WHITEPAPER

# Cyber Risk Intelligence: Iran-Linked Attack on U.S. Water Treatment Facility

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com

1140 Avenue of the Americas
Floor 19
New York, NY 10036
1.800.682.1707

## Executive Summary

- On November 25, a U.S. municipal water authority confirmed that one of its booster stations had suffered an attack by a threat actor group known as CyberAv3ngers, which analysts believe acts in support of Iranian geopolitical interests.
- The attack compromised a programmable logic controller (PLC) for a water pressure monitoring and regulation system, but officials noted that the incident did not threaten local water supplies.
- The SecurityScorecard Threat Research, Intelligence, Knowledge, and Engagement (STRIKE) Team researched the incident further using SecurityScorecard's attribution data, Attack Surface Intelligence module, and access to a strategic partner's network flow (NetFlow) data.
- The STRIKE Team's research suggests that suspicious activity experienced by a water authority-attributed IP before the attack may have originated from the following Iranian IP addresses:

    - 88.135.36[.]82
    - 5.144.130[.]35
    - 217.144.104[.]53
    - 31.7.73[.]176
    - 217.144.107[.]183
    - 185.143.233[.]120

## Background

On November 25, the U.S. municipal water authority of Aliquippa, Pennsylvania confirmed that one of its booster stations had suffered an attack by a threat actor group known as CyberAv3ngers, which analysts believe acts in support of Iranian geopolitical interests. Prior to the U.S. incident, the group claimed similar attacks against ten Israeli water treatment facilities on October 30. And on November 28, the group posted a message to its Telegram channel (also displayed on the device affected by the recent attack) declaring, "Every Equipment ' Made In Israel ' Is Cyber Av3ngers Legal Target!" in an apparent reference to the Israeli components of the Unitronics PLCs targeted in the groups' attacks.

State-affiliated Iranian hacking groups have been known for their involvement in defacements, distributed denial of service (DDoS) attacks, and targeting specific critical infrastructures for over a decade. One notable early example of such activity was the 2013 breach of the Bowman Dam in New York. These groups have historically increased their activities during periods of heightened geopolitical tension like the current conflict in Gaza. The technical sophistication of these groups' operations—especially those exploiting PLC or Supervisory Control and Data Acquisition (SCADA) systems in general and Israeli-designed systems in particular—has evolved over time.

Although the attack compromised a programmable logic controller (PLC) for a water pressure monitoring and regulation system, officials have noted that the incident did not threaten local water supplies. A CISA advisory published in response to the attack on November 28 suggests that the affected device was exposed to the wider Internet over the default port for such devices (TCP port 20256) and still used the default password ("1111"), which may have rendered it particularly vulnerable to attack.

To derive further insights, STRIKE Team researchers analyzed SecurityScorecard's attribution data, Attack Surface Intelligence module, and related NetFlow data obtained from a strategic partner.

### Findings

The STRIKE Team's research suggests that the IP address SecurityScorecard attributes to the affected water authority experienced suspicious activity in the month leading up to this attack and that this activity may have originated from the following Iranian IP addresses:

- 88.135.36[.]82
- 5.144.130[.]35
- 217.144.104[.]53
- 31.7.73[.]176
- 217.144.107[.]183
- 185.143.233[.]120

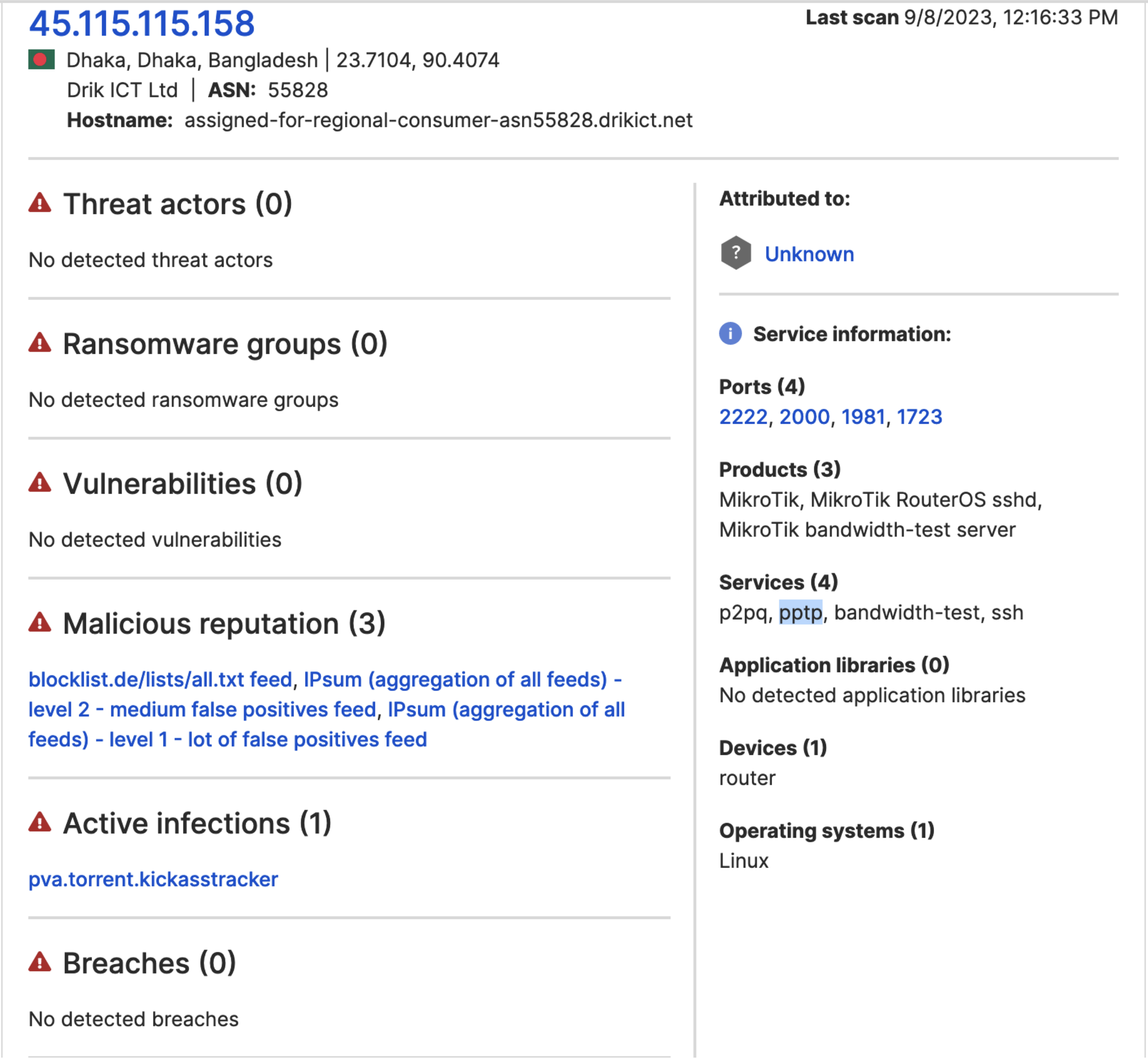
**Methodology**

Researchers first consulted SecurityScorecard's ratings platform to identify IP addresses attributed to the water authority targeted in the attack. The affected organization's digital footprint only contains one IP address, so researchers next collected a one-month traffic sample for that address using a strategic partner's NetFlow data.

The resulting traffic sample suggests that in the month leading up to the incident, four IP addresses communicated with the water authority-attributed IP address particularly frequently and that these communications may reflect activity linked to the attack. The following four IP addresses were responsible for more than half (180 of 308) of the flows in the sample:

- 45.115.115[.]158
- 103.143.208[.]192
- 45.232.73[.]84
- 154.70.207[.]242

Each of the above IP addresses may have served as proxies for traffic from other locations. The partner furnishing the sample linked 45.115.115[.]158 to a virtual private network (VPN), and the findings in SecurityScorecard's Attack Surface Intelligence module appear to support a similar conclusion, as Attack Surface Intelligence observes PPTP (a VPN protocol) to be one of the services in use at the same IP address.



45.115.115.158

**Last scan** 9/8/2023, 12:16:33 PM

Dhaka, Dhaka, Bangladesh | 23.7104, 90.4074
Drik ICT Ltd | **ASN:** 55828
**Hostname:** assigned-for-regional-consumer-asn55828.drikict.net

Threat actors (0)

No detected threat actors

Ransomware groups (0)

No detected ransomware groups

Vulnerabilities (0)

No detected vulnerabilities

Malicious reputation (3)

blocklist.de/lists/all.txt feed, IPsum (aggregation of all feeds) - level 2 - medium false positives feed, IPsum (aggregation of all feeds) - level 1 - lot of false positives feed

Active infections (1)

pva.torrent.kickasstracker

Breaches (0)

No detected breaches

**Attributed to:**

Unknown

**Service information:**

**Ports (4)**
2222, 2000, 1981, 1723

**Products (3)**
MikroTik, MikroTik RouterOS sshd, MikroTik bandwidth-test server

**Services (4)**
p2pq, pptp, bandwidth-test, ssh

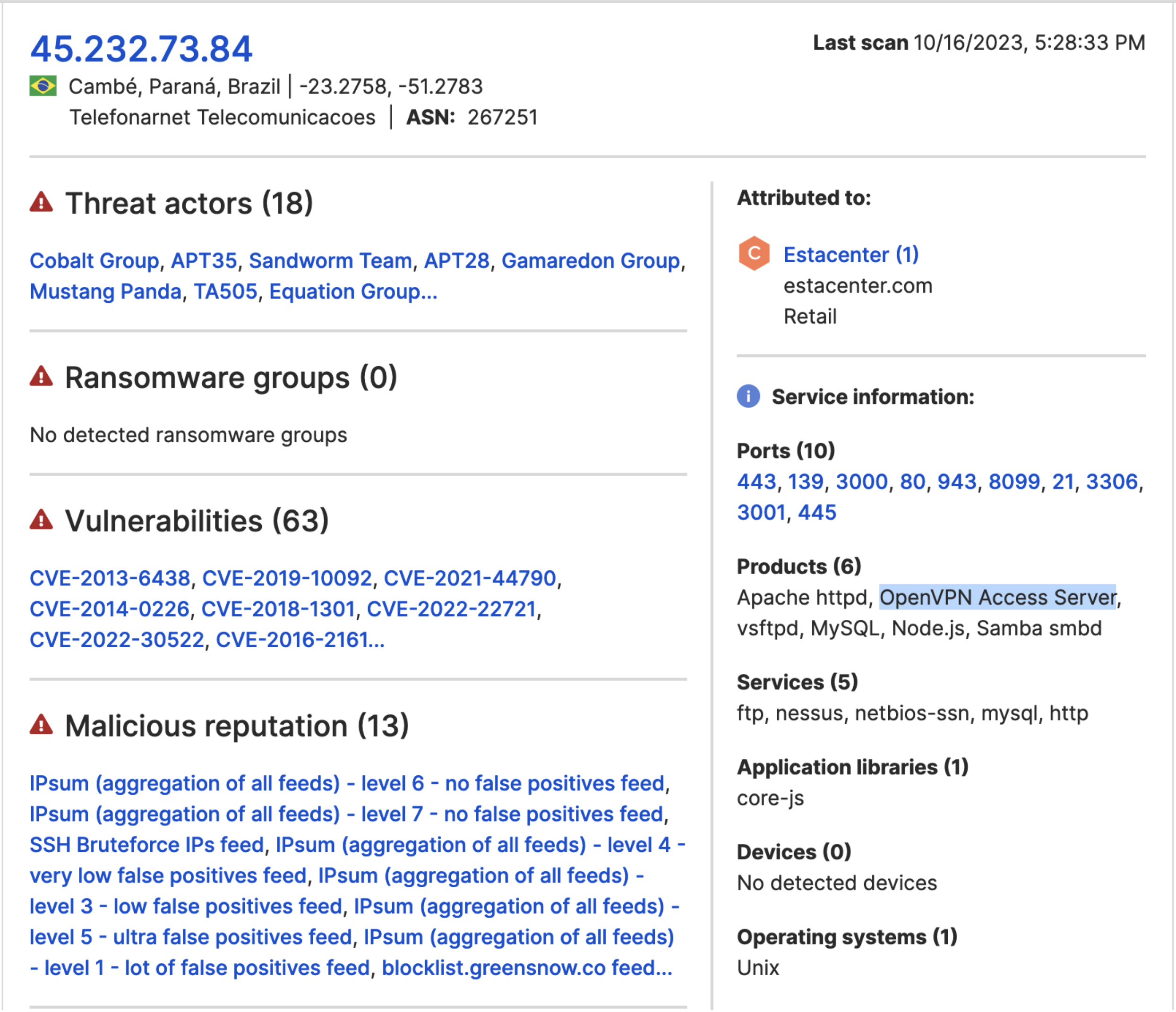
**Application libraries (0)**
No detected application libraries

**Devices (1)**
router

**Operating systems (1)**
Linux

*Image 1: Attack Surface Intelligence observes a VPN protocol in use at one IP address that communicated repeatedly with the IP address attributed to the water authority targeted in the recent incident.*

Attack Surface Intelligence also indicates that a VPN server is in use at 45.232.73[.]84, another of the four IP addresses that appear especially frequently in the traffic sample.



**45.232.73.84**

**Last scan** 10/16/2023, 5:28:33 PM

Cambé, Paraná, Brazil | -23.2758, -51.2783
Telefonarnet Telecomunicacoes | **ASN:** 267251

### Threat actors (18)

Cobalt Group, APT35, Sandworm Team, APT28, Gamaredon Group, Mustang Panda, TA505, Equation Group...

### Ransomware groups (0)

No detected ransomware groups

### Vulnerabilities (63)

CVE-2013-6438, CVE-2019-10092, CVE-2021-44790, CVE-2014-0226, CVE-2018-1301, CVE-2022-22721, CVE-2022-30522, CVE-2016-2161...

### Malicious reputation (13)

IPsum (aggregation of all feeds) - level 6 - no false positives feed, IPsum (aggregation of all feeds) - level 7 - no false positives feed, SSH Bruteforce IPs feed, IPsum (aggregation of all feeds) - level 4 - very low false positives feed, IPsum (aggregation of all feeds) - level 3 - low false positives feed, IPsum (aggregation of all feeds) - level 5 - ultra false positives feed, IPsum (aggregation of all feeds) - level 1 - lot of false positives feed, blocklist.greensnow.co feed...

**Attributed to:**

C Estacenter (1)
estacenter.com
Retail

**Service information:**

**Ports (10)**
443, 139, 3000, 80, 943, 8099, 21, 3306, 3001, 445

**Products (6)**
Apache httpd, OpenVPN Access Server, vsftpd, MySQL, Node.js, Samba smbd

**Services (5)**
ftp, nessus, netbios-ssn, mysql, http

**Application libraries (1)**
core-js

**Devices (0)**
No detected devices

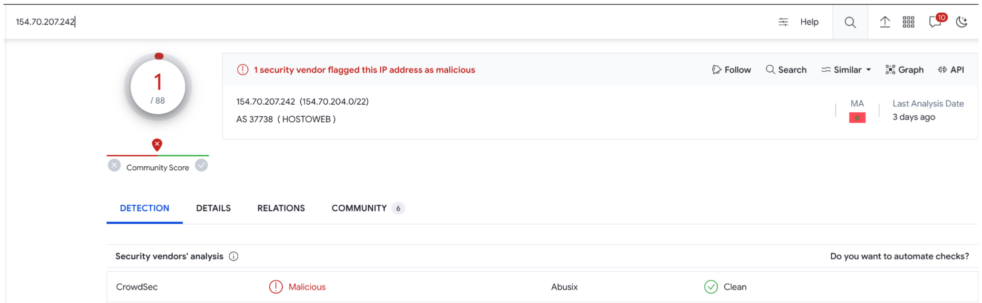
**Operating systems (1)**
Unix

*Image 2: Attack Surface Intelligence observes an OpenVPN Access Server in use at another of the traffic sample's most frequently-appearing IP addresses.*

Public sources have additionally noted that both of the other two IP addresses that appeared especially regularly in the traffic sample, 103.143.208[.]192 and 154.70.207[.]242, correspond to commercial servers that could, despite being located in Vietnam and Morocco respectively, act as proxies for traffic from elsewhere in the world.

Threat actors often route their traffic through VPNs, other proxy services, and compromised hosts to conceal the actual IP address and location from which their activity originates. Therefore, communication between IP addresses linked to such services and an IP address attributed to an organization that recently suffered a cyber incident in the weeks before that incident may reflect activity linked to it, (including probing or other reconnaissance).

The cybersecurity vendors that contribute detections to public cybersecurity information-sharing platform VirusTotal have also previously linked all four IP addresses to malicious activity. This may cast further suspicion upon their frequent communication with the IP address attributed to the recently-attacked water authority.



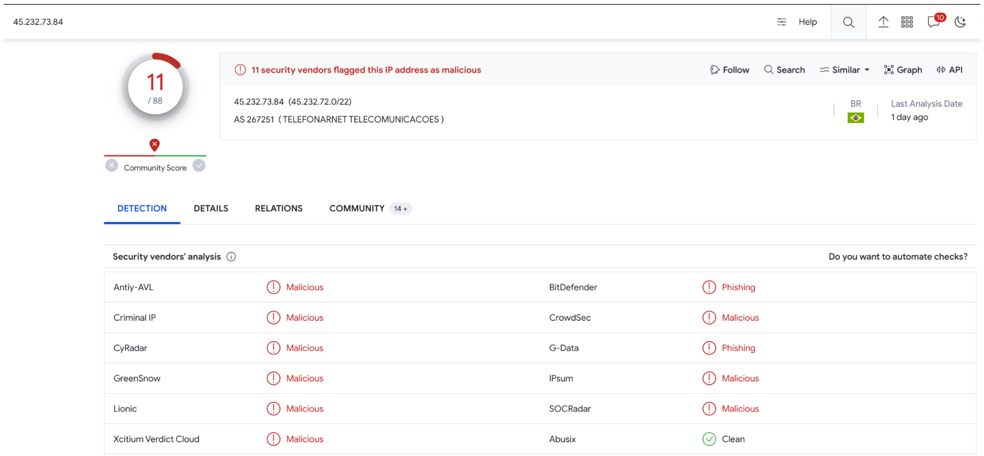
1 security vendor flagged this IP address as malicious

154.70.207.242 (154.70.204.0/22)
AS 37738 ( HOSTOWEB )

Last Analysis Date
3 days ago

Security vendors' analysis

| | | | |
|---|---|---|---|
| CrowdSec | Malicious | Abusix | Clean |



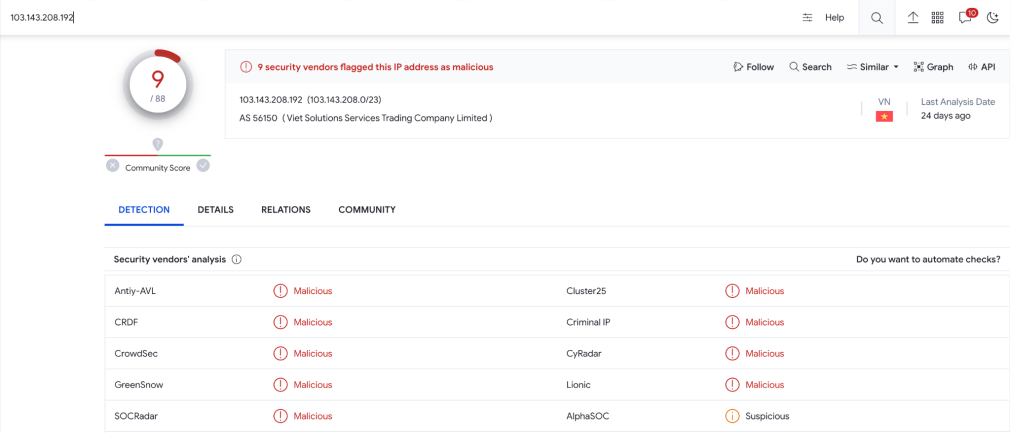
11 security vendors flagged this IP address as malicious

45.232.73.84 (45.232.72.0/22)
AS 267251 ( TELEFONARNET TELECOMUNICACOES )

Last Analysis Date
1 day ago

Security vendors' analysis

| | | | |
|---|---|---|---|
| Antiy-AVL | Malicious | BitDefender | Phishing |
| Criminal IP | Malicious | CrowdSec | Malicious |
| CyRadar | Malicious | G-Data | Phishing |
| GreenSnow | Malicious | IPsum | Malicious |
| Lionic | Malicious | SOCRadar | Malicious |
| Xcitium Verdict Cloud | Malicious | Abusix | Clean |



9 security vendors flagged this IP address as malicious

103.143.208.192 (103.143.208.0/23)
AS 56150 ( Viet Solutions Services Trading Company Limited )

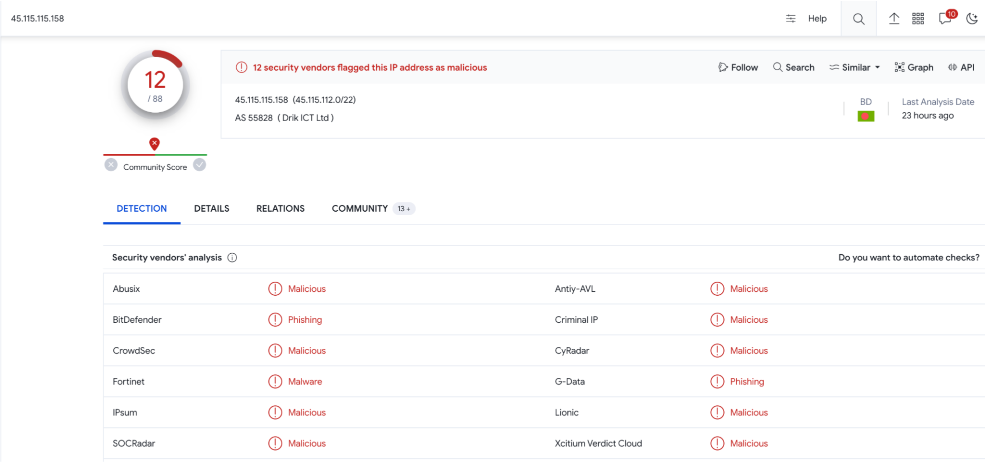
VN

Last Analysis Date
24 days ago

Security vendors' analysis

Do you want to automate checks?

| | | | |
|---|---|---|---|
| Antiy-AVL | Malicious | Cluster25 | Malicious |
| CRDF | Malicious | Criminal IP | Malicious |
| CrowdSec | Malicious | CyRadar | Malicious |
| GreenSnow | Malicious | Lionic | Malicious |
| SOCRadar | Malicious | AlphaSOC | Suspicious |



12 security vendors flagged this IP address as malicious

45.115.115.158 (45.115.112.0/22)
AS 55828 ( Drik ICT Ltd )

BD

Last Analysis Date
23 hours ago

Security vendors' analysis

Do you want to automate checks?

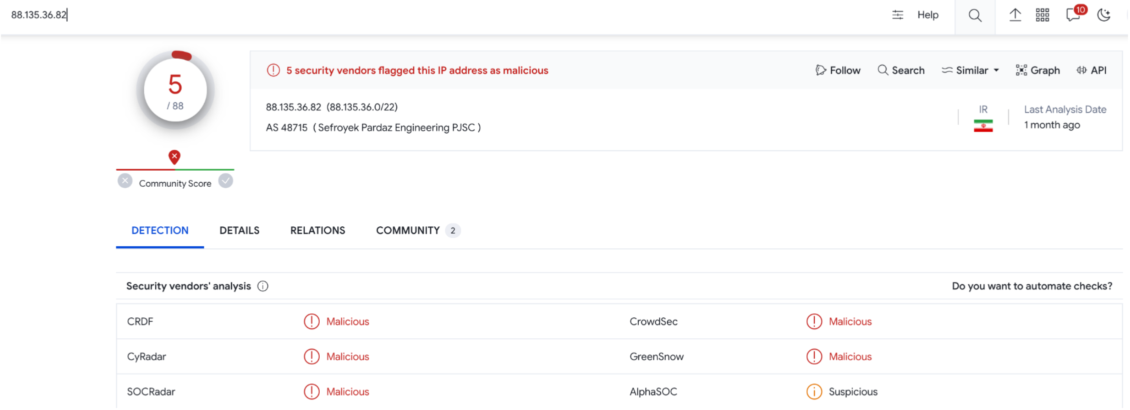
| | | | |
|---|---|---|---|
| Abusix | Malicious | Antiy-AVL | Malicious |
| BitDefender | Phishing | Criminal IP | Malicious |
| CrowdSec | Malicious | CyRadar | Malicious |
| Fortinet | Malware | G-Data | Phishing |
| IPsum | Malicious | Lionic | Malicious |
| SOCRadar | Malicious | Xcitium Verdict Cloud | Malicious |

*Images 3-6: Four of the most-frequently appearing IP addresses in the water authority's traffic sample have detections for malicious activity in VirusTotal.*

Bearing in mind that previous analysis has assessed that CyberAv3ngers likely acts in the interest of the Islamic Republic of Iran, researchers next collected additional samples of traffic involving these four IP addresses to identify possible links to Iran. They limited these samples to a ten-minute window surrounding the periods in which the IP addresses communicated with the water authority-attributed IP address and then searched the resulting samples for IP addresses located in Iran. This yielded a total of 368 Iranian IP addresses that communicated with the four suspicious IP addresses identified previously.

Given that it would be unlikely for all 368 of the resulting Iranian IP addresses to have been involved in malicious activity (there are, after all, legitimate uses for VPNs), researchers next sought to narrow the results further and focus on those most likely to have been involved in activity targeting the water authority. For this, researchers compared each of the suspicious IP addresses' traffic samples and selected only those Iranian IP addresses that appeared in more than one of the suspicious IP addresses that communicated with the target organization. This could suggest that they communicated with the suspicious IP addresses that in turn communicated with the water authority more than once, which may indicate that threat actors traffic from them to the water authority by way of the suspicious IPs appearing in the original traffic sample. This yielded the six Iranian IP addresses listed in the Findings section above.

Of those six, four (88.135.36[.]82, 217.144.104[.]53, 217.144.107[.]183, and 185.143.233[.]120) additionally have detections in VirusTotal, which further suggests their involvement in malicious activity. A member of the VirusTotal community has additionally linked one (217.144.104[.]53)to Iranian nation-state cyber activity, including it in a graph titled "IRGC APT35;" IRGC is the usual abbreviation for Islamic Revolutionary Guard Corps, the branch of the Iranian armed forces believed to be responsible for the cyber activity attributed to the advanced persistent threat group tracked as APT35.



5 security vendors flagged this IP address as malicious

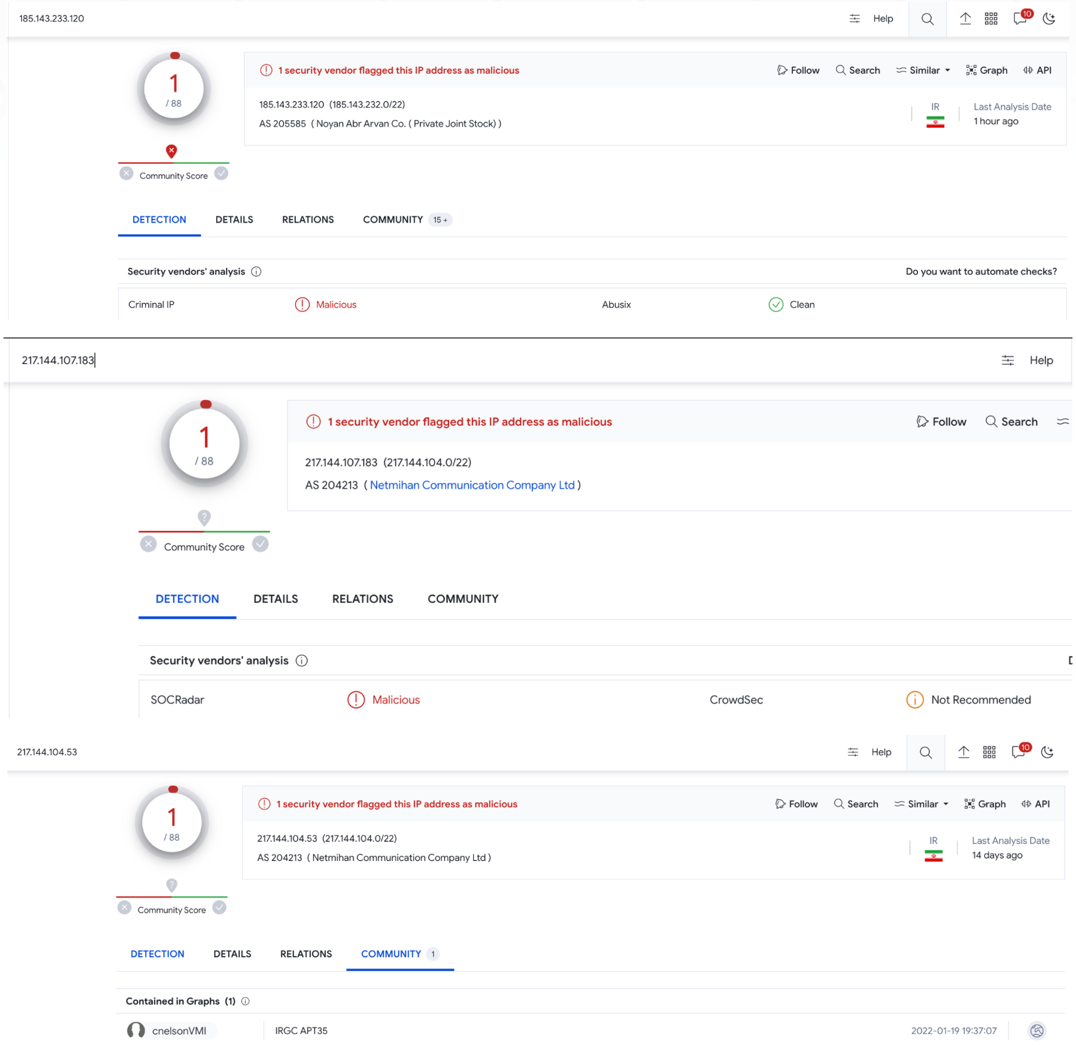
88.135.36.82 (88.135.36.0/22)
AS 48715 ( Sefroyek Pardaz Engineering PJSC )

Last Analysis Date
1 month ago

Security vendors' analysis

Do you want to automate checks?

| | | | |
|---|---|---|---|
| CRDF | Malicious | CrowdSec | Malicious |
| CyRadar | Malicious | GreenSnow | Malicious |
| SOCRadar | Malicious | AlphaSOC | Suspicious |


185.143.233.120

1 / 88

Community Score

1 security vendor flagged this IP address as malicious

185.143.233.120 (185.143.232.0/22)
AS 205585 ( Noyan Abr Arvan Co. ( Private Joint Stock) )

IR

Last Analysis Date
1 hour ago

Security vendors' analysis

Do you want to automate checks?

| | | | |
|---|---|---|---|
| Criminal IP | Malicious | Abusix | Clean |

217.144.107.183

1 / 88

Community Score

1 security vendor flagged this IP address as malicious

217.144.107.183 (217.144.104.0/22)
AS 204213 ( Netmihan Communication Company Ltd )

Security vendors' analysis

| | | | |
|---|---|---|---|
| SOCRadar | Malicious | CrowdSec | Not Recommended |

217.144.104.53

1 / 88

Community Score

1 security vendor flagged this IP address as malicious

217.144.104.53 (217.144.104.0/22)
AS 204213 ( Netmihan Communication Company Ltd )

IR

Last Analysis Date
14 days ago

Contained in Graphs (1)

| | | |
|---|---|---|
| cnelsonVMI | IRGC APT35 | 2022-01-19 19:37:07 |

*Images 7-10: VirusTotal contributors have previously linked four of the observed Iranian IP addresses to malicious activity, including Iranian APT activity.*

While an APT group may be unlikely to reuse the same infrastructure once it has been linked to the group's activity, these findings may nonetheless suggest that the IP addresses listed have been involved in recent malicious activity originating from the IRGC, even if APT35 is not responsible for these more recent operations.

## Conclusion

While it does not appear to have had an impact on water supplies, the recent attack may highlight significant cybersecurity challenges within the United States, especially at the local level. Local and municipal governments and utilities are often less equipped to defend against sophisticated cyber threats, making them attractive targets for state-sponsored actors.

As these threats continue to evolve, the need for continuous monitoring of the threat landscape, increased vigilance at the perimeter, and preparedness for the eventuality of an incident will likely increase. In addition to the security improvements CISA recommended in its November 28 advisory, monitoring networks for evidence of communication with the IP addresses identified above may help organizations defend against activity like the recent water authority attack.

### About SecurityScorecard

Funded by world-class investors, including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings, response, and resilience, with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight.

SecurityScorecard makes the world safer by transforming how companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. SecurityScorecard achieved the Federal Risk and Authorization Management Program (FedRAMP) Ready designation, highlighting the company's robust security standards to protect customer information, and is listed as a free cyber tool and service by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Every organization has the universal right to its trusted and transparent Instant SecurityScorecard rating.

For more information, visit securityscorecard.com or connect with us on LinkedIn.

**SecurityScorecard.com**
info@securityscorecard.com

1140 Avenue of the Americas
Floor 19
New York, NY 10036
1.800.682.1707

SecurityScorecard