OilRig, APT 34, Helix Kitten, Chrysene

Archived: 2026-04-05 16:30:02 UTC

APT group: OilRig, APT 34, Helix Kitten, Chrysene

Names	OilRig *(Palo Alto)* APT 34 *(FireEye)* Helix Kitten *(CrowdStrike)* Twisted Kitten *(CrowdStrike)* Crambus *(Symantec)* Chrysene *(Dragos)* Cobalt Gypsy *(SecureWorks)* TA452 *(Proofpoint)* IRN2 *(Area 1)* ATK 40 *(Thales)* ITG13 *(IBM)* DEV-0861 *(?)* EUROPIUM *(Microsoft)* Hazel Sandstorm *(Microsoft)* Scarred Manticore *(Check Point)* Evasive Serpens *(Palo Alto)* Yellow Maero *(PWC)* Storm-0861 *(Microsoft)* UNC1860 *(Mandiant)* Earth Simnavaz *(Trend Micro)* G0049 *(MITRE)*
Country	Iran
Sponsor	State-sponsored, Ministry of Intelligence and Security (MOIS)
Motivation	Information theft and espionage
First seen	2014
Description	OilRig is a threat group with suspected Iranian origins that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East. It appears the group carries out supply chain attacks, leveraging the trust relationship

	between organizations to attack their primary targets. FireEye assesses that the group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests. This group was previously tracked under two distinct groups, APT 34 and OilRig, but was combined due to additional reporting giving higher confidence about the overlap of the activity. OilRig has 1 subgroup: 1. Subgroup: Greenbug, Volatile Kitten OilRig seems to be closely related to APT 33, Elfin, Magnallium since at least 2017 and perhaps DNSpionage. They also seem to overlap with Hexane. Also see HomeLand Justice and Orangeworm.	
Observed	Sectors: Aviation, Chemical, Defense, Education, Energy, Financial, Government, High-Tech, IT, Hospitality, Oil and gas, Telecommunications. Countries: Albania, Azerbaijan, Bahrain, China, Egypt, Iraq, Israel, Jordan, Kuwait, Lebanon, Mauritius, Oman, Pakistan, Qatar, Saudi Arabia, Turkey, UAE, UK, USA.	
Tools used	Alma Communicator, BONDUPDATER, certutil, Clayslide, DistTrack, DNSExfitrator, DNSpionage, Dustman, Fox Panel, GoogleDrive RAT, Helminth, ISMAgent, ISMDoor, ISMInjector, Jason, Karkoff, LaZagne, LIONTAIL, LONGWATCH, Mimikatz, MrPerfectInstaller, Nautilus, Neuron, OilRig, OopsIE, PICKPOCKET, Plink, POWBAT, PowerExchange, POWRUNER, PsList, QUADAGENT, RDAT, RGDoor, Saitama, SideTwist, SpyNote RAT, StoneDrill, ThreeDollars, TONEDEAF, TONEDEAF 2.0, TwoFace, VALUEVAULT, Webmask, WinRAR, ZeroCleare, Living off the Land.	
Operations performed	Aug 2012	Shamoon Attacks W32.Disttrack is a new threat that is being used in specific targeted attacks against at least one organization in the energy sector. It is a destructive malware that corrupts files on a compromised computer and overwrites the MBR (Master Boot Record) in an effort to render a computer unusable. Target: Saudi Aramco and Rasgas. <https://www.symantec.com/connect/blogs/shamoon-attacks>
	May 2016	Targeted Attacks against Banks in the Middle East In the first week of May 2016, FireEye's DTI identified a wave of emails containing malicious attachments being sent to multiple banks in the Middle East region. The threat actors appear to be performing initial reconnaissance against would-be targets, and the attacks caught our attention since they were using unique scripts not commonly seen

	in crimeware campaigns. <https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksaga.html> <https://unit42.paloaltonetworks.com/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/>
Jun 2016	We have identified two separate testing efforts carried out by the OilRig actors, one occurring in June and one in November of 2016. The sample set associated with each of these testing activities is rather small, but the changes made to each of the files give us a chance to understand what modifications the actor performs in an attempt to evade detection. This testing activity also suggests that the threat group responsible for the OilRig attack campaign have an organized, professional operations model that includes a testing component to the development of their tools. <https://unit42.paloaltonetworks.com/unit42-oilrig-actors-provide-glimpse-development-testing-efforts/>
Oct 2016	In recent weeks we've discovered that the group have been actively updating their Clayslide delivery documents, as well as the Helminth backdoor used against victims. Additionally, the scope of organizations targeted by this group has expanded to not only include organizations within Saudi Arabia, but also a company in Qatar and government organizations in Turkey, Israel and the United States. <https://unit42.paloaltonetworks.com/unit42-oilrig-malware-campaign-updates-toolset-and-expands-targets/>
Nov 2016	Shamoon v2 The malware used in the recent attacks (W32.Disttrack.B) is largely unchanged from the variant used four years ago. In the 2012 attacks, infected computers had their master boot records wiped and replaced with an image of a burning US flag. The latest attacks instead used a photo of the body of Alan Kurdi, the three year-old Syrian refugee who drowned in the Mediterranean last year. <https://www.symantec.com/connect/blogs/shamoon-back-dead-and-destructive-ever> <https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/> <https://unit42.paloaltonetworks.com/unit42-second-wave-shamoon-2-attacks-identified/>
Jan 2017	Delivers Digitally Signed Malware, Impersonates University of Oxford In recent attacks they set up a fake VPN Web Portal and targeted at

	least five Israeli IT vendors, several financial institutes, and the Israeli Post Office. Later, the attackers set up two fake websites pretending to be a University of Oxford conference sign-up page and a job application website. In these websites they hosted malware that was digitally signed with a valid, likely stolen code signing certificate. <https://www.clearskysec.com/oilrig/>
Jun 2017	In July 2017, we observed the OilRig group using a tool they developed called ISMAgent in a new set of targeted attacks. The OilRig group developed ISMAgent as a variant of the ISMDoor Trojan. In August 2017, we found this threat group has developed yet another Trojan that they call 'Agent Injector' with the specific purpose of installing the ISMAgent backdoor. We are tracking this tool as ISMInjector. <https://unit42.paloaltonetworks.com/unit42-oilrig-group-steps-attacks-new-delivery-documents-new-injector-trojan/>
Jul 2017	The web server logs on the system we examined that was compromised with the TwoFace shell gave us a glimpse into the commands the actor executed through their malware. These commands also enabled us to create a profile of the actor, specifically their intentions and the tools and techniques used to carry out their operation. <https://unit42.paloaltonetworks.com/unit42-twoface-webshell-persistent-access-point-lateral-movement/>
Sep 2017	While expanding our research into the TwoFace webshell from this past July, we were able to uncover several IP addresses that logged in and directly interfaced with the shell we discovered and wrote about. Investigating deeper into these potential adversary Ips revealed a much larger infrastructure used to execute the attacks. <https://unit42.paloaltonetworks.com/unit42-striking-oil-closer-look-adversary-infrastructure/>
Nov 2017	New Targeted Attack in the Middle East In this latest campaign, APT34 leveraged the recent Microsoft Office vulnerability CVE-2017-11882 to deploy POWRUNER and BONDUPDATER. <https://www.fireeye.com/blog/threat-research/2017/12/targeted-attack-in-middle-east-by-apt34.html>
Jan 2018	On January 8, 2018, Unit 42 observed the OilRig threat group carry out an attack on an insurance agency based in the Middle East. Just

	over a week later, on January 16, 2018, we observed an attack on a Middle Eastern financial institution. In both attacks, the OilRig group attempted to deliver a new Trojan that we are tracking as OopsIE. The January 8 attack used a variant of the ThreeDollars delivery document, which we identified as part of the OilRig toolset based on attacks that occurred in August 2017. <https://unit42.paloaltonetworks.com/unit42-oopsie-oilrig-uses-threedollars-deliver-new-trojan/>
Jan 2018	While investigating files uploaded to a TwoFace webshell, Unit 42 discovered actors installing an Internet Information Services (IIS) backdoor that we call RGDoor. Our data suggests that actors have deployed the RGDoor backdoor on webservers belonging to eight Middle Eastern government organizations, as well as one financial and one educational institution. <https://unit42.paloaltonetworks.com/unit42-oilrig-uses-rgdoor-iis-backdoor-targets-middle-east/>
May 2018	Technology Service Provider and Government Agency Between May and June 2018, Unit 42 observed multiple attacks by the OilRig group appearing to originate from a government agency in the Middle East. Based on previously observed tactics, it is highly likely the OilRig group leveraged credential harvesting and compromised accounts to use the government agency as a launching platform for their true attacks. <https://unit42.paloaltonetworks.com/unit42-oilrig-targets-technology-service-provider-government-agency-quadagent/>
Dec 2018	Shamoon v3 After a two-year absence, the destructive malware Shamoon (W32.Disttrack.B) re-emerged on December 10 in a new wave of attacks against targets in the Middle East. These latest Shamoon attacks are doubly destructive, since they involve a new wiper (Trojan.Filerase) that deletes files from infected computers before the Shamoon malware wipes the master boot record. <https://www.symantec.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail> <https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/shamoon-attackers-employ-new-tool-kit-to-wipe-infected-systems/>
Jun 2019	[W]e identified three new malware families and a reappearance of PICKPOCKET, malware exclusively observed in use by APT34. The new malware families, which we will examine later in this post, show

	APT34 relying on their PowerShell development capabilities, as well as trying their hand at Golang. <https://www.fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html>
Dec 2019	New Destructive Wiper ZeroCleare Targets Energy Sector in the Middle East <https://securityintelligence.com/posts/new-destructive-wiper-zerocleare-targets-energy-sector-in-the-middle-east/>
Jan 2020	Our researchers Paul Litvak and Michael Kajilolti have discovered a new campaign conducted by APT34 employing an updated toolset. Based on uncovered phishing documents, we believe this Iranian actor is targeting Westat employees, or United States organizations hiring Westat services. <https://intezer.com/blog-new-iranian-campaign-tailored-to-us-companies-uses-updated-toolset/>
Mar 2020	Karkoff 2020: a new APT34 espionage operation involves Lebanon Government <https://blog.yoroi.company/research/karkoff-2020-a-new-apt34-espionage-operation-involves-lebanon-government/>
Apr 2020	While analyzing an attack against a Middle Eastern telecommunications organization, we discovered a variant of an OilRig-associated tool we call RDAT using a novel email-based command and control (C2) channel that relied on a technique known as steganography to hide commands and data within bitmap images attached to emails. <https://unit42.paloaltonetworks.com/oilrig-novel-c2-channel-steganography/>
Jan 2021	Iran’s APT34 Returns with an Updated Arsenal <https://research.checkpoint.com/2021/irans-apt34-returns-with-an-updated-arsenal/>
2021	OilRig’s Outer Space and Juicy Mix: Same ol’ rig, new drill pipes <https://www.welivesecurity.com/en/eset-research/oilrigs-outer-space-juicy-mix-same-ol-rig-new-drill-pipes/>
2022	From Albania to the Middle East: The Scarred Manticore is Listening <https://research.checkpoint.com/2023/from-albania-to-the-middle-east-the-scarred-manticore-is-listening/>
Apr 2022	APT34 targets Jordan Government using new Saitama backdoor <https://blog.malwarebytes.com/threat-intelligence/2022/05/apt34-

		targets-jordan-government-using-new-saitama-backdoor/>
	May 2022	It began with a spearphishing email to a diplomat in Jordan. <https://www.fortinet.com/blog/threat-research/please-confirm-you-received-our-apt>
	Jul 2022	Microsoft investigates Iranian attacks against the Albanian government <https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/>
	Dec 2022	New APT34 Malware Targets The Middle East <https://www.trendmicro.com/en_us/research/23/b/new-apt34-malware-targets-the-middle-east.html>
	Feb 2023	Crambus: New Campaign Targets Middle Eastern Government <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/crambus-middle-east-government>
	Aug 2023	APT34 Unleashes New Wave of Phishing Attack with Variant of SideTwist Trojan <https://nsfocusglobal.com/apt34-unleashes-new-wave-of-phishing-attack-with-variant-of-sidetwist-trojan/> <https://www.trendmicro.com/en_fi/research/23/i/apt34-deploys-phishing-attack-with-new-malware.html>
	Sep 2024	The Unraveling of an Iranian Cyber Attack Against the Iraqi Government <https://blog.checkpoint.com/research/the-unraveling-of-an-iranian-cyber-attack-against-the-iraqi-government/>
	Sep 2024	Earth Simnavaz (aka APT34) Levies Advanced Cyberattacks Against Middle East <https://www.trendmicro.com/en_us/research/24/j/earth-simnavaz-cyberattacks.html>
Counter operations	Mar 2019	In an incident reminiscent of the Shadow Brokers leak that exposed the NSA's hacking tools, someone has now published similar hacking tools belonging to one of Iran's elite cyber-espionage units, known as APT34, Oilrig, or HelixKitten. <https://www.zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram/> Update: this leak may have been the work of the CIA.

	Jun 2019	A new hacking tool believed to have been in the arsenal of Iranian state hackers has been published today online, in a Telegram channel. This new tool is named Jason and was published online earlier today in the same Telegram channel where the leaker – going by the name of Lab Dookhtegan – dumped the six other previous hacking tools. <https://www.zdnet.com/article/new-iranian-hacking-tool-leaked-on-telegram/> Update: this leak may have been the work of the CIA.
Information		<https://unit42.paloaltonetworks.com/unit42-striking-oil-closer-look-adversary-infrastructure/> <https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-november-helix-kitten/> <https://marcoramilli.com/2019/08/07/oilrig-the-techniques-evolution-over-time/> <https://en.wikipedia.org/wiki/Helix_Kitten> <https://www.welivesecurity.com/en/eset-research/oilrig-persistent-attacks-cloud-service-powered-downloaders/> <https://cloud.google.com/blog/topics/threat-intelligence/unc1860-iran-middle-eastern-networks/>
MITRE ATT&CK		<https://attack.mitre.org/groups/G0049/>
Playbook		<https://pan-unit42.github.io/playbook_viewer/?pb=evasive-serpens>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
