microsoft observed Peach Sandstorm conducting large-scale password spray campaigns against thousands of environments between February and July 2023. The attacks targeted the satellite, defense, and pharmaceutical sectors. Successful compromises led to data theft from a limited number of victims. Post-compromise activity included lateral movement via AzureHound and Roadtools for Azure AD reconnaissance, Active Directory snapshot collection, installation of remote management tools, and credential harvesting using stolen tokens. This campaign marked the group's decisive shift from spearphishing to cloud-focused initial access. (Source: Microsoft, Sept 2023)

FalseFont Backdoor (Defense Industrial Base)

Nov-Dec 2023

Global · Defense Industrial Base

Microsoft identified a new custom backdoor called FalseFont deployed by Peach Sandstorm against the Defense Industrial Base sector worldwide. FalseFont provides remote access, file execution, and C2 data exfiltration capabilities. First use was observed in early November 2023. The backdoor was distributed to defense sector organizations globally, demonstrating APT33's persistent focus on military and defense intelligence collection. (Source: Microsoft, Dec 2023)

Tickler Backdoor Campaign

Apr-Jul 2024

United States · UAE · Satellite · Oil & Gas · Government

Between April and July 2024, Microsoft observed Peach Sandstorm deploying a new custom multi-stage backdoor called Tickler against targets in the satellite, communications equipment, oil and gas, and federal/state government sectors in the United States and UAE. The initial Tickler sample was distributed in an archive named "Network Security.zip" alongside legitimate PDF decoy documents. A second sample (sold.dll) added Trojan dropper functionality with DLL sideloading capabilities.

The group's C2 infrastructure relied on fraudulent Azure subscriptions. APT33 compromised education sector accounts, then created Azure for Students subscriptions within attacker-controlled tenants. These Azure resources served as Tickler's C2 servers. Post-compromise activity included SMB lateral movement, RMM tool installation for persistent access, and Active Directory snapshot collection. (Source: Microsoft, Aug 2024)

6 Detection & Response Recommendations

Detection Opportunities

Cloud Authentication Anomalies

- > High-volume failed sign-in attempts from distributed IPs against Azure AD/Entra ID
- > Password spray patterns: single password tested against many accounts in sequence
- > Successful sign-ins from anomalous locations following spray campaigns
- > New Azure subscription creation from recently compromised accounts
- > Azure for Students subscription creation from non-educational organizational accounts

Tickler / FalseFont Indicators

- > HTTP POST requests sending system/network enumeration data to Azure-hosted endpoints
- > DLL sideloading activity (sold.dll or similar) from unexpected directories
- > Archive files named "Network Security.zip" or similar lure-themed archives
- > Batch scripts establishing persistence for unknown DLLs
- > Unexpected outbound connections to Azure blob storage from non-cloud workloads

Post-Compromise Behaviors

- > Active Directory snapshot creation (ntdsutil, DCSync)
- > Installation of unauthorized RMM tools (AnyDesk, ScreenConnect, etc.)
- > AzureHound or Roadtools execution for Azure AD reconnaissance
- > SMB lateral movement from accounts with recent anomalous sign-in activity
- > Mimikatz, LaZagne, or PowerSploit execution on domain controllers

Legacy Indicators (Spearphishing Era)

- > HTA file execution from email attachments or web downloads
- > POWERTON PowerShell implant activity (encrypted C2, scheduled task persistence)
- > Ruler tool activity against Exchange servers (mail rule abuse)
- > StoneDrill/SHAPESHIFT MBR wiping indicators on endpoints
- > Empire or PoshC2 C2 beaconing patterns

Sample Detection Queries

Password Spray Detection in Azure AD Sign-In Logs (KQL)

DETECTION ONLY

```
// Detect password spray patterns: many accounts, few passwords, distributed failures
// Source: Microsoft Threat Intelligence password spray detection guidance
SigninLogs
| where ResultType == "50126" // Invalid username or password
| summarize
    TargetedAccounts = dcount(UserPrincipalName),
    FailedAttempts = count(),
    DistinctIPs = dcount(IPAddress),
    SampleAccounts = make_set(UserPrincipalName, 5)
    by bin(TimeGenerated, 1h), AppDisplayName
| where TargetedAccounts > 20 and FailedAttempts > 50
| sort by TargetedAccounts desc
```

Tuning Required

Password spray detection generates false positives in large environments with frequent legitimate authentication failures. Adjust the TargetedAccounts and FailedAttempts thresholds to match your baseline. Focus on ResultType 50126 (invalid password) rather than 50034 (user not found) for spray detection.

Anomalous Azure Subscription Creation (KQL)

DETECTION ONLY

```
// Detect new Azure subscription creation from accounts not typically managing subscriptions
// APT33 creates Azure for Students subscriptions from compromised education accounts
AzureActivity
| where OperationNameValue == "Microsoft.Subscription/CreateSubscription/action"
    or OperationNameValue has "subscriptions/write"
| project TimeGenerated, Caller, CallerIpAddress,
    OperationNameValue, ActivityStatusValue, SubscriptionId
| sort by TimeGenerated desc
```

RMM Tool Installation Detection (KQL)

DETECTION ONLY

```
// Detect installation of remote management tools used by APT33 post-compromise
// Source: Microsoft (2024) documents RMM tool deployment in Peach Sandstorm campaigns
DeviceProcessEvents
| where FileName in~ ("AnyDesk.exe", "ScreenConnect.exe",
    "ConnectWise.exe", "TeamViewer.exe", "Splashtop.exe")
    or ProcessCommandLine has_any (
        "anydesk", "screenconnect", "connectwise",
        "teamviewer", "splashtop")
| where InitiatingProcessFileName !in~ ("services.exe", "msiexec.exe")
| project Timestamp, DeviceName, FileName, ProcessCommandLine,
    InitiatingProcessFileName, AccountName
| sort by Timestamp desc
```

False Positive Risk

RMM tools are commonly used by IT departments and managed service providers. Correlate with approved software inventories and focus on installations from unexpected accounts, unusual times, or machines not managed by IT.

Tickler-Style DLL Sideloading Detection (KQL)

DETECTION ONLY

```
// Detect DLL sideloading patterns consistent with Tickler backdoor
// Tickler's second stage (sold.dll) uses DLL sideloading from non-standard paths
DeviceImageLoadEvents
| where FileName endswith ".dll"
| where FolderPath !startswith "C:\\Windows\\"
    and FolderPath !startswith "C:\\Program Files"
    and FolderPath !startswith "C:\\Program Files (x86)"
| where InitiatingProcessFileName !in~ ("explorer.exe", "svchost.exe",
    "services.exe", "RuntimeBroker.exe")
| summarize LoadCount = count(), DLLs = make_set(FileName, 10)
    by DeviceName, InitiatingProcessFileName, FolderPath,
    bin(Timestamp, 1h)
| where LoadCount > 3
| sort by LoadCount desc
```

Active Directory Snapshot / DCSync Detection (KQL)

DETECTION ONLY

```
// Detect Active Directory snapshot collection, a documented APT33 post-compromise activity
// Source: Microsoft (2023, 2024) Peach Sandstorm post-compromise behaviors
DeviceProcessEvents
| where ProcessCommandLine has_any (
    "ntdsutil", "ifm", "create full",
    "secretsdump", "dcsync",
    "ntds.dit", "SYSTEM.hive")
| project Timestamp, DeviceName, FileName,
    ProcessCommandLine, AccountName, InitiatingProcessFileName
| sort by Timestamp desc
```

Mitigation Recommendations

1. **Enforce multi-factor authentication (MFA) on all cloud accounts.** MFA is the single most effective control against APT33's password spray campaigns. Prioritize Azure AD/Entra ID, Microsoft 365, and VPN access. (Source: Microsoft, Sept 2023)
2. **Implement conditional access policies.** Block sign-ins from unexpected geographies, require compliant devices, and enforce risk-based access controls. Monitor for "impossible travel" sign-in events.
3. **Audit Azure subscription creation.** Alert on new subscription creation, particularly Azure for Students subscriptions from organizational accounts. Restrict subscription creation to authorized administrators.
4. **Disable legacy authentication protocols.** APT33 targets protocols that do not support MFA. Disable POP, IMAP, SMTP AUTH, and Exchange ActiveSync where not required.
5. **Deploy credential hygiene controls.** Rotate passwords for accounts that showed authentication anomalies. Implement password protection policies to block common passwords targeted in spray attacks.
6. **Monitor for unauthorized RMM tool installations.** Maintain an approved software inventory and alert on installations of AnyDesk, ScreenConnect, or similar tools outside of change windows.
7. **Review Azure AD/Entra ID sign-in logs regularly.** Establish baselines for authentication patterns. Investigate sign-ins from new locations or devices following periods of elevated failed authentication.
8. **Restrict education sector account privileges.** If your organization includes educational accounts, limit their ability to create Azure subscriptions or tenants.

A Appendix A: Indicators of Compromise

Blocking Guidance: 3-Tier IOC Classification

Tier 1: Block (High Confidence)

All custom malware file hashes listed below (TURNEDUP, POWERTON, StoneDrill, Tickler, FalseFont): Confirmed malicious with no legitimate use case. Safe for hash-based blocking and EDR prevention policies.

Tier 2: Alert / Monitor (Shared Infrastructure)

Azure infrastructure IPs: APT33 uses Azure subscriptions for C2. These IPs belong to Microsoft Azure, a cloud provider used by millions of legitimate organizations. Blocking Azure IP ranges will disrupt legitimate cloud services. Recommend monitoring for specific patterns (unusual Azure blob storage connections from non-cloud workloads) rather than IP-based blocking.

Education sector compromised accounts: Accounts from educational institutions may be compromised for infrastructure procurement. Monitor for anomalous subscription creation from education accounts, but do not block educational IPs or domains at the network level.

Tier 3: Investigate (Unconfirmed)

Password spray source IPs: APT33 distributes spray attacks across many IP addresses. Source IPs may include VPN exit nodes, cloud provider IPs, or residential ISP addresses. Do not block without individual verification. Use sign-in log analysis to identify specific IPs associated with successful compromise rather than all spray source IPs.

Spearphishing domains: Domains mimicking aviation and energy companies may be registered for credential harvesting. Verify domain ownership and registration dates before blocking. Some domains identified in 2017 reporting may no longer be active.

File Indicators

IOC Availability Note

APT33 has been tracked since 2013, but publicly available file hashes are limited in open-source reporting. The indicators below are sourced from published vendor research. Full SHA256 hash sets for Tickler and FalseFont should be obtained from Microsoft Threat Intelligence (MSTIC) publications and may require Microsoft Defender Threat Intelligence (MDTI) access. Tickler hashes published in the August 2024 Microsoft blog were referenced but full SHA256 values were not extractable from the web content accessed during this research session.

Indicator	Type	Context	Source	Confidence
`sold.dll`	Filename	Tickler backdoor second stage; Trojan dropper with DLL sideloading	Microsoft (Aug 2024)	High
`Network Security.zip`	Filename	Archive containing first Tickler sample alongside legitimate PDF decoys	Microsoft (Aug 2024)	High
`xman_1365_x`	PDB Handle	Developer handle found in TURNEDUP backdoor PDB paths	FireEye (Sept 2017)	High

Behavioral Indicators

Indicator	Type	Context	Source
Password spray against Azure AD with ResultType 50126	Behavioral	High-volume failed authentication (20+ accounts/hour) against Azure AD/M365	Microsoft (Sept 2023)
Azure for Students subscription creation from org accounts	Behavioral	Fraudulent Azure subscription creation for C2 infrastructure	Microsoft (Aug 2024)
HTTP POST with system enumeration data to Azure endpoints	Network	Tickler first stage sending hostname, IP, OS version to C2	Microsoft (Aug 2024)
AD snapshot (ntdsutil) followed by RMM tool installation	Behavioral	Post-compromise pattern: AD data collection + persistent access	Microsoft (2023, 2024)
SMB lateral movement from recently compromised cloud accounts	Behavioral	Cloud-to-on-premises pivot using harvested credentials	Microsoft (Aug 2024)

IOCs Requiring Additional Research

The following IOC categories should be obtained from vendor-specific threat intelligence platforms for a complete detection posture:

- **Tickler SHA256 hashes:** Obtain from Microsoft Defender Threat Intelligence (MDTI) portal or the August 2024 MSTIC blog appendix
- **FalseFont file hashes:** Obtain from Microsoft December 2023 advisory details
- **POWERTON file hashes:** Obtain from FireEye/Mandiant APT33 reporting (2018-2019)
- **TURNEDUP file hashes:** Obtain from FireEye September 2017 report appendix
- **Azure C2 tenant IDs:** Microsoft has disrupted known attacker tenants; check MDTI for current indicators

B Appendix B: References

Sources

[1] MITRE ATT&CK, "APT33, HOLMIUM, Elfin, Peach Sandstorm, Group G0064." https://attack.mitre.org/groups/G0064/

[2] FireEye (Mandiant), "APT33: New Insights into Iranian Cyber Espionage Group," September 2017. https://cloud.google.com/blog/topics/threat-intelligence/apt33-insights-into-iranian-cyber-espionage

[3] Microsoft Threat Intelligence, "Peach Sandstorm password spray campaigns enable intelligence collection at high-value targets," September 14, 2023. https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/

[4] Microsoft Threat Intelligence, "Peach Sandstorm deploys new custom Tickler malware in long-running intelligence gathering operations," August 28, 2024. https://www.microsoft.com/en-us/security/blog/2024/08/28/peach-sandstorm-deploys-new-custom-tickler-malware-in-long-running-intelligence-gathering-operations/

[5] Microsoft Threat Intelligence, "Microsoft Warns of New 'FalseFont' Backdoor Targeting the Defense Sector," December 2023. https://thehackernews.com/2023/12/microsoft-warns-of-new-falsefont.html

[6] Symantec Threat Intelligence, "Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S.," March 2019.

[7] Booz Allen Hamilton, "APT33 Hunt Report." https://www.boozallen.com/insights/cyber/tech/apt33-hunt-report.html

[8] MITRE ATT&CK, "TURNEDUP, Software S0199." https://attack.mitre.org/software/S0199/

[9] MITRE ATT&CK, "POWERTON, Software S0371." https://attack.mitre.org/software/S0371/

[10] MITRE ATT&CK, "StoneDrill, Software S0380." https://attack.mitre.org/software/S0380/

[11] Intruvent Technologies, Golden CTI Database (Codex), APT33 full profile. Accessed March 18, 2026.

[12] Brandefense, "APT33/Peach Sandstorm: 2025 Threat Forecast and Analysis of a Cloud-Focused Adversary." https://brandefense.io/blog/apt33-2025-threat-forecast-and-analysis/

[13] Kaspersky Lab, "From Shamoon to StoneDrill," 2017.

TRACK THIS THREAT ACTOR CONTINUOUSLY

BRACE monitors APT33 / Peach Sandstorm and 275+ threat actors with sector-specific intelligence, detection rules, and automated alerting.

✓ Real-time threat actor tracking
✓ Sector-specific risk scoring (ITR)
✓ Detection rules updated with each reporting cycle

See BRACE Plans →

or

Need incident response or forensics support? Contact us at contact@intruvent.com