Molerats, Extreme Jackal, Gaza Cybergang

Archived: 2026-04-02 11:00:49 UTC

APT group: Molerats, Extreme Jackal, Gaza Cybergang

Names	Molerats *(FireEye)* Extreme Jackal *(CrowdStrike)* Gaza Cybergang *(Kaspersky)* Gaza Hackers Team *(Kaspersky)* TA402 *(Proofpoint)* Aluminum Saratoga *(SecureWorks)* ATK 89 *(Thales)* TAG-CT5 *(Recorded Future)* G0021 *(MITRE)*	
Country	[Gaza]	
Sponsor	Hamas	
Motivation	Information theft and espionage	
First seen	2012	
Description	(Kaspersky) The Gaza cybergang is an Arabic-language, politically-motivated cybercriminal group, operating since 2012 and a Gaza cybergang's attacks have never slowed down and its typical targets include government entities/embassies, oil and gas, n One of the interesting new facts, uncovered in mid-2017, is its discovery inside an oil and gas organization in the MENA regio year. An overlap has been found between Molerats and Operation Parliament and these may also be an association with The Big Ba	
Observed	Sectors: Aerospace, Defense, Embassies, Energy, Financial, Government, High-Tech, Media, Oil and gas, Telecommunication Countries: Afghanistan, Algeria, Canada, China, Chile, Denmark, Egypt, Germany, India, Iran, Iraq, Israel, Jordan, Kuwait, Le Palestine, Qatar, Russia, Saudi Arabia, Serbia, Slovenia, Somalia, South Korea, Syria, Turkey, UAE, UK, USA, Yemen and th	
Tools used	BadPatch, BrittleBush, Downeks, DropBook, DustySky, H-Worm, IronWind, JhoneRAT, KasperAgent, LastConn, Micropsia, Ivy, QuasarRAT, Scote, SharpSploit, SharpStage, Spark, XtremeRAT.	
Operations performed	Jan 2012	Defacement of Israel fire service website Hackers claiming to be from the Gaza Strip defaced the website of the Israel Fire and Rescue services, postir <https://middle-east-online.com/en/cyber-war-gaza-hackers-deface-israel-fire-service-website>
	Oct 2012	Operation "Molerats" In October 2012, malware attacks against Israeli government targets grabbed media attention as officials tem the use of USB memory sticks. Security researchers subsequently linked these attacks to a broader, yearlong and as discovered later, even the U.S. and UK governments. <https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-
	Jun 2013	We observed several attacks in June and July 2013 against targets in the Middle East and the U.S. that dropp infrastructure used by the Molerats attackers. <https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-
	Apr 2014	Between 29 April and 27 May, FireEye Labs identified several new Molerats attacks targeting at least one m organizations. <https://www.fireeye.com/blog/threat-research/2014/06/molerats-here-for-spring.html>
	Summer 2014	Attacks against Israeli & Palestinian interests The decoy documents and filenames used in the attacks suggest the intended targets include organizations w <https://pwc.blogs.com/cyber_security_updates/2015/04/attacks-against-israeli-palestinian-interests.html>

2014	Operation “Moonlight” Vectra Threat Labs researchers have uncovered the activities of a group of individuals currently engaged in t 200 samples of malware generated by the group over the last two years. These attacks are themed around Mi espionage, as opposed to opportunistic or criminal intentions. <https://blog.vectra.ai/blog/moonlight-middle-east-targeted-attacks>
May 2015	One interesting new fact about Gaza Cybergang activities is that they are actively sending malware files to I also obvious from the file names they are sending to victims, which reflect the IT functions or IR tools used <https://securelist.com/gaza-cybergang-wheres-your-ir-team/72283/>
Sep 2015	Operation “DustySky” These attacks are targeted, but not spear-phished. I.e., malicious email messages are sent to selected targets r to each and every target. Dozens of targets may receive the exact same message. The email message and the on the target audience. Targeted sectors include governmental and diplomatic institutions, including embassi institutions; journalists; software developers. The attackers have been targeting software developers in gener management software, and linking to it in an online freelancing marketplace. <https://www.clearskysec.com/wp-content/uploads/2016/01/Operation%20DustySky_TLP_WHITE.pdf>
Dec 2015	Palo Alto Networks Traps Advanced Endpoint Protection recently prevented recent attacks that we believe ar <https://unit42.paloaltonetworks.com/unit42-downeks-and-quasar-rat-used-in-recent-targeted-attacks-agains
Apr 2016	Operation “DustySky” Part 2 Attacks against all targets in the Middle East stopped at once, after we published our first report. However, tl renewed in less than 20 days. In the beginning of April 2016, we found evidence that the attacks against Isra being the source of the attacks, and on the type of information the attackers are after –we estimate with medi these attacks. <https://www.clearskysec.com/wp-content/uploads/2016/06/Operation-DustySky2_-6.2016_TLP_White.pdf> <https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/26000/PD
Nov 2016	PwC analysts have been tracking the same malware campaign, which has seen a noticeable spike since at lea political figures and other targets that possess influence in the Palestinian territories and other neighbouring Our investigation began by nalyzing around 20 executable files associated with the attacks. Several of these exclusively in Arabic-language. <https://pwc.blogs.com/cyber_security_updates/2016/11/molerats-theres-more-to-the-naked-eye.html>
Mid-2017	New targets, use of MS Access Macros and CVE 2017-0199, and possible mobile espionage One of the interesting new facts, uncovered in mid-2017, is its discovery inside an oil and gas organization i apparently for more than a year. Another interesting finding is the use of the recently discovered CVE 2017-0199 vulnerability, and Microsof reduce the likelihood of their detection. Traces of mobile malware that started to appear from late April 2017 <https://securelist.com/gaza-cybergang-updated-2017-activity/82765/>
Sep 2017	Operation “TopHat” In recent months, Palo Alto Networks Unit 42 observed a wave of attacks leveraging popular third-party serv The attacks we found within the TopHat campaign began in early September 2017. In a few instances, origin <https://unit42.paloaltonetworks.com/unit42-the-tophat-campaign-attacks-within-the-middle-east-region-usi
Jan 2019	“Spark” Campaign This campaign uses social engineering to infect victims, mainly from the Palestinian territories, with the Spa been continuously active since then. The campaign’s lure content revolves around recent geopolitical events, Qasem Soleimani, and the ongoing conflict between Hamas and Fatah Palestinian movements. <https://www.cybereason.com/blog/new-cyber-espionage-campaigns-targeting-palestinians-part-one>
Feb 2019	New Attack in the Middle East Recently, 360 Threat Intelligence Center captured a bait document designed specifically for Arabic users. It i drop and execute a backdoor packed by Enigma Virtual Box. The backdoor program has a built-in keyword l with C2, distributes control commands to further control the victim’s computer device. After investigation, w <https://ti.360.net/blog/articles/suspected-molerats-new-attack-in-the-middle-east-en/>
Apr 2019	Operation “SneakyPastes” The campaign is multistage. It begins with phishing, using letters from one-time addresses and one-time dom attachments. If the victim executes the attached file (or follows the link), their device receives Stage One ma <https://www.kaspersky.com/blog/gaza-cybergang/26363/>
Oct 2019	Between October 2019 through the beginning of December 2019, Unit 42 observed multiple instances of phi (AKA Gaza Hackers Team and Gaza Cybergang) targeting eight organizations in six different countries in th of which the latter two were quite peculiar. <https://unit42.paloaltonetworks.com/molerats-delivers-spark-backdoor/>

	Dec 2019	“Pierogi” Campaign This campaign uses social engineering attacks to infect victims with a new, undocumented backdoor dubbed discovered by Cybereason. In this campaign, the attackers use different TTPs and decoy documents reminisc and Kaperagent malware. <https://www.cybereason.com/blog/new-cyber-espionage-campaigns-targeting-palestinians-part-one>
	Mar 2020	Molerats Delivers Spark Backdoor to Government and Telecommunications Organizations <https://unit42.paloaltonetworks.com/molerats-delivers-spark-backdoor/> <https://www.bleepingcomputer.com/news/security/hackers-hide-malware-c2-communication-by-faking-nev
	Oct 2020	New Malware Arsenal Abuses Cloud Platforms in Middle East Espionage Campaign <https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-A <https://www.cybereason.com/blog/molerats-apt-new-malware-and-techniques-in-middle-east-espionage-ca
	Early 2021	New TA402 Molerats Malware Targets Governments in the Middle East <https://www.proofpoint.com/us/blog/threat-insight/new-ta402-molerats-malware-targets-governments-midc
	Apr 2021	Threat Group Uses Voice Changing Software in Espionage Attempt <https://www.cadosecurity.com/post/threat-group-uses-voice-changing-software-in-espionage-attempt>
	Jul 2021	New espionage attack by Molerats APT targeting users in the Middle East <https://www.zscaler.com/blogs/security-research/new-espionage-attack-molerats-apt-targeting-users-middle
	Nov 2021	Ugg Boots 4 Sale: A Tale of Palestinian-Aligned Espionage <https://www.proofpoint.com/us/blog/threat-insight/ugg-boots-4-sale-tale-palestinian-aligned-espionage>
	Jul 2023	TA402 Uses Complex IronWind Infection Chains to Target Middle East-Based Government Entities <https://www.proofpoint.com/us/blog/threat-insight/ta402-uses-complex-ironwind-infection-chains-target-m
Information	<https://www.sentinelone.com/labs/gaza-cybergang-unified-front-targeting-hamas-opposition/>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0021/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
