INTRUVENT

THREAT ACTOR INTELLIGENCE PROFILE

Charming Kitten

APT35 / APT42 / Mint Sandstorm / TA453 (IRGC Intelligence Organization)

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

Intruvent Technologies
INT-TAP-2026-APT35-v1.0

1 Attribution & Identity

STATE SPONSOR: ISLAMIC REPUBLIC OF IRAN

Charming Kitten operates on behalf of the Islamic Revolutionary Guard Corps Intelligence Organization (IRGC-IO). The group conducts long-term, resource-intensive cyber espionage operations targeting government officials, academics, journalists, think tanks, and diaspora communities. MITRE tracks the group under two designations: Magic Hound (G0059) for the broader APT35 cluster and APT42 (G1044) for the Mandiant-defined subset focused on surveillance and social engineering.

`APT35 (Mandiant legacy)` `APT42 (Mandiant)` `Magic Hound (MITRE G0059)` `Charming Kitten (ClearSky)` `Mint Sandstorm (Microsoft)` `Phosphorus (Microsoft legacy)` `TA453 (Proofpoint)` `COBALT ILLUSION (Secureworks)` `Yellow Garuda (PwC)` `ITG18 (IBM X-Force)` `Educated Manticore (Check Point)` `CharmingCypress (Volexity)` `Newscaster (iSIGHT)` `CALANQUE (Google TAG)`

Actor Summary

Charming Kitten is one of Iran's most prolific and operationally mature cyber espionage groups. Active since at least 2014, the group specializes in highly targeted social engineering campaigns that build rapport with victims over weeks or months before delivering malicious payloads or credential-harvesting links. The group's primary mission is intelligence collection against individuals and organizations of strategic interest to the Iranian government, including foreign policy researchers, nuclear security experts, journalists covering the Middle East, and Iranian diaspora activists.

The broader Charming Kitten cluster encompasses two related but distinct operational groups as tracked by Mandiant. APT35 (Magic Hound, MITRE G0059) represents the legacy classification covering credential harvesting, exploitation of public-facing applications, and deployment of custom backdoors such as CharmPower and BellaCiao. APT42 (MITRE G1044) represents a more tightly scoped subset focused on surveillance, social engineering, and mobile device compromise via the PINEFLOWER Android malware. Other vendors (Microsoft, Proofpoint, ClearSky, Secureworks) track the combined activity under unified designations.

Between 2023 and 2026, the group significantly expanded its credential harvesting infrastructure, deploying over 130 phishing domains registered primarily through NameCheap and operating React-based phishing kits capable of real-time MFA token interception. In August 2024, Google TAG publicly attributed APT42 to targeting both the Trump and Biden/Harris presidential campaigns. The group continues to conduct high-tempo operations against Israeli academics, cybersecurity professionals, and journalists.

QUICK REFERENCE

- **Origin:** Iran (IRGC-IO)
- **Active Since:** 2014
- **Motivation:** Espionage, Surveillance
- **MITRE IDs:** G0059, G1044
- **Sophistication:** High
- **Primary Vector:** Social Engineering
- **MFA Bypass:** Real-time Phishing Proxies
- **Target Focus:** Policy, Media, Academia
- **Attribution Confidence:** HIGH

APT35 vs. APT42 Taxonomy

Mandiant distinguishes APT42 (G1044) from the broader Magic Hound / APT35 (G0059) cluster. APT42 focuses on surveillance, credential theft, and social engineering operations. Magic Hound encompasses a wider range of activity including exploitation of public-facing applications, ransomware deployment (T1486), and custom backdoor operations. Both groups are assessed to operate under the IRGC-IO. This profile covers the combined activity set, noting distinctions where relevant. Source: Mandiant, "Uncharmed: Untangling Iran's APT42 Operations" (May 2024); MITRE ATT&CK.

2 Targeting Profile

30+

Countries Targeted Since 2015

Source: Mandiant APT42 Report (May 2024), MITRE ATT&CK G0059/G1044

Priority Sectors

- Think Tanks / Policy Research
- Academia (Middle East Studies)
- Media / Journalism
- Government (Foreign Affairs)
- Defense / Military
- Nuclear Security
- Diaspora / Civil Society
- Cybersecurity Professionals

Priority Geographies

- United States
- Israel
- United Kingdom
- Middle East (broadly)
- Europe (France, Germany)
- Iranian Diaspora (Global)

Individual Targeting Profile

- Policy researchers / analysts
- Journalists covering Iran / Middle East
- University professors
- Current/former government officials
- Political campaign staff
- Human rights activists
- Nuclear negotiation participants

Targeting Driven by IRGC Intelligence Requirements

Charming Kitten's targeting shifts in response to Iranian geopolitical priorities. During nuclear negotiations (JCPOA), the group targeted nuclear policy experts and diplomats. During U.S. elections, the group targeted campaign staff and political consultants. During periods of elevated Iran-Israel tension, the group intensifies operations against Israeli academics, journalists, and cybersecurity professionals. Source: Mandiant (2024), Google TAG (August 2024).

3 Tactics, Techniques & Procedures

The following MITRE ATT&CK techniques have been observed across APT35 (G0059) and APT42 (G1044) operations. Sources include MITRE ATT&CK, Mandiant, Google TAG, Volexity, Proofpoint, Bitdefender, and Microsoft.

RECONNAISSANCE

- `T1589` Gather Victim Identity Info
- `T1589.001` Credentials
- `T1589.002` Email Addresses
- `T1591.001` Determine Physical Locations
- `T1592.002` Client Configs
- `T1595.002` Vulnerability Scanning

RESOURCE DEVELOPMENT

- `T1583.001` Acquire Domains
- `T1583.003` Virtual Private Server APT42
- `T1583.006` Web Services
- `T1584.001` Compromise Domains
- `T1585.001` Social Media Accounts
- `T1585.002` Email Accounts
- `T1586.002` Compromise Email Accounts
- `T1588.002` Obtain Tools
- `T1608.001` Upload Malware APT42

INITIAL ACCESS

- `T1189` Drive-by Compromise
- `T1190` Exploit Public-Facing App
- `T1566.002` Spearphishing Link CORE
- `T1566.003` Spearphishing via Service
- `T1598.003` Spearphishing for Info
- `T1656` Impersonation APT42

EXECUTION

- `T1047` WMI
- `T1053.005` Scheduled Task
- `T1059.001` PowerShell
- `T1059.003` Windows Command Shell
- `T1059.005` Visual Basic
- `T1204.001` Malicious Link
- `T1204.002` Malicious File

CREDENTIAL ACCESS

- `T1003.001` LSASS Memory
- `T1056.001` Keylogging
- `T1111` MFA Interception CORE
- `T1539` Steal Web Session APT42
- `T1555.003` Browser Credentials APT42

PERSISTENCE & DEFENSE EVASION

- `T1036.005` Match Legitimate Name
- `T1070.003` Clear Command History
- `T1070.004` File Deletion
- `T1098.002` Additional Email Delegate
- `T1505.003` Web Shell
- `T1547.001` Registry Run Keys
- `T1564.003` Hidden Window

COLLECTION & EXFILTRATION

- `T1005` Data from Local System
- `T1113` Screen Capture
- `T1114.001` Local Email Collection
- `T1114.002` Remote Email Collection
- `T1530` Cloud Storage Object APT42
- `T1567` Exfil Over Web Service

COMMAND & CONTROL

- `T1071.001` Web Protocols
- `T1090` Proxy
- `T1102.002` Bidirectional C2 via Web
- `T1105` Ingress Tool Transfer
- `T1132.001` Standard Encoding APT42
- `T1572` Protocol Tunneling
- `T1573` Encrypted Channel

Social Engineering Kill Chain

Charming Kitten Social Engineering Attack Flow

Based on Mandiant, Volexity, and Proofpoint reporting (2023-2026)

STEP 1: PERSONA DEVELOPMENT (T1585.001, T1585.002)

- Create fake personas impersonating journalists, academics, think tank researchers, or cybersecurity professionals
- Register email accounts using real names of known individuals at plausible institutions
- Build social media presence and professional profiles to support the persona

↓

STEP 2: TRUST BUILDING (T1598.003, T1656)

- Initiate benign email correspondence over days or weeks; discuss shared research interests
- Use WhatsApp, Signal, or other messaging platforms for follow-up communication
- Send invitations to fake webinars, podcasts, or conferences

↓

STEP 3: PAYLOAD DELIVERY (T1566.002, T1204.001)

- Send credential harvesting link disguised as Google Meet invite, shared document, or conference registration
- Alternatively, deliver malware via RAR archive, LNK file, or poisoned VPN installer
- Links resolve to React-based phishing kits mimicking Gmail, Outlook, or Yahoo login pages

↓

STEP 4: CREDENTIAL THEFT / MFA BYPASS (T1111, T1539)

- Phishing proxy relays credentials and MFA tokens to the real service in real time
- Attacker captures authenticated session cookie before TOTP token expires
- Victim's cloud email, documents, and contacts are accessed and exfiltrated

4 Tooling & Infrastructure

Custom Malware

Name	MITRE ID	Type	Language	First Seen	Source
CharmPower / PowerStar	`S0674`	Modular Backdoor	PowerShell	2022	MITRE ATT&CK; Volexity (2023)
NICECURL	`S1192`	Backdoor	VBScript	January 2024	Mandiant (May 2024)
TAMECAT	`S1193`	Backdoor (toehold)	PowerShell	2024	Mandiant (May 2024)
BellaCiao	N/A	Dropper (DNS-based C2)	.NET	April 2023	Bitdefender (April 2023)
BellaCPP	N/A	Backdoor (SSH tunneling)	C++	December 2024	Kaspersky (December 2024)
BASICSTAR	N/A	Backdoor	Visual Basic	2023	Volexity (February 2024)
PowerLess	`S1012`	Backdoor	PowerShell (.NET)	2022	Cybereason (February 2022)
AnvilEcho	N/A	Intelligence Collection Trojan	PowerShell	August 2024	Proofpoint (August 2024)
BlackSmith Loader	N/A	Malware Loader	Unknown	August 2024	Proofpoint (August 2024)
DownPaper	`S0186`	Downloader	Unknown	2017	MITRE ATT&CK
PINEFLOWER	N/A	Android Surveillance	Android	2019	Mandiant (2024)

Dual-Use and Open-Source Tools

Tool	MITRE ID	Usage	Source
Mimikatz	`S0002`	Credential dumping (LSASS, SAM)	MITRE ATT&CK G0059
Impacket	`S0357`	Lateral movement, remote execution	MITRE ATT&CK G0059
PsExec	`S0029`	Remote process execution	MITRE ATT&CK G0059
Pupy	`S0192`	Cross-platform RAT	MITRE ATT&CK G0059
FRP (Fast Reverse Proxy)	`S1144`	Tunneling and proxy	MITRE ATT&CK G0059
Net / ipconfig / Ping / Systeminfo	`S0039, S0100, S0097, S0096`	Discovery and enumeration	MITRE ATT&CK G0059

Credential Harvesting Infrastructure

Since January 2025, Charming Kitten has operated a large-scale credential harvesting infrastructure consisting of over 130 unique phishing domains and numerous subdomains, most registered through NameCheap. These domains resolve to approximately a dozen IP addresses. The phishing kits are built using React and mimic Google, Microsoft Outlook, and Yahoo login pages with high fidelity. (Source: Google TAG, Mandiant, SecurityAffairs)

The React-based phishing kits include real-time keyloggers that capture credentials as they are typed, and they act as real-time phishing proxies. When a victim enters their password and MFA code on the cloned page, the infrastructure immediately relays those credentials to the legitimate service, captures the authenticated session cookie, and establishes persistence before the time-based OTP (TOTP) expires. Only phishing-resistant MFA methods (FIDO2 security keys, passkeys) are immune to this technique. (Source: Mandiant, Google TAG)

FIDO2 / Passkeys Are the Only Effective MFA Countermeasure

Charming Kitten's real-time phishing proxy infrastructure defeats SMS-based MFA, TOTP authenticator apps, and push notification MFA. The only MFA methods that resist this attack are hardware security keys (FIDO2/WebAuthn) and passkeys, because the cryptographic challenge is bound to the legitimate domain and cannot be relayed. Organizations protecting high-value personnel should mandate FIDO2 enrollment. Source: Google TAG (August 2024), Mandiant (May 2024).

BellaCiao: DNS-Based C2 Mechanism

BellaCiao is a .NET dropper that uses a novel DNS-based command-and-control mechanism. Every 24 hours, the implant performs a DNS resolution for a victim-specific subdomain. The DNS server (controlled by the threat actor) returns an IP address that encodes instructions. The implant compares the resolved IP against hardcoded values to determine which action to take. This approach produces no active C2 traffic that traditional network monitoring can detect. The payload is hardcoded into the executable as malformed base64 strings and decoded only when triggered. (Source: Bitdefender, April 2023)

Each BellaCiao sample is customized per victim and includes hardcoded information such as the company name, target-specific subdomains, and public IP addresses. In December 2024, Kaspersky identified BellaCPP, a C++ variant that implements similar DNS-based C2 but replaces the web shell component with covert SSH tunneling. (Source: Bitdefender 2023, Kaspersky December 2024)

5 Notable Campaigns

Israeli Academics and Cybersecurity Professionals Phishing Campaign

January 2025 - Present

Israel · Academia · Cybersecurity Professionals · Journalists

APT42 operators impersonated cybersecurity professionals to target Israeli academics, journalists, and computer science researchers. The campaign used WhatsApp for initial contact, followed by phishing links to spoofed Google login pages prefilled with victims' email addresses. Over 130 unique phishing domains were identified, most registered through NameCheap, operating React-based phishing kits with real-time MFA token interception. Fake Google Meet invites hosted on Google Sites added legitimacy to the lures. Source: SecurityAffairs (2025), Google TAG.

U.S. Presidential Campaign Targeting

May - June 2024

United States · Political Campaigns · Government Officials

APT42 targeted approximately twelve individuals associated with both the Trump and Biden/Harris presidential campaigns, including current and former government officials, political consultants, and campaign workers. Google TAG detected and publicly attributed the activity in August 2024. The group used credential harvesting phishing pages mimicking Google login portals. Source: Google TAG (August 2024), The Hill.

BlackSmith / AnvilEcho (TA453 Religious Figure Targeting)

August 2024

United States · Religious Leader · Jewish Community

Proofpoint documented TA453 targeting a prominent Jewish religious figure with a fake podcast invitation. The campaign delivered the BlackSmith malware loader, which deployed the AnvilEcho PowerShell trojan. AnvilEcho is a modular intelligence collection tool with capabilities for system reconnaissance, screenshot capture, file download/upload, and data exfiltration via FTP and Dropbox. Source: Proofpoint (August 2024).

CharmingCypress Fake Webinar Campaign

2023 - January 2024

Think Tanks · NGOs · Middle East Policy

Volexity documented CharmingCypress (Charming Kitten) creating a fake webinar platform and requiring targets to install malware-laden VPN applications before granting access. The campaign impersonated the Rasanah International Institute for Iranian Studies and delivered the BASICSTAR backdoor. Targets included Middle East policy researchers and think tank analysts. The group also used RAR archives containing LNK files to deliver NICECURL backdoor payloads masquerading as Harvard feedback forms. Source: Volexity (February 2024), Mandiant (May 2024).

BellaCiao Multi-Country Deployment

2023

United States · Europe · Middle East · India

Bitdefender identified BellaCiao deployments across multiple countries. Each sample was customized for a specific victim organization with hardcoded company names and target-specific DNS subdomains. The malware used DNS-based C2 to avoid network detection. Bitdefender assessed BellaCiao as representing a modernization of Iranian APT malware capabilities. Source: Bitdefender (April 2023).

POWERSTAR / CharmPower Espionage Operations

2022 - 2023

Nuclear Security · Policy Research · Think Tanks

Charming Kitten deployed updated versions of its PowerStar (CharmPower) modular PowerShell backdoor against nuclear security experts and policy researchers. POWERSTAR provides remote command execution, persistence management, screenshot capture, process enumeration, file search, and a cleanup module. The group delivered POWERSTAR through spearphishing emails containing macro-enabled documents. Source: Volexity (2023), GovInfoSecurity (2023).

6 Detection & Response Recommendations

Identity and Access Protection

- > Mandate FIDO2 / passkeys for all high-value accounts (executives, researchers, journalists)
- > Implement Conditional Access policies requiring compliant devices and managed locations
- > Enable continuous access evaluation (CAE) to detect session token replay
- > Monitor for impossible travel alerts in Azure AD / Entra ID sign-in logs
- > Review OAuth application consent grants for suspicious third-party apps
- > Alert on new email forwarding rules or inbox delegation changes

Email and Social Engineering Defense

- > Flag external emails impersonating internal executives or known contacts
- > Implement DMARC/DKIM/SPF enforcement on all organizational domains
- > Train high-risk personnel (researchers, executives) on multi-stage social engineering tactics
- > Alert on login pages hosted on recently registered domains (less than 30 days old)
- > Block or alert on WhatsApp/Signal links in corporate email that redirect to login pages

Endpoint and Malware Detection

- > Hunt for PowerShell modules matching POWERSTAR/CharmPower patterns (modular loader, IPFS C2)
- > Detect VBScript execution chains consistent with NICECURL (LNK to VBS to download)
- > Monitor for DNS queries to subdomains with victim-specific naming (BellaCiao indicator)
- > Alert on macro-enabled documents spawning PowerShell (TAMECAT delivery)
- > Detect SSH tunnel establishment by non-standard processes (BellaCPP indicator)

Network and Cloud Monitoring

- > Monitor for bulk email download or calendar export from cloud mailboxes
- > Alert on cloud storage access from unfamiliar geographic locations
- > Detect abnormal OneDrive/Google Drive exfiltration patterns (large downloads after initial access)
- > Monitor for FRP (Fast Reverse Proxy) or similar tunneling tool usage
- > Inspect DNS traffic for periodic resolution of random-appearing subdomains (BellaCiao C2)

Priority Recommendation for High-Risk Organizations

Organizations in think tanks, academia, media, government foreign affairs, or defense sectors should assume they are targets. The single most effective countermeasure against Charming Kitten is mandating FIDO2/passkey enrollment for all user accounts with access to sensitive information. This nullifies the group's primary attack vector: real-time phishing proxy credential harvesting with MFA token interception.

A Appendix A: Indicators of Compromise

Blocking Guidance: 3-Tier IOC Classification

Tier 1: Block (High Confidence)

Malware file hashes listed below: Confirmed Charming Kitten backdoors and tools with no legitimate use case. Safe for hash-based blocking and EDR prevention policies.

Tier 2: Alert / Monitor (Shared Infrastructure)

Phishing domains: Charming Kitten registers phishing domains through NameCheap and other registrars. Domains may be parked or repurposed. Block confirmed phishing domains at the DNS/proxy level, but monitor newly registered domains rather than blocking entire registrars.

Cloud service IPs: The group abuses Google Sites, Dropbox, and other legitimate cloud services for hosting phishing pages and exfiltrating data. Blocking these services will disrupt legitimate business operations. **Recommend contextual monitoring only.**

Tier 3: Investigate (Unconfirmed)

NameCheap-registered domains: Over 130 domains have been linked to this campaign, but NameCheap hosts millions of legitimate domains. Treat NameCheap registration as contextual enrichment, not an IOC.

VPN/VPS provider IPs: Charming Kitten uses commercial VPN and VPS providers for infrastructure. Blocking provider IP ranges will affect legitimate users. Do not block without verifying against employee/partner usage.

Malware Families

Name	MITRE ID	Type	First Seen	Source
CharmPower / PowerStar	`S0674`	PowerShell Modular Backdoor	2022	MITRE ATT&CK, Volexity
NICECURL	`S1192`	VBScript Backdoor	January 2024	Mandiant (May 2024)
TAMECAT	`S1193`	PowerShell Toehold	2024	Mandiant (May 2024)
BellaCiao	N/A	.NET Dropper (DNS C2)	April 2023	Bitdefender (April 2023)
BellaCPP	N/A	C++ Backdoor (SSH tunneling)	December 2024	Kaspersky (December 2024)
BASICSTAR	N/A	VB Backdoor	2023	Volexity (February 2024)
PowerLess	`S1012`	PowerShell/.NET Backdoor	2022	Cybereason (February 2022)
AnvilEcho	N/A	PowerShell Intelligence Trojan	August 2024	Proofpoint (August 2024)
BlackSmith	N/A	Malware Loader	August 2024	Proofpoint (August 2024)
DownPaper	`S0186`	Downloader	2017	MITRE ATT&CK
PINEFLOWER	N/A	Android Spyware	2019	Mandiant (2024)

IOCs Requiring Verification

The following vendor reports contain additional IOCs (file hashes, domains, IPs) that should be obtained directly from the original publications:

- **Mandiant** (cloud.google.com): SHA256 hashes for NICECURL, TAMECAT; C2 domains and phishing infrastructure
- **Volexity** (volexity.com): SHA256 hashes for BASICSTAR, POWERSTAR; phishing domains and VPN installer hashes; YARA rules available on GitHub
- **Proofpoint** (proofpoint.com): SHA256 hashes and IOCs for BlackSmith loader and AnvilEcho trojan
- **Bitdefender** (bitdefender.com): SHA256 hashes for BellaCiao samples, victim-specific DNS subdomains, C2 infrastructure
- **Google TAG**: 130+ phishing domain list from the 2025 credential harvesting campaign

B Appendix B: References

MITRE ATT&CK

MITRE ATT&CK: Magic Hound (G0059) - Primary MITRE group profile for APT35/Charming Kitten

MITRE ATT&CK: APT42 (G1044) - MITRE group profile for APT42 subset

MITRE ATT&CK: CharmPower (S0674) - PowerShell modular backdoor

MITRE ATT&CK: NICECURL (S1192) - VBScript backdoor

MITRE ATT&CK: TAMECAT (S1193) - PowerShell toehold

Mandiant / Google Threat Intelligence

Mandiant (May 2024): "Uncharmed: Untangling Iran's APT42 Operations" - Comprehensive APT42 profile with NICECURL and TAMECAT analysis

Mandiant (2022): "APT42: Crooked Charms, Cons, and Compromises" - Initial APT42 designation and operational analysis

Google TAG (August 2024): APT42 targeting of U.S. presidential campaigns (Trump and Biden/Harris)

Volexity

Volexity (February 2024): "CharmingCypress: Innovating Persistence" - BASICSTAR backdoor, fake webinar platform, VPN app malware

Proofpoint

Proofpoint (August 2024): "Best Laid Plans: TA453 Targets Religious Figure with Fake Podcast Invite Delivering New BlackSmith Malware Toolset" - BlackSmith loader and AnvilEcho trojan analysis

Bitdefender

Bitdefender (April 2023): "Unpacking BellaCiao: A Closer Look at Iran's Latest Malware" - BellaCiao DNS-based C2 mechanism analysis

Other Vendor Research

SecurityAffairs (2025): "APT42 impersonates cyber professionals to phish Israeli academics and journalists" - 130+ domain campaign details

CyberScoop: "Iranian hackers impersonate journalists in social engineering campaign" - Social engineering tradecraft

The Hacker News (May 2024): "APT42 Hackers Pose as Journalists to Harvest Credentials and Access Cloud Data" - Credential harvesting and cloud access

The Hacker News (June 2023): "Iranian Hackers Using POWERSTAR Backdoor in Targeted Espionage Attacks" - POWERSTAR analysis

CyberSRC (December 2024): "Iran's Charming Kitten Deploys BellaCPP" - BellaCPP C++ variant analysis

Intruvent Golden CTI Database (Codex) - Actor profiles for Magic Hound (G0059) and APT42 (G1044)

TRACK THIS THREAT ACTOR CONTINUOUSLY

BRACE monitors APT35 / Charming Kitten 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