SOCRadar®

PROSOL
TECHNOLOGY POWER HOUSE

Threat Landscape Report

AZERBAIJAN

March 2022

TABLE OF CONTENTS

EXECUTIVE SUMMARY

While rapidly developing companies of Azerbaijan are growing their technological infrastructure, they have also been becoming a significant target for many threat actors and ransomware groups in 2021.

SOCRadar Threat Landscape Report provides organizations with an understanding of evolving cyber threats relevant to their geographical operating locations to enable security leaders to make better decisions.

The intelligence provided in this report can help plan enterprise-wide security programs, make investment decisions, and define cybersecurity requirements.

SOCRadar characterizes the threat landscape based on recently observed threat actor activities, malware campaigns, new critical vulnerabilities, exploits, data gathered from open threat sharing platforms, and leveraging the comprehensive data monitoring, collection, classification, and analysis capabilities.

SOCRadar CTIA Team performs deep/dark web threat research, HUMINT observations, cybersecurity vendor blogs, and aggregating information gathered on social media trends, thanks to its unique perspective on understanding its competitors.

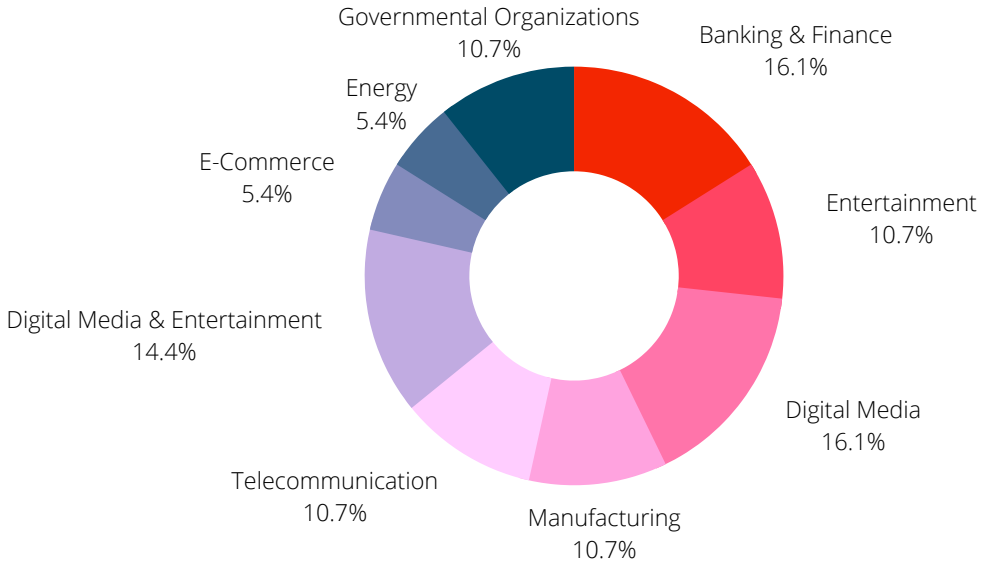
KEY FINDINDS

- **14 different threat actors targeting the the Azerbaijan entities shared posts on the deepweb.**
- **Top ransomware gangs targeting Azerbaijan are "LockBit, Conti, and Cring".**
- **13 APT groups that have targeted government, military, and private sectors in the past from Azerbaijan.**
- **SOCRadar has detected 339 phishing attacks targeting Azerbaijan since the beginning of 2021.**
- **In 2021, Open 3389 RDP Port vulnerability was the most exploited vulnerability in Azerbaijan.**
- **Currently there are 65 bots available for Azerbaijan.**
- **DDoS attacks in 2021 impacted critical emergency services.**

Copyright © 2022 SOCRadar

Dark Web Threats

The dark web underground ecosystem is the number one communication channel and a global marketplace with various hacking tools and stolen databases available for purchase. Fourteen different threat actors targeting the Azerbaijan entities shared posts on the dark web. Most of these posts were customer-user database sales and sales of unauthorized network access (RDP and VPN). These campaigns have exposed an extensive dataset belonging to different organizations from various verticals, including local government, banking & finance, digital media, and education.



The most targeted verticals in the Azerbaijan based on DarkMirror Intelligence data

14

Dark web threat actors / aliases

Banking & Finance

The most targeted vertical

Leaked database

RDP Access Sale

The most common threat category

TRY FOR FREE

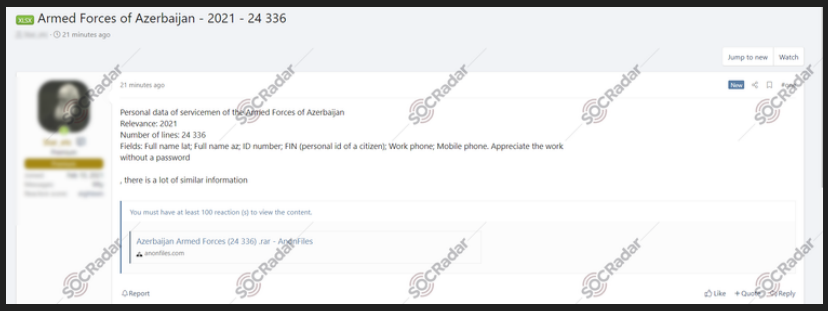
Copyright © 2022 SOCRadar

Major Dark Web Incidents of 2021

Database Sale Detected For A Social Media Platform from Azerbaijan On The Underground Marketplace

On September 9, 2021, an alleged database belonging to one of the biggest chat sites in Azerbaijan was on sale on a dark web forum monitored by SOCRadar. While how the dark web vendor gained access to the database is unclear, it includes the personal information of 91,000 registered users and their chat recordings.

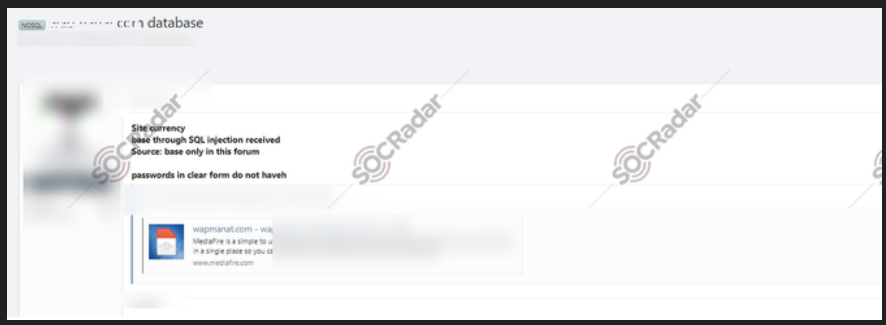
A Personal Database Sale Detected for Azerbaijan



On June 18, 2021, a personal database sale detected for Armed Forces of Azerbaijan on the dark web market. According to the vendor, the database includes more than 24 thousand lines and comprises full names, citizen IDs and mobile phone number which may be used in different social engineering campaigns.

Credential Database Leaked On The Dark Web

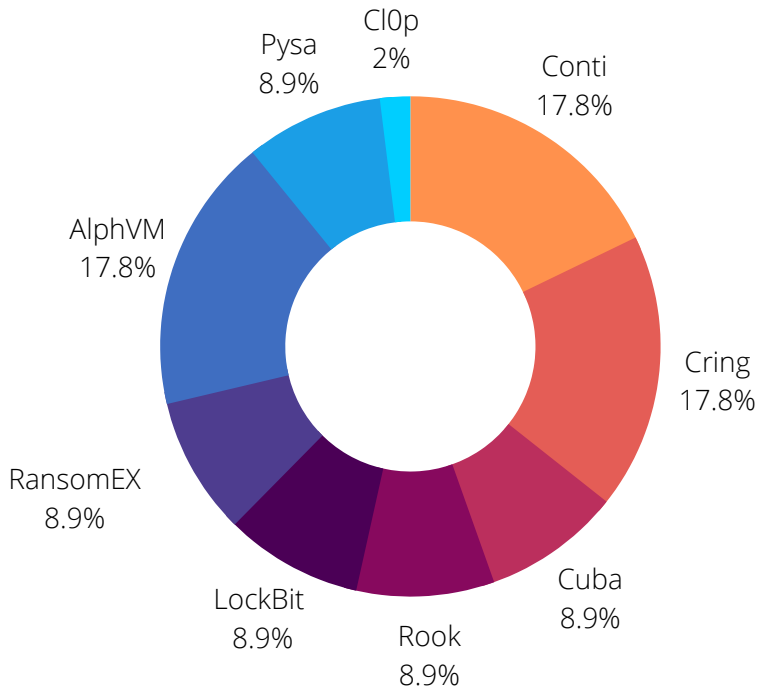
On April 24, 2021, allegedly, a database of a mobile phone operator in Azerbaijan was leaked on a dark web platform. The vendor has mentioned the attack is carried through the SQL injection method and claimed that the database is available on just the forum where the publication was made. Also, passwords were involved in the database.



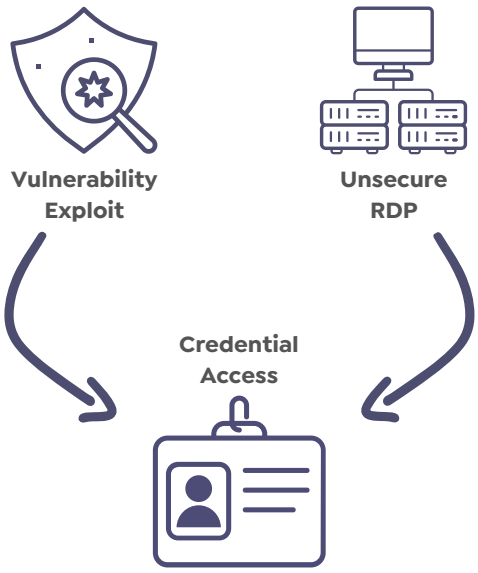
Copyright © 2022 SOCRadar

Ransomware Threats

Ransomware attacks dominated the headlines in 2021. The top 10 ransomware gangs believed to be behind criminal activity had moved about $5.2bn worth of bitcoin over the past three years. Due to tensions between Azerbaijan and Armenia, cyberattacks against these countries have increased significantly in the past year. Concerning verticals, detections affected the banking & finance, and transportation sectors. Ransomware has been consistently attacking crucial industries. Financially motivated ransomware groups gain initial access through compromised RDP, or they can also prefer to get into the system through specific vulnerability exploits.



Distribution of ransomware gang activities targeting the Azerbaijan organizations in 2021



Most preferred methods to gain initial access in ransomware attacks in 2021

Copyright © 2022 SOCRadar

Top Ransomware Gangs Targeting Azerbaijan

LockBit

- Ransomware-as-a-service (RaaS) operator.
- It's one of the best-designed lockers regarding encryption speed and overall functionality.
- Lately, the long list of victims has lately included logistic firms from Azerbaijan.

Conti

- Ransomware-as-a-service (RaaS) operator, operating out of Russia.
- The group has pulled off multiple high-profile attacks on Azerbaijan companies.
- A playbook related to Conti was allegedly released by an affiliate upset with Conti in September 2021.

Cring

- First disclosed and patched in 2019
- Threat actors behind Cring used weaponized tools like Mimikatz.
- The ransomware use Cobalt Strike to distribute BAT files that will be used later for various purposes.

Copyright © 2022 SOCRadar

State-Sponsored APT Activities

Organizations in Azerbaijan continue to be targets of advanced persistent threat actors with diverse motivations. Specific APT groups from China and Iran have recently targeted leading organizations in the military, government, high-tech, and finance verticals. To reach the state goals through the collection of strategic intelligence is believed to be the primary motivation of the state-sponsored actors.

Financial gain through the direct theft of funds is another common motivation. Over the last few months, the SOCRadar CTIA team has observed multiple activities reflecting these motivations by continuously collecting data across the surface, deep and dark web sources while tracking 13 APT groups that have targeted government, military, and private sectors in the past from Azerbaijan.

Significant APT Groups

APT17

Last activity:
November 19, 2021

MuddyWater

Last activity:
November 25, 2021

APT28

Last activity:
October 15, 2021

APT36

Last activity:
September 9, 2021

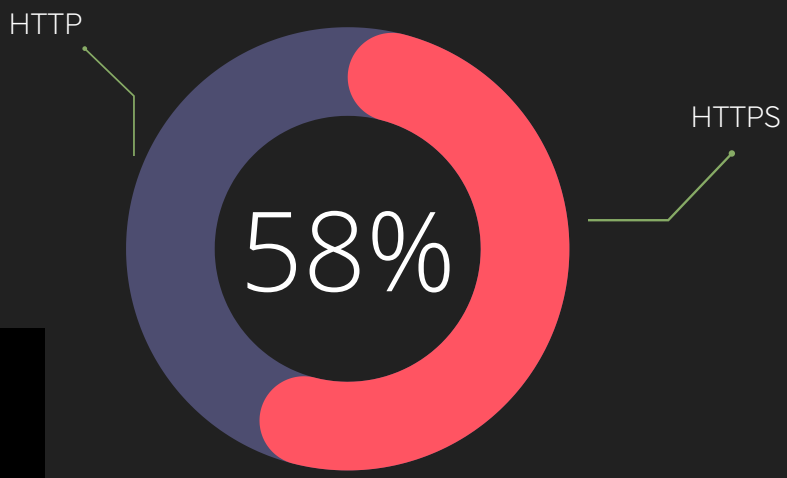
SOCRadar collects Advanced Persistent Threat (APT) IOC Feeds from several public and private sources and sensors. These feeds are free and refreshed daily.

DOWNLOAD

Copyright © 2022 SOCRadar

Phishing Threats

Email phishing remains the top ransomware attack vector. The typical tactic is to deliver malicious macro-enabled Office documents attached to the email. The effects can increase dramatically with business email compromise (BEC) scams and social engineering methods.



Attackers are increasingly using HTTPS
to lure their victims into clicking malicious links

Most used phishing lure keywords: "Whatsapp, Facebook, USPS, Instagram, Event Mobile Legend, DHL"

SOCRadar has detected 339 primary phishing attacks targeting organizations from Azerbaijan since the beginning of 2021. SOCRadar CTIA team is seeing a phishing-enabled fraud trend targeting fast-growing digital industries, including e-commerce, FinTech, and cloud/SaaS.

Search On Phishing Radar

Enter your domain

339
Total phishing attacks detected over the last 1 year

Microsoft
Top SaaS phishing scheme for credential harvesting

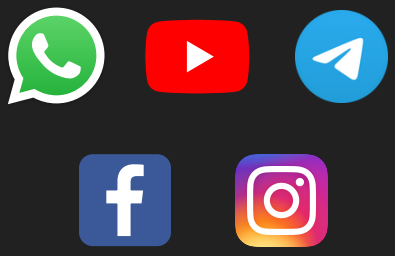
Banking & Finance
Education
Energy
Top targeted sectors in Azerbaijan

Copyright © 2022 SOCRadar

The Digital Industries Commonly Targeted by Phishing Attacks

Comman Platforms

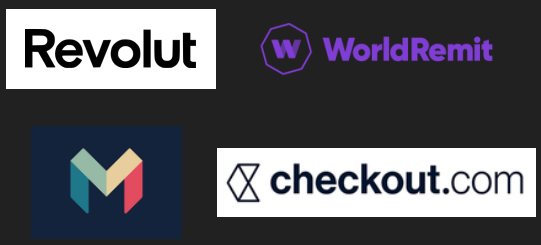
Social Media /IM



Cloud / Webmail

E-commerce

FinTech



Attackers Objective

To distribute malware and steal the social media login credentials of individuals.

To steal the corporate email credentials to gain an initial foothold to the victim's communication channels.

To steal the credentials of individuals/companies and other personal info (PII) for using in fraudulent e-shopping activities.

With London as the "superhub" of FinTech, attackers' objective is to steal the login accounts of individuals/businesses for financial gain or use them in illegal transactions.

Copyright © 2022 SOCRadar

Critical Asset Exposures & Vulnerabilities

When SOC analysts, vulnerability management teams, and security leaders have limited time and budget, prioritizing vulnerabilities to reduce the public attack surface becomes paramount. Following is a high-level statistical view of the critical ports and vulnerabilities on the internet-facing infrastructure and technologies.

Ransomware gangs heavily exploit these as they are exposed, but we can still observe them unpatched or exposed to any remote actors. It is highly recommended to check the technologies listed so far for unpatched, critical, exploited vulnerabilities.

Vulnerable Hosts | CVE ID | CVSSv3

The most commonly exploited vulnerabilities in Azerbaijan.

7	Microsoft Exchange Server Unauthenticated Remote Code Execution Vulnerability	CVE-2021-26855 #ProxyLogon	CVSS: 9.8
52	Open 3389 RDP Port RDP Vulnerability	CVE-2019-0708	CVSS: 9.8
	The Fortinet VPN vulnerable Fortigate SSL VPN endpoint	CVE-2021-13379	CVSS: 9.8

GAIN VISIBILITY INTO HACKERS' PERSPECTIVE

Copyright © 2022 SOCRadar

Identity & Credentials Intelligence

Using stolen credentials is one of the most common initial access techniques leveraged by your adversaries. C-level certificates are significantly more helpful for BEC attackers. Last year, SOCRadar detected more than 1 billion exposed credentials by analyzing the breach datasets shared on the deep and dark web forums, which are tied to plain-text passwords.

However, according to the statistics, digital identity theft is not a significant threat. The Genesis Marketplace is a dark web underground avenue for threat actors to buy digital identities. Currently, there are 65 bots available for Azerbaijan.

65
Bots for sale | Azerbaijan

428K
Total bots for sale

CHECK FOR ACCOUNT BREACH

Enter your domain/email

Critical Incidents in 2021

Due to the war with Armenia, 2021 was a challenging year for the cyber world of Azerbaijan. Governmental organizations and many different sectors were damaged in the attacks.

Surveilance Malware

The Israeli surveillance group developed a surveillance malware named Pegasus that could infect both Apple and Android devices. The governments and law enforcements purchase it. The surveillance attacks targeted activists, politicians, and journalists.

The examination of the published data and the forensics analyses performed on the mobile devices demonstrated that more than 11 countries were purchasing the surveillance software from the Israeli company. These countries included Azerbaijan, Mexico, Hungary and various countries...

Ashes of the 44-day war

The Azerbaijan Government asked for help from international organizations related to the 44-day war, and some information about the attacks appeared at the end of 2021. The workers of an Armenian company conducted the campaigns by collecting a satisfactory database and appealing to international structures. The attacks mainly targeted the Central Bank of Azerbaijan, and there were also cyber-attacks on banking infrastructures. Moreover, there were DDoS attacks and phishing attacks by Armenian hackers. Emails were sent on behalf of the control belonging to banks and the Association of Banks Azerbaijan.

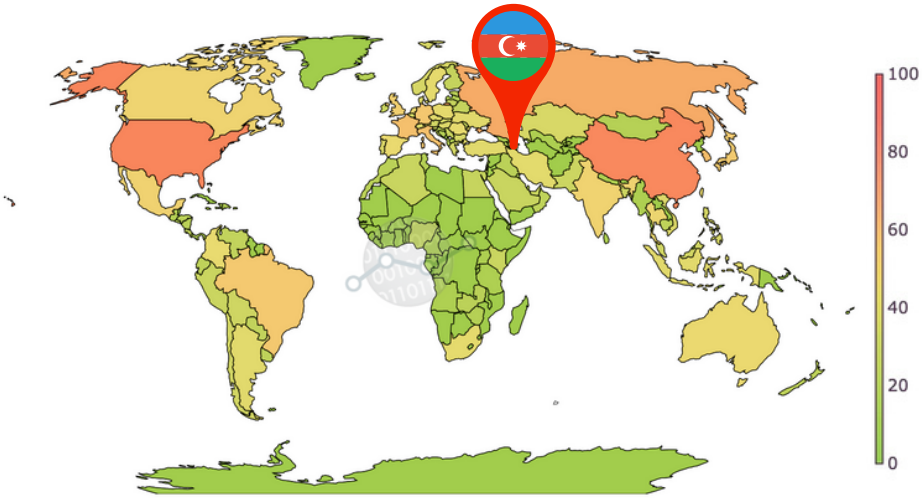
Copyright © 2022 SOCRadar

socradar.io

DDoS | Risk-to-others

The global internet ecosystem is currently vulnerable and carrying high malicious traffic. Sophisticated threat actors take advantage of these weak points for amplifying disruptive DDoS attacks against businesses, resulting in financial losses and critical service disruptions.

Azerbaijan telecommunication, financial and banking entities were also among the victims hit by DDoS attacks in 2021. Based on the global risk condition dataset provided by Cyber Green Initiative, Azerbaijan can generate ~3TBit/sec DDoS traffic, ranking #87 in the world.



Global heatmap view of total potential DDoS bandwidth by country

Data source: CyberGreen

CHECK FOR DoS RESILIENCE

Enter your domain/IP Block

3 TBit/Sec

Azerbaijan | Total DDoS Potential

7,492
Open Recursive DNS

1,338
Open SNMP

4,391
Open NTP

4
Open CHARGEN

46
Open SSDP

Copyright © 2022 SOCRadar

ABOUT SOCRadar®

SOCRadar platform is an all-in-one solution that provides Extended Threat Intelligence, Digital Risk Protection, and External Attack Surface Management. Its false-positive free platform helps companies proactively defend themselves against cyber incidents. SOCRadar is empowered with robust AI algorithms and a highly talented analyst team; together, they eliminate false positives.

FOLLOW US!

If you have a business in Azerbaijan and want to benefit from the solutions offered by SOCRadar, you can contact our valuable partner Prosol in Azerbaijan:

90A Nizami St, Baku, Azerbaijan
+994 12 404 12 21

PROSOL
TECHNOLOGY POWER HOUSE

DISCOVER SOCRADAR® FREE EDITION

With SOCRadar® Free Edition, you'll be able to:

- **Discover your unknown hacker-exposed assets**
- **Check if your IP addresses tagged as malicious**
- **Monitor your domain name on hacked websites and phishing databases**
- **Get notified when a critical zero-day vulnerability is disclosed**

TRY FOR FREE

CONTACT US info@socradar.io +1 (571) 249-4598 651 N Broad St, Suite 205, Middletown, DE 19709