



2021

# Top Cyber Threats for Turkey

## Threat Landscape Report

# CONTENTS

Executive Summary & Key Findings	<b>03</b>
Dark Web Threats On The Rise	<b>04</b>
Recent Dark Web Activities Targeting Turkish Companies	<b>05</b>
Growing Turkish-Speaking Underground Forums	<b>06</b>
Examples of Turkish-Speaking Underground Hacker Community Discussions	<b>06</b>
Skyrocketing Ransomware Threats in 2021	<b>08</b>
Top Ransomware Gangs Targeting Turkey	<b>09</b>
APT Groups Targeting Turkey	<b>10</b>
Significant APT Groups Around Turkish Deep Web	<b>10</b>
Recent APT Activities Round Up	<b>10</b>
Phishing Threats in Turkey	<b>11</b>
The Digital Industries Commonly Targeted by Phishing Attacks	<b>12</b>
Critical Asset Exposures & Vulnerabilities	<b>13</b>
Other Critical Findings	<b>13</b>
Identity & Credentials Intelligence	<b>14</b>
Blackmarket Stats	<b>14</b>
DDoS   Risk-to-others	<b>15</b>

## Executive Summary

As a strategic transit country between Asia and Europe, Turkey remains far from immune to sophisticated cyber-attacks performed by APT groups in an inter-connected world. Turkish businesses and governments are becoming highly digitized with the youngest growing population in Europe, increasing the potential attack surface and exposing the digital assets to notorious threat actors.

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 and their TTPs.

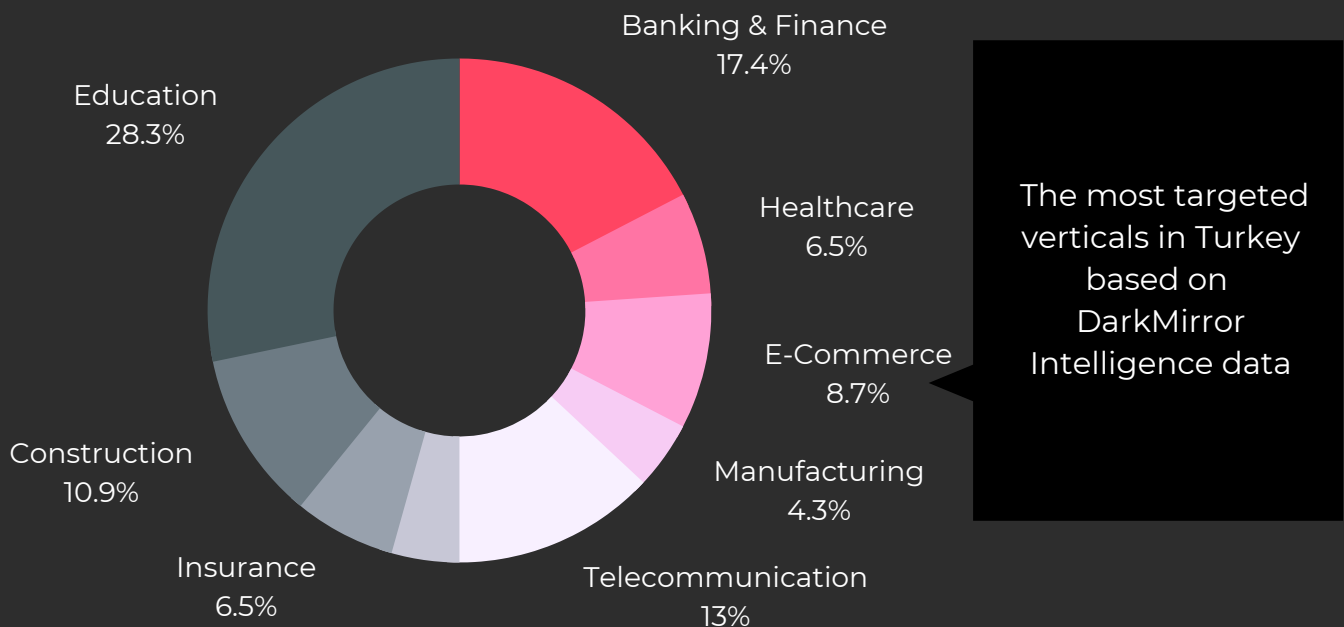
## Key Findings

- There are more than **150 listings of 30 threat actors** targeting the Turkish entities. 22% of these posts were customer database sales, and 9% were unauthorized network access sales.
- E-commerce, banking, and insurance are among the top affected industries.
- The top 10 ransomware gangs believed to be behind criminal activity had moved about \$5.2bn worth of bitcoin over the past three years. Top ransomware groups targeting Turkey are **LockBit, Conti and Xing**.
- Due to its geographical location, Turkey is likely to be targeted by nation-state actors looking to gain influence regarding geopolitics, such as the Russia-Ukraine tension. Significant APT groups around Turkish deep web are **APT28, APT29, APT39 and APT41**.
- SOCRadar detected **42,136 phishing attacks** targeting millions of consumers over the last 12 months.
- The most commonly exploited vulnerabilities beside Logshell are **CVE-2021-31206, CVE-2021-21985, CVE-2020-5902 and CVE-2021-3064**.
- Over the last year, SOCRadar discovered more than **1 billion exposed login data** with plaintext passwords by monitoring dark web forums and marketplaces.
- Turkey can generate ~31Tbit/sec DDoS traffic, ranking number 27 globally.

## Dark Web Threats On The Rise

With various hacking tools, fraudulent methods, and stolen databases available for purchase, the dark web is a springboard to launch cyberattacks. The cyber threats born in the dark web increasingly target and impact the organizations in Turkey.

Based on the data gleaned from SOCRadar DarkMirror Intelligence Portal, there are more than 150 listings of 30 threat actors targeting the Turkish entities. 22% of these posts were customer database sales, and 9% were unauthorized network access sales. These posts listed by threat actors have impacted different organizations from various industries, including finance, telecommunication, and education.



# 158

Threat posts over the last 1 year



# 30

Dark web threat actors / aliases



# Finance | Education

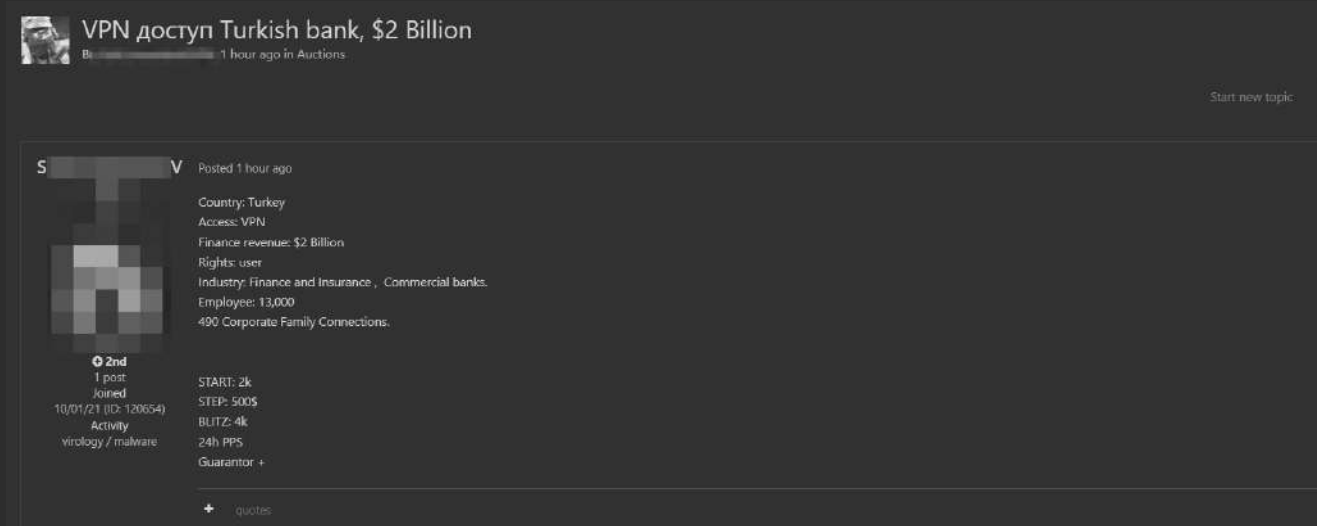
Top targeted verticals



# Customer database

# Recent Dark Web Activities Targeting Turkish Companies

## The Ratio of Deep Web Posts Targeting E-commerce Institutions



VPN доступ Turkish bank, \$2 Billion  
B... 1 hour ago in Auctions

Start new topic

S V Posted 1 hour ago

Country: Turkey  
Access: VPN  
Finance revenue: \$2 Billion  
Rights: user  
Industry: Finance and Insurance, Commercial banks  
Employee: 13,000  
490 Corporate Family Connections.

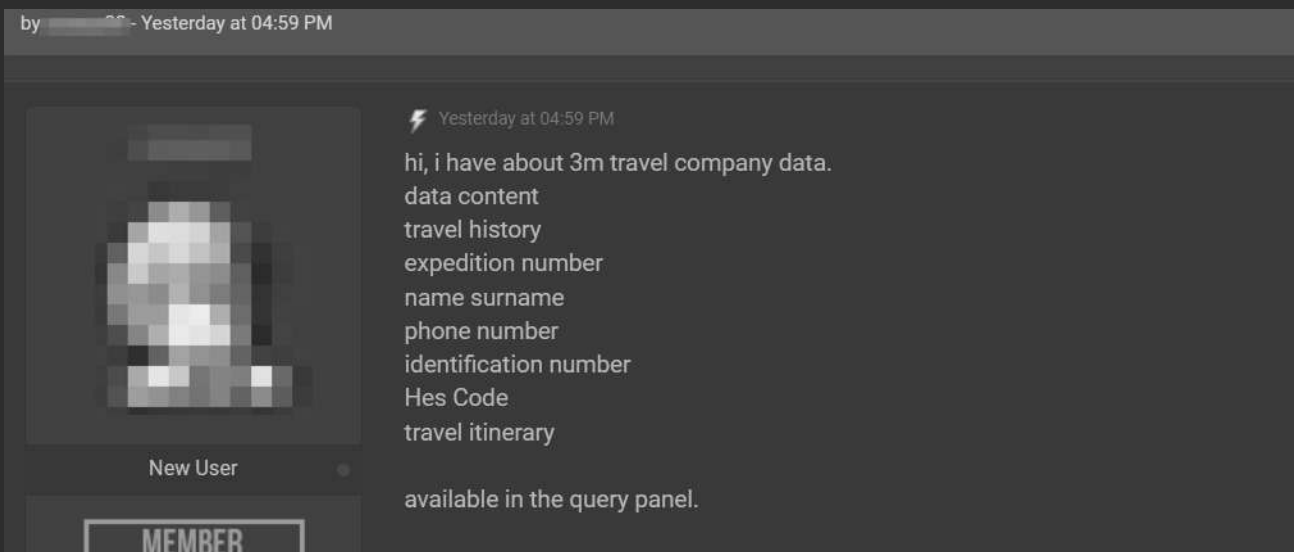
2nd  
1 post  
Joined  
10/01/21 (ID: 120654)  
Activity  
virology / malware

START: 2k  
STEP: 500\$  
BUTZ: 4k  
24h PPS  
Guarantor +

+ quotes

On December 10th, on a dark web forum tracked by SOCRadar, a threat actor attempted to sell unauthorized VPN access allegedly for a Turkish financial institution. While the dark web vendor did not give the name of the victim organization, it is claimed that its revenue is more than \$2 billion with 13,000 employees. The dark web vendor auctioned the VPN access setting a starting price of \$2000.

## Customer Database with 3 Million Lines of a Turkish Travel Company For Sale



by ... - Yesterday at 04:59 PM

⚡ Yesterday at 04:59 PM

hi, i have about 3m travel company data.  
data content  
travel history  
expedition number  
name surname  
phone number  
identification number  
Hes Code  
travel itinerary

available in the query panel.

New User

MEMBER

On November 28th, a dark web vendor offered to sell a customer database for a large travel agency from Turkey on a dark web forum monitored by SOCRadar. According to the listing, the buyer would have various data types, including expedition numbers, full ID details, travel history, and itineraries, consisting of 3 million data lines. The vendor also stated that it's available for potential buyers to query the database to check the validity.

## Growing Turkish-speaking Underground Forums

The Turkish-language underground hacking/fraud forums provide a shelter for criminal hackers to anonymously network and advertise. Through these forums, along with messaging apps, threat actors are exchanging and trading hacking tools for various attacks, including credential stuffing.

E-commerce, banking, and insurance are among the top affected industries. Cybercriminal forum communities are not alone, however. SOCRadar CTIA team is observing a spike in Turkish-speaking hacker activities moving to the remote corners of legitimate IM platforms such as Telegram, ICQ, and Discord.

## Examples of Turkish-Speaking Underground Hacker Community Discussions

### Stealer Virus as-a-Service for Sale on a Turkish Dark Web Forum



An image of a dark web post describing and selling an info stealer malware as-a-Service which can help facilitate future attacks.

### Full-fledged DDoS Attack for Sale to Illegally Disrupt Competitors

A listing for a Distributed Denial of Service attack-for-hire as shown as advertised as a tool to disrupt the competitors' businesses.



SOCRadar opens the door of the deep web securely and efficiently with its search engine for deep web: **ThreatHose**.

[Request a free deep web report](#) today to see what threat actors post about your company.



## POS-compatible Credit Card Cloning Malware for Sale

In this post, the threat actor is selling a malware program to copy&steal payment card data from specific Point-of-sale devices.



## PII Data of 35 Million Turkish Citizens Allegedly For Sale



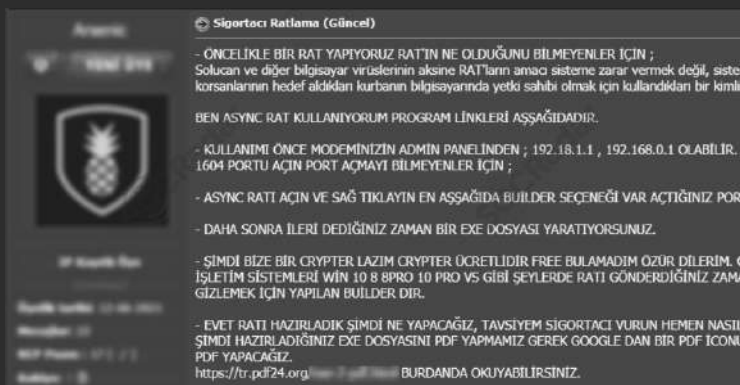
The Central Registration Administration System (tr. MERNİS) data is valuable since it contains citizens' complete address and identity information. This situation can easily use for social engineering attacks.

## Threat Actors Keeping Up with the Credential Stuffing Trend

A threat actor claimed to have accessed and posted 20K+ credentials (username and password) belonging to the customers of an online streaming and media platform. Not surprisingly, it's available for free to gain a reputation for potential future sales.



## Method for Remote Access Tool Targeting Insurance Companies

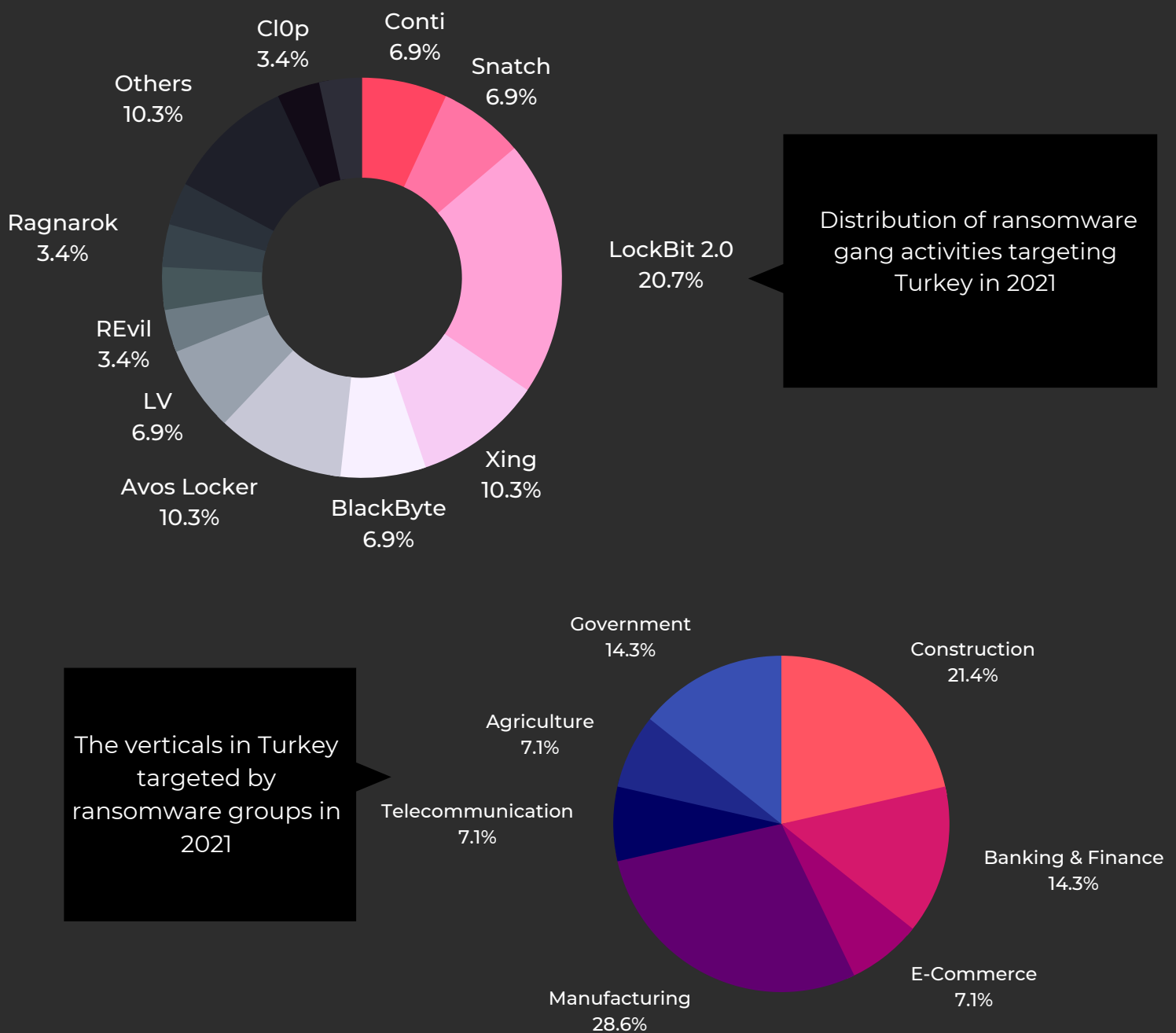


This listing of a threat actor provides a detailed description of AsyncRAT and dives into how it can be used to hack insurance brokers and agencies operating in Turkey.

## Skyrocketing Ransomware Threats in 2021

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. Many global enterprises with large Turkey operations also faced significant attacks this year, disrupting businesses.

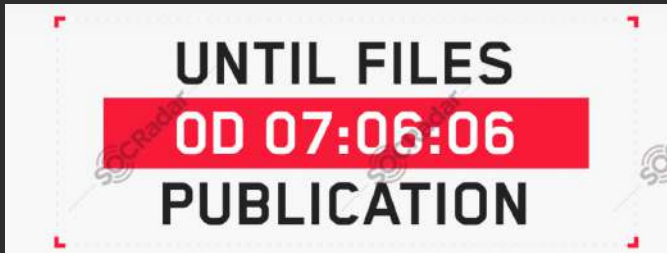
In the last three months of 2021, the increase in ransomware attacks skyrocketed. Alarming, the activities of ransomware groups targeting Turkey more than tripled from June to December 2021. Manufacturing and Finance are the most targeted verticals based on the insights gained from SOCRadar DarkMirror.





## Top Ransomware Gangs Targeting Turkey

### 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 included Schneider Electric, the consultancy firm Accenture, and Bangkok Airways.

### Conti

- Ransomware-as-a-service (RaaS) operator, operating out of Russia.

The group has pulled off several high-profile attacks on the Turkish companies in a broad range of verticals, including pharmaceutical.

- A playbook related to Conti was allegedly released by an affiliate upset with Conti in September 2021.



### Xing



- This name comes from a Mandarin word for "star"
- Assessed to be a rebranding of the MountLocker/Avaddon ransomware
- Targeted Turkish food production and logistics companies
- Using Enterprise Windows Active Directory APIs to worm through networks

## APT Groups Targeting Turkey

Organizations in Turkey continue to target resourceful APT groups with diverse objectives. The sophisticated APT actors frequently target the organizations in verticals with a sheer amount of valuable information and assets that could gain financial advantage, access strategic processes, or gather strategic intelligence.

Due to its geographical location, Turkey is likely to be targeted by nation-state actors looking to gain influence regarding geopolitics, such as the Russia-Ukraine tension. Over the last year, new APT groups like ChamelGang were also identified to be stretching their muscles in Turkey and neighboring countries while energy, critical government infrastructure, and finance remain the top 3 verticals deemed quite attractive.

## Significant APT Groups Around Turkish Deep Web

APT41

Last activity:  
December 27, 2021

APT28

Last activity:  
December 25, 2021

APT29

Last activity:  
December 25, 2021

APT39

Last activity:  
December 14, 2021

## Recent APT Activities Round Up

### New APT Group ChamelGang targeting Turkey through Supply Chain Attacks

In 2021, researchers identified a new APT group targeting fuel, energy, government, and aviation sectors in various countries, including Turkey, the United States, Russia, and Japan. The investigations revealed that the group exploited vulnerabilities such as ProxyShell in Microsoft Exchange Servers and CVE-2017-12149 in the RedHat JBoss Application Server platform.

After gaining the initial access, the attackers installed a modified version of the backdoor called DoorMe and named it legitimate IIS server modules for hiding purposes. The APT group also registered phishing domains and used SSL certificates mimicking legitimate, well-known technology companies like Microsoft, GitHub, and McAfee, which are all known to be commonly preferred vendors for organizations in Turkey. By performing these attack stages in a subsidiary, the group aimed to infiltrate into the leading target organization by compromising trusted supply-chain networks channels.

## Cyberespionage Group Gelsemium targeting Turkish organizations with Complex Malware

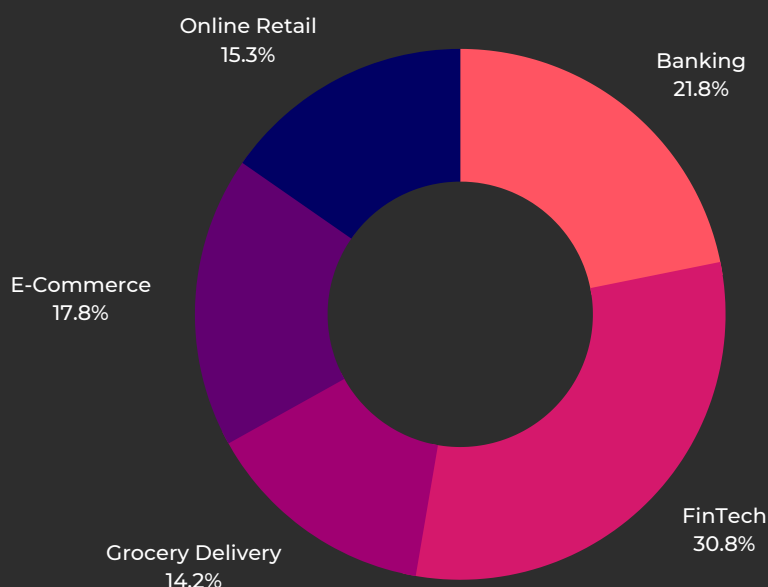
In June 2021, researchers revealed the new campaigns of the Gelsemium group targeting governments, electronic companies, universities, and religious organizations in East Asia and the Middle East. Known to be active since 2014, Gelsemium is showing signs of more sophisticated operational techniques and a higher level of C++ skills by analyzing its new modular malware called Gelsemine.

Experts believe the group is behind the supply chain attack on Nox Player, part of the BigNox Android Emulator, which has more than 150 million users worldwide—exploiting an RCE vulnerability in MS Exchange (CVE-2020-0688) and distributing malicious documents (e.g., resume) in phishing emails are two known initial access vectors the group is leveraging during the attacks. Another typical characteristic of the group is the common usage of Dynamic DNS domain names for malware command&control servers, which are cheaper than regular domain names.

## Phishing Threats in Turkey

Threat actors have been quick to react to the high mobile penetration in Turkey with new digital-born brands such as delivery apps, online retail, and neo banks. Hundreds of phishing domains imitating these companies were registered daily for stealing sensitive information and gaining initial access to internal systems.

As the first choice of major enterprises and banks for Digital Risk Protection Services, SOCRadar detected 42,136 phishing attacks targeting millions of consumers over the last 12 months and proactively disrupted thousands of malicious infrastructures through automation-powered takedown impersonating domains, mobile applications, and social accounts.



The most commonly targeted verticals by cybercriminals based on the data gleaned from SOCRadar's Phishing Domain Alert Generation Data over the last year.



# 42,136

Total phishing attacks detected over the last 1 year



# 10Million+

















Internet users from Turkey are protected from becoming victims of phishing attacks through proactive takedowns.



# FinTech

Top vertical most often targeted by phishing attacks

## The Digital Industries Commonly Targeted by Phishing Attacks

	Attacker Objective	Common Platforms
Social Media /IM	To distribute malware and steal the social media login credentials of individuals.	    
Cloud / Webmail	To steal the corporate email credentials to gain an initial foothold to the victim's communication channels.	   
E-commerce   Retail	To benefit from the popularity of the well-known brands and steal the credentials of consumers/companies and other personal info (PII) for using in fraudulent e-shopping activities.	 
FinTech   Banking	With Turkey having a mobile-first young population increasingly penetrating financial apps, attackers' objective is to steal the login accounts of individuals/ businesses for financial gain or use them in illegal transactions.	    

## Critical Asset Exposures & Vulnerabilities

In the last days of 2021, a new highly-critical vulnerability in the widely used Java logging library (CVE-2021-44228 dubbed #log4shell), Log4j 2, impacted a sheer number of enterprise software applications with dependencies, including security appliances. Attackers immediately began scanning the internet for finding and exploiting this flaw, which is incredibly easy.

Ransomware gangs such as Khonsari and APT groups are also exploiting this vulnerability. While the SOC teams are working hard to detect the vulnerable hosts, SOCRadar Analysts recommend that organizations in Turkey not overlook other well-known vulnerabilities on the internet-facing hosts known to be exploited.

### Internet-facing hosts at risk in Turkey | CVE ID | CVSSv3

(The most commonly exploited vulnerabilities are listed only.)

1924	Microsoft Exchange Server	CVE-2021-31206 #ProxyShell#UnauthRCEvulnerability	CVSS: 9.2
190	VMware vCenter	CVE-2021-21985 #vSphere #PreauthRCEvulnerability	CVSS: 9.8
110	F5 BIG-IP TMUI	CVE-2020-5902 #F5Networks #RCE	CVSS: 10.0
852	Palo Alto Networks VPN	CVE-2021-3064 #GlobalProtect #RCE	CVSS: 9.8

## Other Critical Findings



# 47,354

Exim Mail Server

# 28,000

Open RDP 3389



# 1262

CVE-2014-0160  
#Heartbleed

# 254

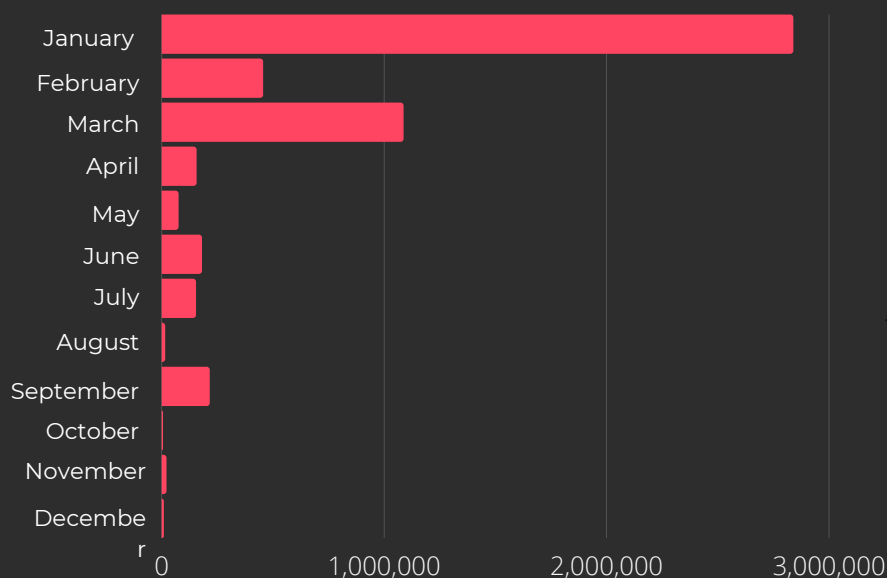
CVE-2019-0708  
#BlueKeep



## Identity & Credentials Intelligence

Using leaked credentials is one of the most effective initial access vectors leveraged by threat actors. Credentials belonging to VIPs are beneficial for BEC attackers. Over the last year, SOCRadar discovered more than 1 billion exposed login data with plaintext passwords by monitoring dark web forums and marketplaces.

When password reuse merges with the lack of 2FA mechanisms, the result can be devastating. Attackers, including ransomware actors, continuously look for easy-to-obtain digital identities to gain an initial foothold into the victim network. Following are the statistics about the current risk situation of Turkey.



Month-over-month  
number of detected  
credentials  
related to TURKEY in  
2021

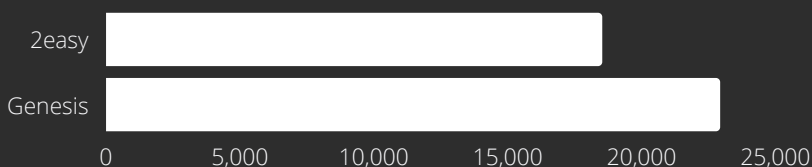
## Blackmarket Stats

41.4K

Turkish bots for sale

1Million

Total bots for sale



"Genesis and 2easy" Black markets are the dark web underground avenues for threat actors to buy digital identities of the bot devices infected by info stealer malware such as RedLine, 2% of which are from Turkey.





# 5.2 Million

## Total leaked credentials

Country code TLDs: com.tr | gov.tr | org.tr | mil.tr | net.tr



# 108.169

## Leaked credentials from government agencies

2020  
4.7M



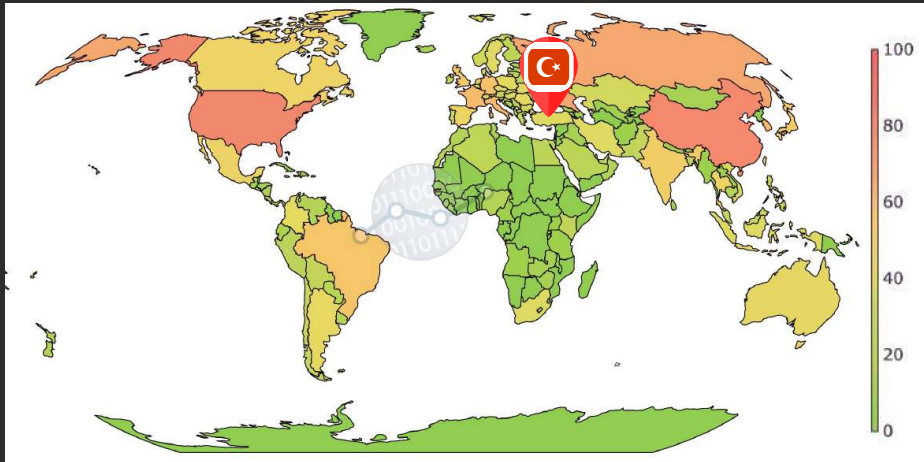
2021  
5.2M

In 2021 alone, SOCRadar has discovered 5.2 million stolen credentials related to Turkey, which added up to a total of 4.7 million credentials found in 2020.

## DDoS | Risk-to-others

The global internet ecosystem is highly connected and vulnerable to disruptive DDoS attacks. Attackers leverage this connectivity with protocol dependencies for amplifying disruptive DDoS attacks against enterprises of all sizes, causing financial losses and outage of services affecting the whole internet ecosystem.

DDoS attacks can be challenging to stop; however, a collective "risk-to-others" mindset can help us all mitigate the global-level risks. Based on the global risk condition dataset provided by Cyber Green Initiative, Turkey can generate ~31Tbit/sec DDoS traffic, ranking #27 globally.



Global heatmap view  
of total potential  
DDoS bandwidth by  
country

Data source:  CyberGreen

Protocol	Bandwidth Amplification Factor
DNS	28 to 54
SNMPv2	6,3
SSDP	30,8
CHARGEN	358,8
NTP	556,9

# 31 TBit/Sec

## Turkey | Total DDoS Potential

### 97,977

Open Recursive DNS

### 9,643

Open SNMP

### 48,595

Open NTP

### 92

Open CHARGEN

### 1,043

Open SSDP

# 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 strong AI algorithms and a highly talented analyst team, together they eliminate false positives.

## FOLLOW US!



### FREE ACCESS

Discover unknown exposed assets, dive into the deep web, and monitor your digital risk for **FREE!**

- Spot malicious/typosquatted domains targeting your business
- Know if your employees' credentials have been compromised in the latest data breach
- 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

**SIGN UP**

### REQUEST DEMO

SOCRadar® provides an early warning system with an extended threat intelligence platform.

See SOCRadar® Platform in action!

 [info@socradar.io](mailto:info@socradar.io)

 +1 (571) 249-4598

**SOCRadar HQ**  
4000 Legato Road, Suite 1100  
Fairfax, VA 22033 USA

**GET A DEMO**

### Radar

SOCRadar® analyzes thousands of incidents throughout the cyberspace

-  **Deep Web Index**
-  **Leaked Large Databases**
-  **Major Cyber Attacks**
-  **Critical Vulnerabilities**
-  **CTI Glossary**
-  **Financial Data Breaches**

**LEARN MORE**

### SOCRADAR LABS

A new and developing platform informing users about existing and possible cyber threats with the help of several XTI® services **FOR FREE!**

-  **Deep Web Report**
-  **VPN Radar**
-  **Account Breach**
-  **IP Reputation**
-  **DoS Resilience**
-  **APT Feeds**
-  **Phishing Radar**
-  **DarkMirror**

**TRY NOW!**

**CONTACT US**



[info@socradar.io](mailto:info@socradar.io)



+1 (571) 249-4598