Chafer, APT 39 - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:31:22 UTC

APT group: Chafer, APT 39

Names	Chafer *(Symantec)* APT 39 *(Mandiant)* Remix Kitten *(CrowdStrike)* Cobalt Hickman *(SecureWorks)* TA454 *(Proofpoint)* ITG07 *(IBM)* Radio Serpens *(Palo Alto)* Burgundy Sandstorm *(Microsoft)* G0087 *(MITRE)*
Country	Iran
Sponsor	State-sponsored, Rana Intelligence Computing Company
Motivation	Information theft and espionage
First seen	2014
Description	(FireEye) APT39 was created to bring together previous activities and methods used by this actor, and its activities largely align with a group publicly referred to as “Chafer.” However, there are differences in what has been publicly reported due to the variances in how organizations track activity. APT39 primarily leverages the SEAWEED and CACHEMONEY backdoors along with a specific variant of the POWBAT backdoor. While APT39’s targeting scope is global, its activities are concentrated in the Middle East. APT39 has prioritized the telecommunications sector, with additional targeting of the travel industry and IT firms that support it and the high-tech industry. APT39’s focus on the telecommunications and travel industries suggests intent to perform monitoring, tracking, or surveillance operations against specific individuals, collect proprietary or customer data for commercial or operational purposes that serve strategic requirements related to national priorities, or create additional accesses and vectors to facilitate future campaigns. Government entities targeting suggests a potential secondary intent to collect geopolitical data that may benefit nation-state decision making. Targeting data supports the belief that APT39’s key mission is to track or monitor targets of interest, collect personal information, including travel itineraries, and gather customer data from telecommunications firms.

Observed	Sectors: Aviation, Engineering, Government, High-Tech, IT, Shipping and Logistics, Telecommunications, Transportation. Countries: Israel, Jordan, Kuwait, Saudi Arabia, Spain, Turkey, UAE, USA and Middle East.	
Tools used	Antak, ASPXSpy, EternalBlue, HTTPTunnel, MechaFlounder, Metasploit, Mimikatz, nbtscan, Non-sucking Service Manager, OilRig, Plink, POWBAT, pwdump, Rana, Remcom, Remexi, SafetyKatz, SEAWEED, UltraVNC, Windows Credentials Editor, Living off the Land and SMB hacking tools.	
Operations performed	2017	Chafer appears to have been undeterred by its exposure in 2015 and continued to be very active during 2017, using seven new tools, rolling out new infrastructure, and attacking nine new target organizations in the region. The group hit organizations in Israel, Jordan, the United Arab Emirates, Saudi Arabia, and Turkey. Sectors targeted included airlines; aircraft services; software and IT services companies serving the air and sea transport sectors; telecoms services; payroll services; engineering consultancies; and document management software. Outside of the Middle East, Symantec has also found evidence of attacks against one African airline and attempts to compromise an international travel reservations firm. <https://www.symantec.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions>
	Feb 2018	Turkish Government Targeting This new secondary payload is Python-based and compiled into executable form using the PyInstaller utility. This is the first instance where Unit 42 has identified a Python-based payload used by these operators. We've also identified code overlap with OilRig's Clayside VBScript but at this time track Chafer and OilRig as separate threat groups. We have named this payload MechaFlounder for tracking purposes. <https://unit42.paloaltonetworks.com/new-python-based-payload-mechaflounder-used-by-chafer/>
	Autumn 2018	Spying on Iran-based foreign diplomatic entities Throughout the autumn of 2018 we analyzed a long-standing (and still active at that time) cyberespionage campaign that was primarily targeting foreign diplomatic entities based in Iran. The attackers were using an improved version of Remexi in what the victimology suggests might be a domestic cyberespionage operation. <https://securelist.com/chafer-used-remexi-malware/89538/>

	2018	Bitdefender researchers have found attacks conducted by this actor in the Middle East region, dating back to 2018. The campaigns were based on several tools, including “living off the land” tools, which makes attribution difficult, as well as different hacking tools and a custom built backdoor. <https://www.bitdefender.com/files/News/CaseStudies/study/332/Bitdefender-Whitepaper-Chafer-creat4491-en-EN-interactive.pdf>
Counter operations	Sep 2020	Treasury Sanctions Cyber Actors Backed by Iranian Intelligence Ministry <https://home.treasury.gov/news/press-releases/sm1127>
Information	<https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html> <https://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets> <https://securityintelligence.com/posts/observations-of-itg07-cyber-operations/> <https://www.ic3.gov/Media/News/2020/200917-2.pdf> <https://www.bitdefender.com/files/News/CaseStudies/study/332/Bitdefender-Whitepaper-Chafer-creat4491-en-EN-interactive.pdf>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0087/>	
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=radioserpens>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
