European Repository of Cyber Incidents

Major Cyber Incidents

BAPCO

Other incident names: DUSTMAN [1]

Description

Iranian state-backed hackers attacked the Bahraini oil company BAPCO with a data-wiping malware.

Timeframe
25 July to 29 December 2019

Incident Type
Data-wiping malware

Initiator
Iranian state-backed hackers

Affected Target
The Bahrain Petroleum Company (BAPCO), government-owned oil company, Bahrain

Impact and significance

Initially, the reported impact consisted of system shutdowns which effected only a limited number of BAPCO's computers. [2] BAPCO was able to continue its operations after the malware discharge. Later, it was reported that the attack was considerably more destructive than initially understood, with nearly 2,000 computers having to be replaced. [3] The attackers did not test the deployment of the DUSTMAN malware but appear to have triggered the data-wiping process as a last-ditch effort to hide forensic evidence that would have revealed their presence on the hacked network. [4] It is suspected that the Dustman attack was executed to protect a larger operation, possibly connected to IBM's report on the similar ZeroCleare malware in Dec. 2019. [5] [11] Dustman was the third data-wiping malware linked to the Iranian government and has been used exclusively against companies in the oil and gas sector. [2] Forbes considers the operation to be a rehearsal of attacks on heavily secured command and control systems or a demonstration of their vulnerability. If these were fully compromised, this would have resulted in significant impact. [6] The incident can be considered above the normal level of Iranian cyber activity (see below **Cyber activities between Iran and Bahrain)**. [7] The Iranian cyber capacity may have affected US security alerts that were issued following the killing of General Soleimani in January 2020. [8] US-Bahraini cybersecurity cooperation has been deepened subsequently. [9]

By Mika Kerttunen and Linda Liang

Cyber activities between Iran and Bahrain

Iran-Saudi-Arabia interactions added for context

2018 **Out to Sea campaign** [a]

Begin of cyber campaign by Iranian hacking group "OilRig" against Saudi Arabia and other states (Israel, Tunisia, United Arab Emirates, South Africa, Morocco)

data theft | hijacking with misuse

APT Chafer attack [b]

Attack on Kuwaiti and Saudi government and transportation networks

data theft | hijacking with misuse

Seedworm attack [c]

Iranian actor targets Saudi telecommunication

data theft | hijacking with misuse

2019 **APT33 attacks** [d]

Iran-sponsored hacking of Saudi civilian infrastructure and corporations

data theft | hijacking with misuse

Hacks on Bahraini state networks [e]

Iranian state-backed attacks on Bahrain

data theft | hijacking with misuse

BAPCO [f]

Iran-affiliated actor attacks Bahraini oil industry

disruption | hijacking with misuse

Supply Chain attack [g]

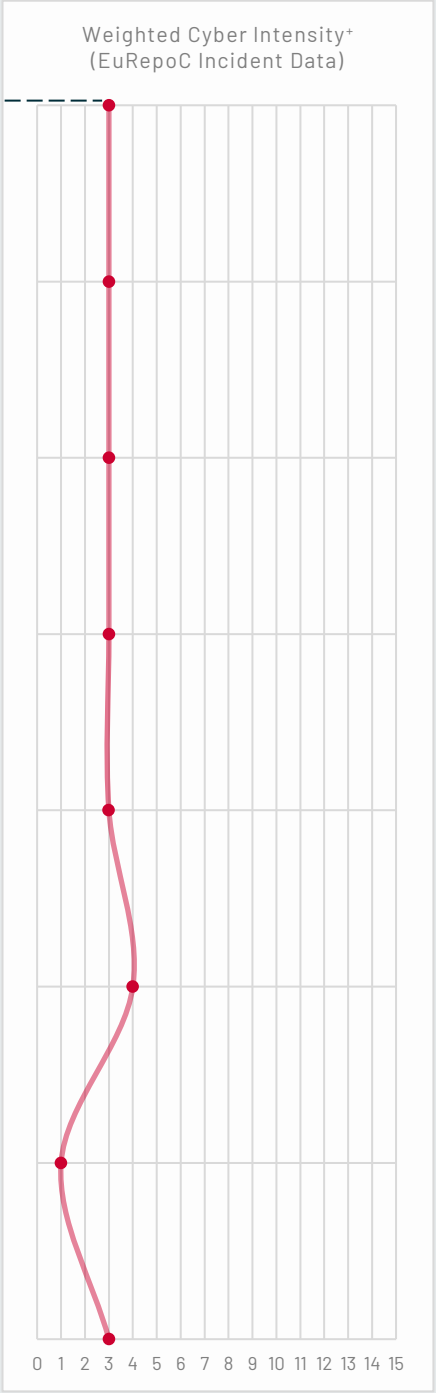
Iranian state-backed attack on Bahraini government

disruption | hijacking with misuse

Fake Interview [h]

Iranian APT "Charming Kitten" attacks Saudi academics

data theft | hijacking with misuse



+ The *Weighted Cyber Intensity* score is derived from the EuRepoC 1.0 dataset. It assesses the type of attacks, their potential physical effects in reach and duration, and their socio-poliitcal severity. Scores 0-5 are considered low/moderate in intensity, scores 6-10 indicate high intensity, and 11-15 very high intensity incidents. See here for more information on the EuRepoC codebook.

Links to incidents in the EuRepoC database

[a] https://eurepoc.eu/incident/out-to-sea
[b] https://eurepoc.eu/incident/chafer-vs-kuwait-1
[c] https://eurepoc.eu/incident/seedworm

[d] https://eurepoc.eu/incident/apt-33-vs-saudi-targets-2019
[e] https://eurepoc.eu/incident/iran-hacks-on-bahrain
[f] https://eurepoc.eu/incident/iran-vs-bapco
[g] https://eurepoc.eu/incident/iranian-it-company-supply-chain-attack-in-bahrain
[h] https://eurepoc.eu/incident/fake-interview

Background

For decades, there has been an ongoing tensions between Iran and states in the Middle East. In 2019, Bahrain and Saudi Arabia expressed support for the U.S. designating the Iranian Revolutionary Guard Corps (IRGC) as a foreign terrorist organisation, with businesses and banks with connections to the IRGC facing further sanctions. In June of the same year, Bahrain condemned Iran's capture of foreign oil tankers in the Strait of Hormuz. Iran in turn denounced these allegations and Bahrain's hosting of an international maritime security meeting in October. [10] Iran has demonstrable expertise in developing sophisticated espionage malware with advanced wiper functions and deploying these against its adversaries' oil sectors (see below **Iranian wiper malware against targets in the Middle East**). [2]

Attribution

Media reports cited unnamed experts who attributed the attack to Iran due to the similarities with the ZeroCleare malware and the suggestion of the Saudi report of a state-backed actor. [3] [11]

Operation timeline and attribution

25 July 2019	System access
29 December 2019	System attack Detection and identification of DUSTMAN by Saudi National Cybersecurity Authority, indicating a state actor
8 January 2020	Attribution of attack to Iran by media reporting

Sources: [3] [14] [15] [15]

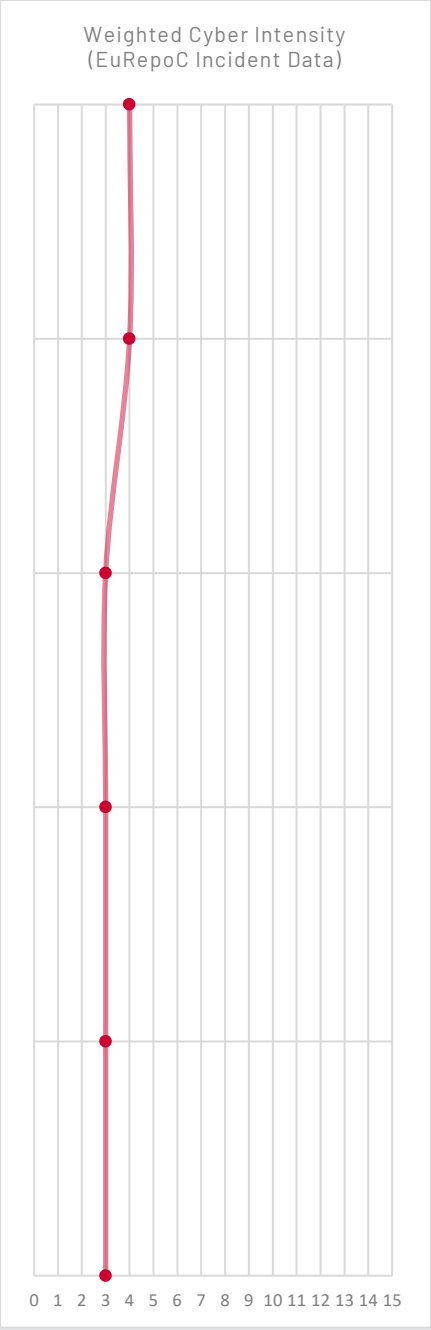
Technical details

Dustman is a so-called data-wiper malware designed to delete data on infected computers once launched. [2] For access to the BAPCO network, the hackers exploited a VPN vulnerability, from where they obtained access to the credentials required to install and execute the malware. They were able to load the data wiper into the central

antivirus software, from where it was distributed to all BAPCO machines. However, the malware did not run properly on some, leaving them unscathed. This left evidence that later pointed towards the attackers and the type of malware used. [14] After execution, the malware downloaded a tool to delete the VPN logs. [4]

Iranian wiper malware against targets in the Middle East

Following the discovery of the Iranian wiper malware Shamoon, subsequent attacks with similar code were found which can be considered new variants of the original Shamoon malware.



Saudi Aramco (Shamoon malware) [a]
Hacking group wiped three-quarters of Saudi oil company's computers, long-term disruption + defacement
oil sector | Saudi Arabia

Malware "Stonedrill" [b]
Similarities to Shamoon 2.0; "Charming Kitten" group (Iranian state-affiliation assumed) attacked Saudi corporations and European Kaspersky networks
corporation | Saudi Arabia | Europe

Shamoon 2.0 [c]
"Crowd strike" group (Iranian state-sponsorship assumed) wiped Saudi airport, government, and corporate systems
corporation | governemnt | transport | Saudi Arabia

Shamoon 3.0 [d]
APT33 (attributed to Iran) attacks oil companies in Saudi Arabia, United Arabian Emirates, Kuwait; start in India.
oil sector | Saudi Arabia | UAE | Kuwait | India

ZeroCleare [e]
APT34 (attributed to Iran) wiper malware attack on oil company systems in the Middle East
oil sector | Middle East

BAPCO (Dustman malware) [f]
Wiper malware (attributed to Iran) attack on Bahraini oil company
oil sector | Bahrain

Links to incidents in the EuRepoC database

[a] https://eurepoc.eu/incident/saudi-aramco-shamoon
[b] https://eurepoc.eu/incident/malware-stonedrill
[c] https://eurepoc.eu/incident/shamoon-2-0
[d] https://eurepoc.eu/incident/shamoon-3-0
[e] https://eurepoc.eu/incident/zero-cleare
[f] https://eurepoc.eu/incident/iran-vs-bapco

Enablers

Underdeveloped corporate cybersecurity practices enabled this attack: a remote execution vulnerability in a VPN appliance was disclosed in July 2019. [3] It is conceivable that Iranian intelligence about the targeted company systems could have originated from parts of the Shi`a political opposition in Bahrain. However, Iran's attempts at influencing Bahrani Shi`a communities have been considerably less successful than in other countries in the Middle East. [15]

Private Sector Engagement

Otorio665 [16]

IBM (analysis and early warning) [11]

Legal Assessment

N/A

Further Reading

Kaspersky ICS CERT. 2020. "Dustman Wiper Attack on Bapco Oil Company." Unpublished manuscript, last modified December 11, 2022. https://icscert.kaspersky.com/news/2020/01/10/bapco-dustman.

Sources

[1] Lemos, Robert. 2020. *Dustman Attack Underscores Iran's Cyber Capabilities*. Dark Reading, January 14. Available at: https://web.archive.org/web/20221217205137/https://www.darkreading.com/advanced-threats/dustman-attack-underscores-iran-s-cyber-capabilities [Archived on: 17.12.2022].

[2] Cimpanu, Catalin. 2020. *New Iranian Data Wiper Malware Hits Bapco, Bahrain's National Oil Company*. ZDNet, January 9. Available at : https://web.archive.org/web/20230120152440/https://www.zdnet.com/article/new-iranian-data-wiper-malware-hits-bapco-bahrains-national-oil-company/ [Archived on 20.01.2023].

[3] Bahrain Mirror. 2020. *Christmas Cyberattack on Bapco: Over 2000 Damaged Computers, Losses Amount to Millions*. January 14. Available at:

https://web.archive.org/web/20230120153059/http://bahrainmirror.com/en/news/56971.html [Archived on 20.01.2023].
[4] Saudi National Cybersecurity Authority. 2020. "Destructive Attack "DUSTMAN". Technical Report." Government report. Available at: https://web.archive.org/web/20230120153313/https://github.com/blackorbird/APT_REPORT/blob/master/International%20Strategic/Iran/Saudi-Arabia-CNA-report.pdf [Archived on: 20.01.2023].
[5] Ackerman, Gwen. 2022. *Ransomware Linked to Iran, Targets Industrial Controls.* Bloomberg, January 28. Available at: https://web.archive.org/web/20230120153436/https://www.bloomberg.com/news/articles/2020-01-28/-snake-ransomware-linked-to-iran-targets-industrial-controls#xj4y7vzkg [Archived on: 20.01.2023].
[6] Doffman, Zak. 2019. *Iranian Hackers Suspected of Cyberattacks on Bahrain – a Warning Beyond the Gulf*. Forbes, August 8. Available at: https://web.archive.org/web/20230120153611/https://www.forbes.com/sites/zakdoffman/2019/08/08/iranian-hackers-suspected-of-cyberattacks-on-bahrain-sending-message-beyond-the-gulf-report/?sh=61923d10324b [Archived on 20.01.2023].
[7] Compare: Hope, Bradley, Warren P. Strobel, and Dustin Volz. 2019. *High-Level Cyber Intrusions Hit Bahrain Amid Tensions with Iran*. Wall Street Journal, August 7. Available at: https://web.archive.org/web/20221128192917/https://www.wsj.com/articles/high-level-cyber-intrusions-hit-bahrain-amid-tensions-with-iran-11565202488 [Archived on: 28.11.2022].
[8] U.S. Department of Homeland Security. 2020. "Summary of Terrorism Threat to the U.S. Homeland." National Terrorism Advisory System Bulletin. Available at: https://web.archive.org/web/20230120153942/https://www.dhs.gov/sites/default/files/ntas/alerts/20_0104_ntas_bulletin.pdf [Archived on: 20.01.2023].
[9] U.S. Department of Homeland Security. 2021. "Bahraini MOI – U.S. DHS Joint Statement on Acting Secretary Wolf's Trip to Bahrain January 2021." Available at: https://web.archive.org/web/20230120154047/https://www.dhs.gov/news/2021/01/11/bahraini-moi-us-dhs-joint-statement-acting-secretary-wolf-s-trip-bahrain-january [Archived on: 20.01.2023].
[10] See: Bahrain Ministry of Foreign Affairs. 2019. "Kingdom of Bahrain Strongly Condemns Iranian Vessels Interception of UK Oil Tanker in Strait of Hormuz." News release. July 12, 2019. Available at: https://web.archive.org/web/20230120154453/https://www.mofa.gov.bh/Default.aspx?tabid=7824&language=en-US&ItemId=11011 [20.01.2023].
Bahrain Ministry of Foreign Affairs. 2019. "Kingdom of Bahrain Is Preparing to Host a Maritime and Air Navigation Security Meeting in Cooperation with United States of America and Poland." News release. July 18, 2019. Available at: https://web.archive.org/web/20230120154336/https://www.mofa.gov.bh/Default.aspx?tabid=7824&language=en-US&ItemId=11065 [Archived on 20.01.2023].
Bahrain Ministry of Foreign Affairs. 2019. "Ministry of Foreign Affairs of Kingdom of Bahrain Strongly Condemns Iranian Seizure of British Oil Tanker in Strait of Hormuz." News release. July 20, 2019. Available at: https://web.archive.org/web/20230120154429/https://www.mofa.gov.bh/Default.aspx?tabid=7824&language=en-US&ItemId=11081 [Archived on 20.02.2023].

Iran Ministry of Foreign Affairs. 2019. "Iran Condemns Saudi, Bahrain's Support for Blacklisting IRGC." News release. April 10, 2019. Available at: https://web.archive.org/web/20230120161410/https://en.mfa.gov.ir/portal/NewsView/37252 [Archived on: 20.01.2023].
Iran Ministry of Foreign Affairs. 2019. "Iran Says Not to Let Any Country Replace It in Oil Market." News release. April 25, 2019. Available at: https://web.archive.org/web/20230120161520/https://en.mfa.gov.ir/portal/NewsView/37299 [Archived on: 20.01.2023].
Iran Ministry of Foreign Affairs. 2019. "Spokesman's Reaction to Bahraini FM's Anti-Iran Remarks." News release. May 4, 2019. Available at: https://web.archive.org/web/20230120161745/https://en.mfa.gov.ir/portal/NewsView/37326 [Archived on: 20.01.2023].
Iran Ministry of Foreign Affairs. 2019. "Spokesman Condemns Bahrain's Anti-Iran Moves." News release. August 8, 2019. Available at: https://web.archive.org/web/20230120161725/https://en.mfa.gov.ir/portal/NewsView/48315 [Archived on: 20.01.2023].

[11] Kessum, Limor and IBM Security X-Force Team. 2020. *New Destructive Wiper "ZeroCleare" Targets Energy Sector in the Middle East*. Available at: https://web.archive.org/web/20230102183031/https://securityintelligence.com/posts/new-destructive-wiper-zerocleare-targets-energy-sector-in-the-middle-east/ [Archived on: 02.01.2023].
Lyngaas, Sean. 2020. *Saudi Cyber Authority Uncovers New Data-Wiping Malware, and Experts Suspect Iran Is Behind It*. CyberScoop, January 8. Available at: https://web.archive.org/web/20230120161156/https://www.cyberscoop.com/saudi-arabia-iran-cyberattack-soleimani/ [Archived on: 20.01.2023].

[12] McLaughlin, Jenna. 2020. *Saudis Warn of New Destructive Cyberattack That Experts Tie to Iran*. yahoo!news, January 8. Available at: https://web.archive.org/web/20230120161845/https://news.yahoo.com/days-before-suleimani-strike-saudis-warned-of-new-destructive-cyber-attack-013125981.html [Archived on: 20.01.2023].

[13] Trade Arabia. 2020. *Iranian Hackers Target Bapco*. January 10. Available at: https://web.archive.org/web/20230120161955/https://www.tradearabia.com/news/IT_362679.html [Archived on: 20.01.2023].

[14] *CPO Magazine*. 2022. "Data Wiper Malware Attack on Bahrain's National Oil Company Linked to Iran, Part of an Ongoing Pattern." January 21. Available at: https://web.archive.org/web/20230120162103/https://www.cpomagazine.com/cyber-security/data-wiper-malware-attack-on-bahrains-national-oil-company-linked-to-iran-part-of-an-ongoing-pattern/ [Archived on: 20.01.2023].

[15] Council on Foreign Relations. 2020. *Compromise of Bapco.* Available at: https://web.archive.org/web/20230120162137/https://www.cfr.org/cyber-operations/compromise-bapco [Archived on: 20.01.2023].

[16] International Institute for Strategic Studies. 2019. "Chapter Six: Bahrain, Saudi Arabia and Kuwait." In *Iran's Networks of Influence in the Middle East*, 179–94. Available at: https://web.archive.org/web/20230120162343/https://www.iiss.org/publications/strategic-dossiers/iran-dossier/iran-19-08-ch-6-bahrain-saudi-arabia-and-kuwait [Archived on: 20.01.2023].

[17] Ackerman, Gwen. 2020. "Cyberattacks Linked to Iran Appear to Target Bahrain Petroleum Co." *World Oil*, January 28. Available at:

https://web.archive.org/web/20230120162315/https://www.worldoil.com/news/2020/1/28/cyberattacks-linked-to-iran-appear-to-target-bahrain-petroleum-co [Archived on: 20.01.2023].

Last updated: 20.01.2023