Magic Hound, APT 35, Cobalt Illusion, Charming Kitten

Archived: 2026-04-05 23:06:55 UTC

APT group: Magic Hound, APT 35, Cobalt Illusion, Charming Kitten

Names	Magic Hound *(Palo Alto)* APT 35 *(Mandiant)* Cobalt Illusion *(SecureWorks)* Cobalt Mirage *(SecureWorks)* Charming Kitten *(CrowdStrike)* TEMP.Beanie *(FireEye)* Timberworm *(Symantec)* Tarh Andishan *(Cylance)* TA453 *(Proofpoint)* Phosphorus *(Microsoft)* TunnelVision *(SentinelOne)* UNC788 *(FireEye)* Yellow Garuda *(PWC)* Educated Manticore *(Check Point)* Mint Sandstorm *(Microsoft)* Ballistic Bobcat *(ESET)* CharmingCypress *(Volexity)* Agent Serpens *(Palo Alto)* G0058 *(MITRE)* G0059 *(MITRE)*
Country	Iran
Sponsor	State-sponsored, Islamic Revolutionary Guard Corps (IRGC)
Motivation	Information theft and espionage
First seen	2012
Description	Magic Hound is an Iranian-sponsored threat group operating primarily in the Middle East that dates back as early as 2014. The group behind the campaign has primarily targeted organizations in the energy, government, and technology sectors that are either based or have business interests in Saudi Arabia. Magic Hound has 2 subgroups: 1. Subgroup: DEV-0270, Nemesis Kitten 2. Subgroup: TA455, Smoke Sandstorm

	This group appears to be the evolvement of Cutting Kitten, TG-2889. There is some infrastructure overlap with Rocket Kitten, Newscaster, NewsBeef, ITG18 and APT 42.	
Observed	Sectors: Defense, Education, Energy, Financial, Government, Healthcare, IT, Manufacturing, NGOs, Oil and gas, Technology, Telecommunications and that are either based or have business interests in Saudi Arabia, and ClearSky, HBO, civil and human rights activists and journalists. Countries: Afghanistan, Belgium, Brazil, Canada, Egypt, France, Iran, Iraq, Israel, Jordan, Kuwait, Morocco, Pakistan, Saudi Arabia, Spain, Syria, Turkey, UAE, UK, USA, Venezuela, Yemen and Gaza.	
Tools used	7-Zip, AnvilEcho, BASICSTAR, BlackSmith, ChromeHistoryView, CommandCam, CWoolger, DistTrack, DownPaper, FireMalv, FRP, Ghambar, GoProxy, Havij, HYPERSCRAPE, Leash, Matryoshka RAT, MediaPl, Mimikatz, MischiefTut, MPKBot, NETWoolger, NOKNOK, PINEFLOWER, PowerLess Backdoor, POWERSTAR, RATHOLE, PsList, PupyRAT, Sponsor, sqlmap, TDTESS, WinRAR.	
Operations performed	Mid-2014	Operation “Thamar Reservoir” This report reviews an ongoing cyber-attack campaign dating back to mid-2014. Additional sources indicate it may date as far back as 2011. We call this campaign Thamar Reservoir, named after one of the targets, Thamar E. Gindin, who exposed new information about the attack and is currently assisting with the investigation. <https://www.clearskysec.com/thamar-reservoir/>
	2016	Unit 42 has discovered a persistent attack campaign operating primarily in the Middle East dating back to at least mid-2016 which we have named Magic Hound. This appears to be an attack campaign focused on espionage. Based upon our visibility it has primarily targeted organizations in the energy, government, and technology sectors that are either based or have business interests in Saudi Arabia. The adversaries appear to have evolved their tactics and techniques throughout the tracked time-period, iterating through a diverse toolset across different waves of attacks. <https://unit42.paloaltonetworks.com/unit42-magic-hound-campaign-attacks-saudi-targets/>
	Jan 2017	PupyRAT campaign SecureWorks Counter Threat Unit (CTU) researchers analyzed a phishing campaign that targeted a Middle Eastern organization in early January 2017. Some of messages were sent from legitimate

	email addresses belonging to several Middle Eastern organizations. <https://www.secureworks.com/blog/iranian-pupyrat-bites-middle-eastern-organizations>
2017	In early 2017, SecureWorks Counter Threat Unit (CTU) researchers observed phishing campaigns targeting several entities in the Middle East and North Africa (MENA), with a focus on Saudi Arabian organizations. The campaigns delivered PupyRAT, an open-source cross-platform remote access Trojan. <https://www.secureworks.com/research/the-curious-case-of-mia-ash>
Jun 2018	Impersonating ClearSky, the security firm that uncovered its campaigns Iranian cyberespionage group Charming Kitten, which has been operating since 2014, has impersonated the cybersecurity firm that exposed its operations and campaigns. Israeli firm ClearSky Security said the group managed to copy its official website hosted on a similar-looking domain – clearskysecurity[.]net. ClearSky's actual website is Clearskysec.com. <https://cyware.com/news/iranian-apt-charming-kitten-impersonates-clearsky-the-security-firm-that-uncovered-its-campaigns-7fea0b4f>
Aug 2017	Breach of HBO On August 7 a small treasure trove of HBO content was posted publicly to the web by a hacker who is now demanding a $6 million payment to stop any further release of data. The hacker who goes by Mr. Smith posted five scripts for Game of Thrones and a month's worth of email from HBO Vice President for Film Programming Leslie Cohen along with some other corporate information, according to the Associated Press. <https://www.scmagazine.com/home/security-news/cybercrime/hbo-breach-accomplished-with-hard-work-by-hacker-poor-security-practices-by-victim/>
Oct 2018	The Return of The Charming Kitten In this campaign, hackers have targeted individuals who are involved in economic and military sanctions against the Islamic Republic of Iran as well as politicians, civil and human rights activists and journalists around the world. Our review in Certfa demonstrates that the hackers – knowing that their victims use two-step verification – target verification codes and also their email accounts such as Yahoo! And Gmail. <https://blog.certfa.com/posts/the-return-of-the-charming-kitten/>

Jul 2019	In August, the campaign has progressed, and unlike July, it seems like the APT group is now expanding its activities toward influential public figures around the world, rather than academic researchers state organizations. <https://www.clearskysec.com/the-kittens-are-back-in-town/>
Aug 2019	In a 30-day period between August and September, the Microsoft Threat Intelligence Center (MSTIC) observed Phosphorus making more than 2,700 attempts to identify consumer email accounts belonging to specific Microsoft customers and then attack 241 of those accounts. <https://blogs.microsoft.com/on-the-issues/2019/10/04/recent-cyberattacks-require-us-all-to-be-vigilant/> <https://www.clearskysec.com/wp-content/uploads/2019/10/The-Kittens-Are-Back-in-Town-2.pdf>
Jan 2020	Fake Interview: The New Activity of Charming Kitten <https://blog.certfa.com/posts/fake-interview-the-new-activity-of-charming-kitten/>
Jun 2020	APT35 ‘Charming Kitten' discovered in a pre-infected environment <https://www.darktrace.com/en/blog/apt-35-charming-kitten-discovered-in-a-pre-infected-environment/>
Jul 2020	Starting July 2020, we have identified a new TTP of the group, impersonating “DeutscheWelle” and the “Jewish Journal” using emails alongside WhatsApp messages as their main platform to approach the target and convince them to open a malicious link. <https://www.clearskysec.com/wp-content/uploads/2020/08/The-Kittens-are-Back-in-Town-3.pdf>
Aug 2020	New cyberattacks targeting U.S. elections <https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/>
Late 2020	Operation “BadBlood” BadBlood: TA453 Targets US and Israeli Medical Research Personnel in Credential Phishing Campaigns <https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential>
Late 2020	Would’ve, Could’ve, Should’ve…Did: TA453 Refuses to be Bound by Expectations <https://www.proofpoint.com/us/blog/threat-insight/ta453-refuses-be-bound-expectations>

Dec 2020	During the Christmas holidays and the beginning of the new year, the Charming Kitten group, the Iranian state-backed hackers, have begun a targeted phishing campaign of espionage against different individuals to collect information. <https://blog.certfa.com/posts/charming-kitten-christmas-gift/>
Jan 2021	Operation “SpoofedScholars” TA453, an Iranian-state aligned actor, masqueraded as British scholars to covertly target individuals of intelligence interest to the Iranian government in what Proofpoint has dubbed Operation SpoofedScholars. <https://www.proofpoint.com/us/blog/threat-insight/operation-spoofedscholars-conversation-ta453>
Late 2021	PowerLess Trojan: Iranian APT Phosphorus Adds New PowerShell Backdoor for Espionage <https://www.cybereason.com/blog/powerless-trojan-iranian-apt-phosphorus-adds-new-powershell-backdoor-for-espionage>
Dec 2021	Iranian Spear Phishing Operation Targets Former Israeli Foreign Minister, Former US Ambassador to Israel, Former Israeli Army General and Three other High-Profile Executives <https://blog.checkpoint.com/2022/06/14/iranian-spear-phishing-operation-targets-former-israeli-foreign-minister-former-us-ambassador-to-israel-former-israeli-army-general-and-three-other-high-profile-executives/>
Dec 2021	Log4Shell attacks expand to nation-state groups from China, Iran, North Korea, and Turkey <https://therecord.media/log4shell-attacks-expand-to-nation-state-groups-from-china-iran-north-korea-and-turkey/>
Dec 2021	New Iranian APT data extraction tool <https://blog.google/threat-analysis-group/new-iranian-apt-data-extraction-tool/>
Jan 2022	APT35 exploits Log4j vulnerability to distribute new modular PowerShell toolkit <https://research.checkpoint.com/2022/apt35-exploits-log4j-vulnerability-to-distribute-new-modular-powershell-toolkit/>
Jan 2022	COBALT MIRAGE Conducts Ransomware Operations in U.S. <https://www.secureworks.com/blog/cobalt-mirage-conducts-ransomware-operations-in-us>

Feb 2022	Iranian-Aligned Threat Actor “TunnelVision” Actively Exploiting VMware Horizon <https://www.sentinelone.com/labs/log4j2-in-the-wild-iranian-aligned-threat-actor-tunnelvision-actively-exploiting-vmware-horizon/>
Early 2022	Tracing State-Aligned Activity Targeting Journalists, Media <https://www.proofpoint.com/us/blog/threat-insight/above-fold-and-your-inbox-tracing-state-aligned-activity-targeting-journalists>
May 2022	Iranian Threat Actor Continues to Develop Mass Exploitation Tools <https://www.deepinstinct.com/blog/iranian-threat-actor-continues-to-develop-mass-exploitation-tools>
May 2022	Operation “Sponsoring Access” Sponsor with batch-filed whiskers: Ballistic Bobcat’s scan and strike backdoor <https://www.welivesecurity.com/en/eset-research/sponsor-batch-filed-whiskers-ballistic-bobcats-scan-strike-backdoor/>
Jun 2022	Opsec Mistakes Reveal COBALT MIRAGE Threat Actors <https://www.secureworks.com/blog/opsec-mistakes-reveal-cobalt-mirage-threat-actors>
Mid 2022	TA453 Uses Multi-Persona Impersonation to Capitalize on FOMO <https://www.proofpoint.com/us/blog/threat-insight/ta453-uses-multi-persona-impersonation-capitalize-fomo>
2023	Nation-state threat actor Mint Sandstorm refines tradecraft to attack high-value targets <https://www.microsoft.com/en-us/security/blog/2023/04/18/nation-state-threat-actor-mint-sandstorm-refines-tradecraft-to-attack-high-value-targets/>
2023	CharmingCypress: Innovating Persistence <https://www.volexity.com/blog/2024/02/13/charmingcypress-innovating-persistence/>
Mar 2023	Iranian Hackers Target Women Involved in Human Rights and Middle East Politics <https://thehackernews.com/2023/03/iranian-hackers-target-women-involved.html>
Mar 2023	Educated Manticore – Iran Aligned Threat Actor Targeting Israel via Improved Arsenal of Tools

		<https://research.checkpoint.com/2023/educated-manticore-iran-aligned-threat-actor-targeting-israel-via-improved-arsenal-of-tools/>
	May 2023	Microsoft: Iranian hacking groups join Papercut attack spree <https://www.bleepingcomputer.com/news/security/microsoft-iranian-hacking-groups-join-papercut-attack-spree/>
	May 2023	Charming Kitten Updates POWERSTAR with an InterPlanetary Twist <https://www.volexity.com/blog/2023/06/28/charming-kitten-updates-powerstar-with-an-interplanetary-twist/>
	Aug 2023	Iranian cyber spies are targeting dissidents in Germany, warns intelligence service <https://therecord.media/charming-kitten-iran-targets-dissidents-in-germany>
	Nov 2023	New TTPs observed in Mint Sandstorm campaign targeting high-profile individuals at universities and research orgs <https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/>
	Jul 2024	Best Laid Plans: TA453 Targets Religious Figure with Fake Podcast Invite Delivering New BlackSmith Malware Toolset <https://www.proofpoint.com/us/blog/threat-insight/best-laid-plans-ta453-targets-religious-figure-fake-podcast-invite-delivering>
	Feb 2025	Iranian Cyber Actors Impersonate Model Agency in Suspected Espionage Operation <https://unit42.paloaltonetworks.com/iranian-attackers-impersonate-model-agency/>
	Jun 2025	Educated Manticore Reemerges: Iranian Spear-Phishing Campaign Targeting High-Profile Figures <https://blog.checkpoint.com/security/educated-manticore-reemerges-iranian-spear-phishing-campaign-targeting-high-profile-figures/>
Counter operations	Feb 2019	Former U.S. Counterintelligence Agent Charged With Espionage on Behalf of Iran; Four Iranians Charged With a Cyber Campaign Targeting Her Former Colleagues <https://www.justice.gov/opa/pr/former-us-counterintelligence-agent-charged-espionage-behalf-iran-four-iranians-charged-cyber>
	Mar 2019	Microsoft slaps down 99 APT35/Charming Kitten domains <https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/>

	Oct 2021	Countering threats from Iran <https://blog.google/threat-analysis-group/countering-threats-iran/>
	Early 2022	We took action against a group of hackers from Iran, known in the security industry as UNC788. <https://about.fb.com/wp-content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf>
	Sep 2022	Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity <https://home.treasury.gov/news/press-releases/jy0948>>
	Aug 2024	Taking Action Against Malicious Accounts in Iran <https://about.fb.com/news/2024/08/taking-action-against-malicious-accounts-in-iran/>
Information	<https://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf> <https://en.wikipedia.org/wiki/Charming_Kitten> <https://vblocalhost.com/uploads/VB2021-Haeghebaert.pdf> <https://therecord.media/the-not-so-charming-kitten-working-for-iran/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0058/> <https://attack.mitre.org/groups/G0059/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
