MuddyWater, Seedworm, TEMP.Zagros, Static Kitten

Archived: 2026-04-02 11:29:21 UTC

APT group: MuddyWater, Seedworm, TEMP.Zagros, Static Kitten

Names	MuddyWater *(Palo Alto)* Seedworm *(Symantec)* TEMP.Zagros *(FireEye)* Static Kitten *(CrowdStrike)* Mercury *(Microsoft)* TA450 *(Proofpoint)* Cobalt Ulster *(SecureWorks)* ATK 51 *(Thales)* T-APT-14 *(Tencent)* ITG17 *(IBM)* Mango Sandstorm *(Microsoft)* Boggy Serpens *(Palo Alto)* Yellow Nix *(PWC)* G0069 *(MITRE)*
Country	Iran
Sponsor	State-sponsored, IRGC (Islamic Republic Guard Corps)
Motivation	Information theft and espionage
First seen	2017
Description	(Reaqta) MuddyWater is an APT group that has been active throughout 2017, targeting victims in Middle East v memory vectors leveraging on Powershell, in a family of attacks now identified as “Living off the land”, as the require the creation of new binaries on the victim’s machine, thus maintaining a low detection profile and a low forensic footprint. The operators behind MuddyWater are likely espionage motivated, we derive this information from the analysis and backdoors behaviors. We also find that despite the strong preponderance of victims from Pakistan, the most targets appear to be in: Saudi Arabia, UAE and Iraq. Amongst the victims we identify a variety of entities with a stronger focus at Governments, Telcos and Oil companies. By tracking the operations we finally figure out that the originating country is likely to be Iran, while it remains to ascertain whether MuddyWater is state sponsored or a criminal organization incline to espionage.
Observed	Sectors: Aviation, Defense, Education, Energy, Financial, Food and Agriculture, Gaming, Government, Healthc High-Tech, IT, Media, NGOs, Oil and gas, Shipping and Logistics, Telecommunications, Transportation. Countries: Afghanistan, Armenia, Austria, Azerbaijan, Bahrain, Belarus, Egypt, Georgia, India, Iran, Iraq, Israe Jordan, Kuwait, Laos, Lebanon, Mali, Netherlands, Oman, Pakistan, Portugal, Qatar, Russia, Saudi Arabia, Sud Tajikistan, Tanzania, Thailand, Tunisia, Turkey, UAE, Ukraine, USA.
Tools used	BugSleep, ChromeCookiesView, chrome-passwords, CLOUDSTATS, Cobalt Strike, CrackMapExec, DCHSpy, DELPHSTATS, EmpireProject, FruityC2, Koadic, LaZagne, Meterpreter, Mimikatz, MuddyC2Go, Mudwater, MZCookiesView, PhonyC2, Powermud, PowerSploit, POWERSTATS, PowGoop, PRB-Backdoor, QUADAGF Secure Socket Funneling, SHARPSTATS, Shootback, Smbmap, Living off the Land.

Operations performed	Feb 2017	The MuddyWater attacks are primarily against Middle Eastern nations. However, we have also ob attacks against surrounding nations and beyond, including targets in India and the USA. <https://unit42.paloaltonetworks.com/unit42-muddying-the-water-targeted-attacks-in-the-middle-
	Jan 2018	Updated Tactics, Techniques and Procedures in Spear Phishing Campaign We attribute this activity to TEMP.Zagros (reported by Palo Alto Networks and Trend Micro as MuddyWater), an Iran-nexus actor that has been active since at least May 2017. This actor has en in prolific spear phishing of government and defense entities in Central and Southwest Asia. <https://www.fireeye.com/blog/threat-research/2018/03/iranian-threat-group-updates-ttps-in-spea phishing-campaign.html>
	Mar 2018	Campaign Possibly Connected to "MuddyWater" Surfaces in the Middle East and Central Asia We discovered a new campaign targeting organizations in Turkey, Pakistan and Tajikistan that has similarities with an earlier campaign named MuddyWater, which hit various industries in several countries, primarily in the Middle East and Central Asia. <https://blog.trendmicro.com/trendlabs-security-intelligence/campaign-possibly-connected-mudd surfaces-middle-east-central-asia/>
	May 2018	Another Potential MuddyWater Campaign uses Powershell-based PRB-Backdoor In May 2018, we found a new sample (Detected as W2KM_DLOADR.UHAOEEN) that may be to this campaign. Like the previous campaigns, these samples again involve a Microsoft Word do embedded with a malicious macro that is capable of executing PowerShell (PS) scripts leading to backdoor payload. One notable difference in the analyzed samples is that they do not directly dov the Visual Basic Script(VBS) and PowerShell component files, and instead encode all the scripts document itself. The scripts will then be decoded and dropped to execute the payload without nee download the component files. <https://blog.trendmicro.com/trendlabs-security-intelligence/another-potential-muddywater-camp uses-powershell-based-prb-backdoor/>
	May 2018	We recently noticed a large amount of spear phishing documents that appear to be targeting gover bodies, military entities, telcos and educational institutions in Jordan, Turkey, Azerbaijan and Pak addition to the continuous targeting of Iraq and Saudi Arabia, other victims were also detected in Austria, Russia, Iran and Bahrain.. These new documents have appeared throughout 2018 and esc from May onwards. The attacks are still ongoing. <https://securelist.com/muddywater/88059/>
	Sep 2018	Group remains highly active with more than 130 victims in 30 organizations hit since September Seedworm's motivations are much like many cyber espionage groups that we observe—they seek acquire actionable information about the targeted organizations and individuals. They accomplish with a preference for speed and agility over operational security, which ultimately led to our identification of their key operational infrastructure. <https://www.symantec.com/blogs/threat-intelligence/seedworm-espionage-group>
	Nov 2018	Operations in Lebanon and Oman MuddyWater has recently been targeting victims likely from Lebanon and Oman, while leveragin compromised domains, one of which is owned by an Israeli web developer. The investigation aim uncover additional details regarding the compromise vector. Further, we wished to determine the infection vector, which is currently unknown. With that in mind, past experience implies that this be a two-stage spear-phishing campaign. <https://www.clearskysec.com/wp-content/uploads/2018/11/MuddyWater-Operations-in-Lebanor Oman.pdf>
	Apr 2019	Targeting Kurdish Political Groups and Organizations in Turkey However, unlike the previous vector, we did not identify this time any compromised servers used the malware's code. Instead, the lure document already contains the malicious code. We also dete five additional files that operate in a similar file to the aforementioned document; but unlike that

	these do not have any content. <https://www.clearskysec.com/muddywater-targets-kurdish-groups-turkish-orgs/>
Apr 2019	The Iranian APT, MuddyWater, has been active since at least 2017. Most recently though, a new campaign, targeting Belarus, Turkey and Ukraine, has emerged that caught the attention of Check researchers. <https://research.checkpoint.com/the-muddy-waters-of-apt-attacks/>
Apr 2019	Operation “BlackWater” Newly associated samples from April 2019 indicate attackers have added three distinct steps to th operations, allowing them to bypass certain security controls and suggesting that MuddyWater’s t techniques and procedures (TTPs) have evolved to evade detection. <https://blog.talosintelligence.com/2019/05/recent-muddywater-associated-blackwater.html>
Jun 2019	Clearsky has detected new and advanced attack vector used by MuddyWater to target governmen entities and the telecommunication sector. Notably, the TTP includes decoy documents exploiting 2017-0199 as the first stage of the attack. This is followed by the second stage of the attack – communication with the hacked C2 servers and downloading a file infected with the macros. <https://www.clearskysec.com/muddywater2/>
Jun 2019	We came across new campaignsthat seem to bear the markings of MuddyWater –a threat actor gr with a history of targeting organizations in Middle Eastern and Asian countries. The group used n tools and payloads in campaigns over the first half of 2019, pointing to the continued work the gr put in since our last report on MuddyWaterin November 2018. <https://documents.trendmicro.com/assets/white_papers/wp_new_muddywater_findings_uncove
Dec 2019	Group continues to be highly active in 2020, while tentative links to recently discovered PowGoo suggest possible retooling. <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/seedworm-apt-iran-mid east>
2019	State-sponsored hackers abuse Slack API to steal airline data <https://www.bleepingcomputer.com/news/security/state-sponsored-hackers-abuse-slack-api-to-s airline-data/>
Sep 2020	Operation “Quicksand” During September 2020, weidentified a new campaign targeting many prominent Israeli organiza <https://www.clearskysec.com/wp-content/uploads/2020/10/Operation-Quicksand.pdf>
Oct 2020	MSTIC has observed activity by the nation-state actor MERCURY using the CVE-2020-1472 exp (ZeroLogon) in active campaigns over the last 2 weeks. <https://www.zdnet.com/article/microsoft-says-iranian-hackers-are-exploiting-the-zerologon- vulnerability/>
Dec 2020	GitHub-hosted malware calculates Cobalt Strike payload from Imgur pic <https://www.bleepingcomputer.com/news/security/github-hosted-malware-calculates-cobalt-stri payload-from-imgur-pic/>
Feb 2021	Probable Iranian Cyber Actors, Static Kitten, Conducting Cyberespionage Campaign Targeting U Kuwait Government Agencies <https://www.anomali.com/blog/probable-iranian-cyber-actors-static-kitten-conducting-cyberesp campaign-targeting-uae-and-kuwait-government-agencies>

	Feb 2021	Operation “Earth Vetala” Earth Vetala used spearphishing emails with embedded links to a legitimate file-sharing service tc distribute their malicious package. The links were embedded within lure documents as well as em <https://www.trendmicro.com/en_us/research/21/c/earth-vetala---muddywater-continues-to-targe organizations-in-t.html>
	Jun 2021	Espionage Campaign Targets Telecoms Organizations across Middle East and Asia <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-campaign-tel asia-middle-east>
	Nov 2021	Iranian APT MuddyWater targets Turkish users via malicious PDFs, executables <https://blog.talosintelligence.com/2022/01/iranian-apt-muddywater-targets-turkey.html>
	Late 2021	New MuddyWater Threat: Old Kitten; New Tricks <https://www.deepinstinct.com/blog/new-muddywater-threat-old-kitten-new-tricks>
	Late 2022	APT groups muddying the waters for MSPs <https://www.welivesecurity.com/2023/05/02/apt-groups-muddying-waters-msps/>
	Apr 2023	MERCURY and DEV-1084: Destructive attack on hybrid environment <https://www.microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive- on-hybrid-environment/>
	Apr 2023	PhonyC2: Revealing a New Malicious Command & Control Framework by MuddyWater <https://www.deepinstinct.com/blog/phonyc2-revealing-a-new-malicious-command-control-fram by-muddywater>
	May 2023	Microsoft: Iranian hacking groups join Papercut attack spree <https://www.bleepingcomputer.com/news/security/microsoft-iranian-hacking-groups-join-paper attack-spree/>
	Jul 2023	MuddyC2Go – Latest C2 Framework Used by Iranian APT MuddyWater Spotted in Israel <https://www.deepinstinct.com/blog/muddyc2go-latest-c2-framework-used-by-iranian-apt-muddy spotted-in-israel>
	Oct 2023	MuddyWater eN-Able spear-phishing with new TTPs <https://www.deepinstinct.com/blog/muddywater-en-able-spear-phishing-with-new-ttps>
	Nov 2023	Seedworm: Iranian Hackers Target Telecoms Orgs in North and East Africa <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/iran-apt-seedworm-afric telecoms>
	Mar 2024	Security Brief: TA450 Uses Embedded Links in PDF Attachments in Latest Campaign <https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta450-uses-embedded-links-pd attachments-latest-campaign>
	May 2024	MuddyWater Threat Group Deploys New BugSleep Backdoor <https://blog.checkpoint.com/research/muddywater-threat-group-deploys-new-bugsleep-backdoo
	Jul 2025	Lookout Discovers Iranian APT MuddyWater Leveraging DCHSpy During Israel-Iran Conflict <https://www.lookout.com/threat-intelligence/article/lookout-discovers-iranian-dchsy-surveillanc
Counter operations	May 2019	New leaks of Iranian cyber-espionage operations hit Telegram and the Dark Web <https://www.zdnet.com/article/new-leaks-of-iranian-cyber-espionage-operations-hit-telegram-ar dark-web/> Update: this leak may have been the work of the CIA.
Information	<https://reaqta.com/2017/11/muddywater-apt-targeting-middle-east/> <https://www.symantec.com/blogs/threat-intelligence/seedworm-espionage-group>	

	<https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-sou tools/> <https://www.cisa.gov/uscert/ncas/alerts/aa22-055a> <https://blog.talosintelligence.com/2022/03/iranian-supergroup-muddywater.html> <https://www.group-ib.com/blog/muddywater-infrastructure/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0069/>
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=boggyserpens>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
