Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 01:02:09 UTC

APT group: Desert Falcons

Names	Desert Falcons *(Kaspersky)* APT-C-23 *(Qihoo 360)* Two-tailed Scorpion *(Qihoo 360)* Arid Viper *(Palo Alto)* ATK 66 *(Thales)* TAG-CT1 *(Recorded Future)* TAG-63 *(Recorded Future)* Mantis *(Symantec)* Niobium *(Microsoft)* Pinstripe Lightning *(Microsoft)* Renegade Jackal *(CrowdStrike)* Scimitar *(?)*
Country	[Gaza]
Sponsor	Hamas
Motivation	Information theft and espionage
First seen	2011
Description	(Kaspersky) The Global Research and Analysis Team (GReAT) at Kaspersky Lab has uncovered new targeted attacks in the Middle East. Native Arabic-speaking cybercriminals have built advanced methods and tools to deliver, hide and operate malware that they have also developed themselves. This malware was originally discovered during an investigation of one of the attacks in the Middle East. Political activities and news are being actively used by the cybercriminals to entice victims into opening files and attachments. Content has been created with professionalism, with well-designed visuals and interesting, familiar details for the victims, as if the information were long awaited. The victims of the attacks to date have been carefully chosen; they are active and influential in their respective cultures, but also attractive to the cybercriminals as a source of intelligence and a target for extortion.

		The attackers have been operating for more than two years now, running different campaigns, targeting different types of victims and different types of devices (including Windows- and Android-based). We suspect that at least 30 people distributed across different countries are operating the campaigns. Recorded Future found possible overlap with Cyber fighters of Izz Ad-Din Al Qassam, Fraternal Jackal.
Observed		Sectors: Critical infrastructure, Defense, Education, Government, Media, Transportation. Countries: Albania, Algeria, Australia, Belgium, Bosnia and Herzegovina, Canada, China, Cyprus, Denmark, Egypt, France, Germany, Greece, Hungary, India, Iran, Iraq, Israel, Italy, Japan, Jordan, Kuwait, Lebanon, Libya, Mali, Mauritania, Mexico, Morocco, Netherlands, Norway, Pakistan, Palestine, Portugal, Qatar, Romania, Russia, Saudi Arabia, South Korea, Sudan, Sweden, Syria, Taiwan, Turkey, UAE, Ukraine, USA, Uzbekistan, Yemen, Zimbabwe.
Tools used		AridSpy, Barb(ie) Downloader, BarbWire, Desert Scorpion, FrozenCell, GlanceLove, GnatSpy, KasperAgent, Micropsia, PyMICROPSIA, SpyC23, VAMP, ViperRAT, VolatileVenom.
Operations performed	Jan 2015	Operation “Arid Viper” Operation Arid Viper attacked five Israeli-based organizations in the government, transport, infrastructure, military, and academic industries, and one organization in Kuwait using spear-phishing emails that dropped a pornographic video on a victim’s computer. <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/sexually-explicit-material-used-as-lures-in-cyber-attacks?linkId=12425812> <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-arid-viper.pdf>
	Sep 2015	Proofpoint researchers recently intercepted and analyzed phishing emails distributing Arid Viper malware payloads with some noteworthy updates. As with the originally documented examples, these messages were part of narrow campaigns targeting specific industry verticals: telecoms, high tech, and business services, primarily in Israel. <https://www.proofpoint.com/us/threat-insight/post/Operation-Arid-Viper-Slithers-Back-Into-View>
	Jul 2016	Around July last year, more than a 100 Israeli servicemen were hit by a cunning threat actor. The attack compromised their devices and exfiltrated data to the attackers’ command and control server. In

	addition, the compromised devices were pushed Trojan updates, which allowed the attackers to extend their capabilities. The operation remains active at the time of writing this post, with attacks reported as recently as February 2017. <https://securelist.com/breaking-the-weakest-link-of-the-strongest-chain/77562/>
Apr 2017	ThreatConnect has identified a KASPERAGENT malware campaign leveraging decoy Palestinian Authority documents. The samples date from April – May 2017, coinciding with the run up to the May 2017 Palestinian Authority elections. <https://threatconnect.com/kasperagent-malware-campaign/>
Apr 2017	We identified one specific spear phishing campaign launched against targets within Palestine, and specifically against Palestinian law enforcement agencies. This campaign started in April 2017, using a spear phishing campaign to deliver the MICROPSIA payload in order to remotely control infected systems. <https://blog.talosintelligence.com/2017/06/palestine-delphi.html>
Sep 2017	FrozenCell is the mobile component of a multi-platform attack we've seen a threat actor known as "Two-tailed Scorpion/APT-C-23," use to spy on victims through compromised mobile devices and desktops. <https://blog.lookout.com/frozencell-mobile-threat>
Dec 2017	Recently, Trend Micro researchers came across a new mobile malware family which we have called GnatSpy. We believe that this is a new variant of VAMP, indicating that the threat actors behind APT-C-23 are still active and continuously improving their product. Some C&C domains from VAMP were reused in newer GnatSpy variants, indicating that these attacks are connected. We detect this new family as ANDROIDOS_GNATSPY. <https://blog.trendmicro.com/trendlabs-security-intelligence/new-gnatspy-mobile-malware-family-discovered/>
Early 2018	Lookout researchers have identified a new, highly targeted surveillanceware family known as Desert Scorpion in the Google Play Store. Lookout notified Google of the finding and Google removed the app immediately while also taking action on it in Google Play Protect. <https://blog.lookout.com/desert-scorpion-google-play>
Apr 2020	We have discovered a previously unreported version of Android spyware used by APT-C-23, a threat group also known as Two-tailed Scorpion and mainly targeting the Middle East. ESET products detect

		the malware as Android/SpyC23.A. <https://www.welivesecurity.com/2020/09/30/aptc23-group-evolves-its-android-spyware/>
	Apr 2020	Operation “Bearded Barbie” APT-C-23 Campaign Targeting Israeli Officials <https://www.cybereason.com/blog/operation-bearded-barbie-apt-c-23-campaign-targeting-israeli-officials>
	Dec 2020	PyMICROPSIA: New Information-Stealing Trojan from AridViper <https://unit42.paloaltonetworks.com/pymicropsia/>
	Sep 2021	Arid Viper APT targets Palestine with new wave of politically themed phishing attacks, malware <https://blog.talosintelligence.com/2022/02/arid-viper-targets-palestine.html>
	Nov 2021	New Variants of Android Spyware Linked to APT C-23 Enhanced for Stealth and Persistence, Sophos Research Reveals <https://www.sophos.com/en-us/press-office/press-releases/2021/11/new-variants-of-android-spyware-linked-to-apt-c-23-enhanced-for-stealth-and-persistence.aspx>
	2022	Arid Viper | APT’s Nest of SpyC23 Malware Continues to Target Android Devices <https://www.sentinelone.com/labs/arid-viper-apts-nest-of-spyc23-malware-continues-to-target-android-devices/>
	2022	Arid Viper poisons Android apps with AridSpy <https://www.welivesecurity.com/en/eset-research/arid-viper-poisons-android-apps-with-aridspy/>
	Apr 2022	Arid Viper disguising mobile spyware as updates for non-malicious Android applications <https://blog.talosintelligence.com/arid-viper-mobile-spyware/>
	Sep 2022	Mantis: New Tooling Used in Attacks Against Palestinian Targets <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/mantis-palestinian-attacks>
	Oct 2023	Hamas Application Infrastructure Reveals Possible Overlap with TAG-63 and Iranian Threat Activity <https://go.recordedfuture.com/hubfs/reports/cta-2023-1019.pdf>
Counter operations	Feb 2020	Operation “Rebound” IDF (Israel Defense Force) and ISA (Israel Security Agency AKA

		"Shin Bet") conducted a joint operation to take down a Hamas operation targeting IDF soldiers. <https://research.checkpoint.com/2020/hamas-android-malware-on-idf-soldiers-this-is-how-it-happened/>
	Apr 2021	Taking Action Against Hackers in Palestine <https://about.fb.com/news/2021/04/taking-action-against-hackers-in-palestine/>
Information	<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064309/The-Desert-Falcons-targeted-attacks.pdf> <https://team-cymru.com/blog/2020/12/16/mapping-out-aridviper-infrastructure-using-augurys-malware-addon/> <https://about.fb.com/wp-content/uploads/2021/04/Technical-threat-report-Arid-Viper-April-2021.pdf>	

Last change to this card: 28 June 2025

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=d337940e-7ef9-4b4e-8c04-c6472d6b8972