SOCRadar®

2021

GLOBAL DEEP WEB REPORT

TABLE OF CONTENTS

EXECUTIVE SUMMARY

2021 became the year Cybersecurity affected the daily lives of ordinary people. Cyberattacks caused massive disruptions that affected many government agencies, major companies, and supply chains for essential goods like gasoline, as in Colonial Pipeline Attack. The year started with Cyber Unified Coordination Group of USA blaming SolarWinds Attack.

Then, the infamous Colonial Pipeline Ransomware Attack hit Eastern parts of the USA in May, causing massive disruption of daily life. As ransomware attacks became a nightmare for many sectors, the total damage to the world economy was estimated at around $20 billion during last year. It is expected to rise more than tenfold by 2031.

2022 is started with operations to Ransomware gangs like REvil and VPN providers. Russia's Federal Security Service (FSB) announced it had arrested 14 members of the REvil gang and raided 25 locations associated with the individuals to disrupt REvil's prodigious ransomware operations. Therefore, last words have not been said on Ransomware, and it seems there will be many developments to come.

KEY FINDINDS

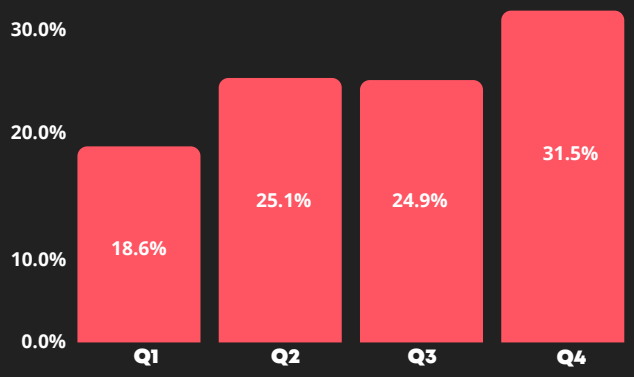
- **The number of deep and dark web posts increased more than 50% in the last quarter compared to the first quarter of 2021.**
- **Ransomware was a more common and a more significant threat in the Americas and Europe than in the rest of the world. For example, according to SOCRadar's U.K. Threat Landscape report, ransomware gangs believed to be behind criminal activity had moved about $5.2bn worth of Bitcoin over the past three years just in the country.**
- **I.T., Government, E-commerce, and Banking sectors focused on the deep and dark web.**
- **Data leaks, i.e., sharing and selling sensitive data about organizations, made up more than 40% of all posts and chatter on the deep web in 2021.**
- **60 % of the phishing domains impersonating legitimate sites have a valid SSL certificate.**

Global Deep Web Analysis

SOCRadar Research Team analyzed more than 13,000 posts and shares on darknet/ deep web forums and hacker channels (Discord, Telegram, etc.) on different mediums to monitor global trends.

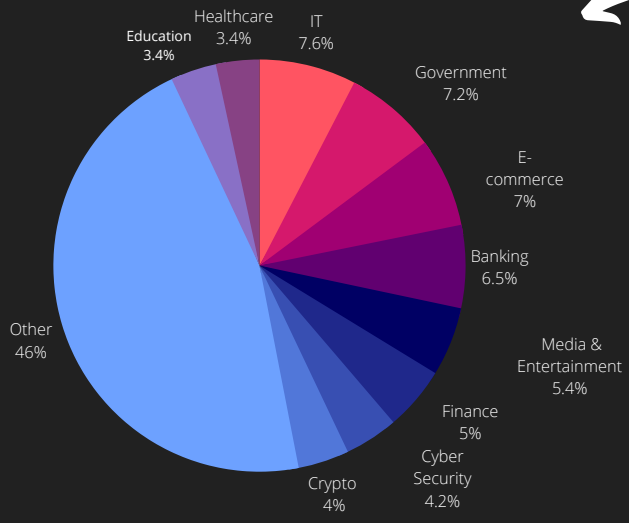
The posts and chatter globally increased throughout 2021. 19% of the chatter happened in the first quarter. In the last quarter that reached almost 32% showing more than 50% increase.

Posts in Hacker Channels Throughout 2021



SOCRadar categorizes industries into more than 40 groups. The top ten sectors that global chatter focused on can be seen in here. Threat actors targeted Information Technologies (IT), Government, E-commerce, and Banking sectors the most in 2021.

Top 10 Industries - Global



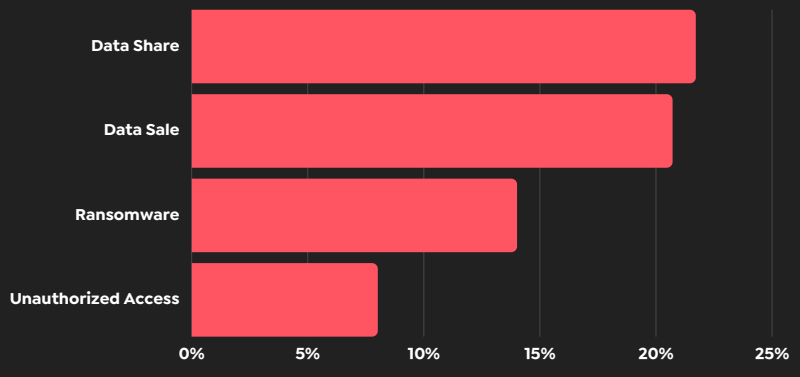
Not surprisingly, the number one issue for deep web posts was data leaks in either form of sale or shared to gain money or anonymity. Data leaks were about 43% of all post researched, followed by ransomware and unauthorized access.

Concerning the deep web post and hacker channel shares, the most mentioned countries during 2021 are

Top 10 Countries

Country	%	Count
United States	23.5%	3113
United Kingdom	4.4%	588
India	3.6%	476
Russian Federation	3.4%	456
France	3.4%	453
Germany	3.2%	426
Canada	3.2%	426
Brazil	3.1%	409
China	2.8%	370
Italy	%20.3	2.2%

Threat Types - Global



Americas Deep Web Threat Analysis

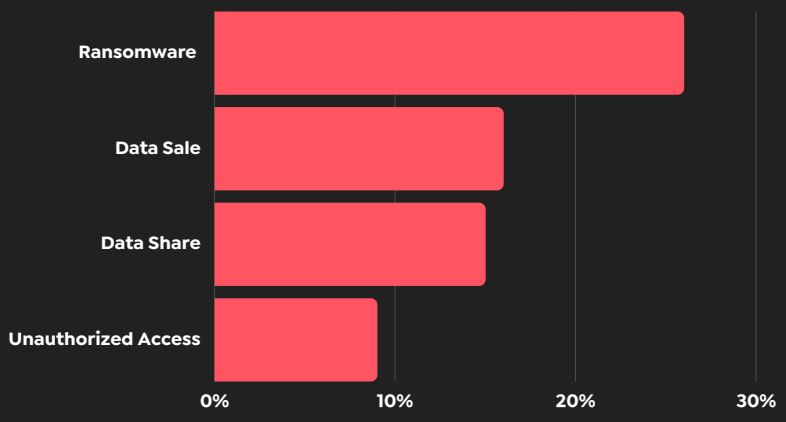
SOCRadar Research Team focused on the posts and shares on darknet/ deep web forums and hacker channels on different mediums to monitor North and South America trends.

The most targeted countries during 2021 on the deep web post and hacker channel shares.

Top 10 Countries - Americas

Country	%	Count
United States	72.4%	3113
Canada	9.9%	425
Brazil	9.5%	409
Mexico	4.7%	203
Argentina	2.3%	98
Colombia	2.2%	93
Chile	1.7%	71
Peru	1.1%	48
Ecuador	0.7%	32
Venezuela	0.7%	32

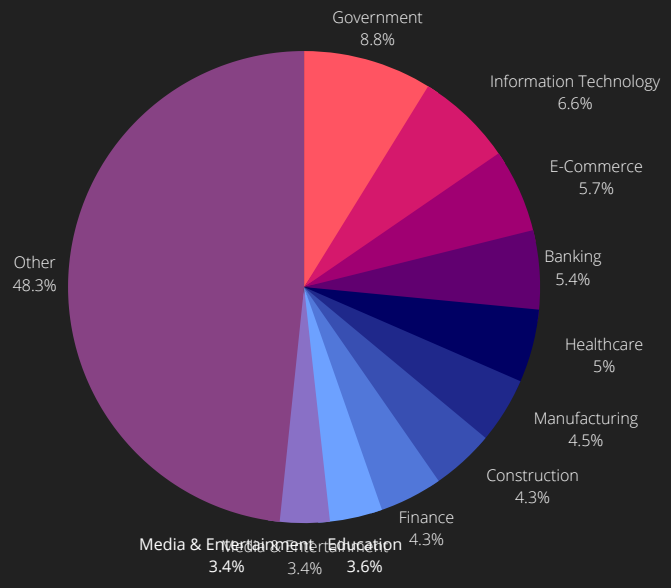
Deep Web Radar for Americas



The chatter aiming at Americas is very different from the rest of the world. The most mentioned topic is ransomware. Given the incidents like colonial pipeline, this is not surprising but a distinct pattern that rest of the world.

Threat actors targeted Government Sector more than Information Technologies in the Americas. The Healthcare sector is also mentioned more compared to Global Trends.

Top 10 Industries - Americas



Europe Deep Web Threat Analysis

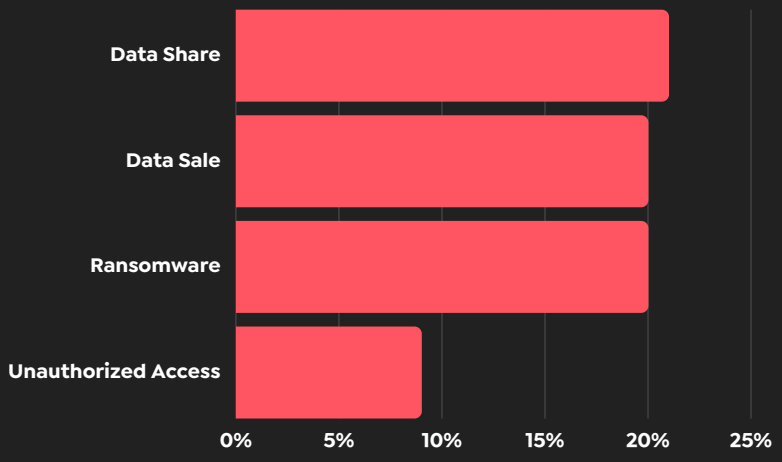
Next, Our team focused on the posts and shares on darknet/ deep web forums and hacker channels to monitor trends in Europe.

The most targeted countries during 2021 on the deep web post and hacker channel shares.

Top 10 Countries - Europe

Country	%	Count
United Kingdom	18.5%	588
Russian Federation	14.3%	456
France	14.2%	453
Germany	13.4%	426
Italy	9.3%	295
Spain	8.3%	263
Turkey	5.6%	178
Netherlands	5.2%	167
Ukraine	4.9%	156
Poland	3.2%	102

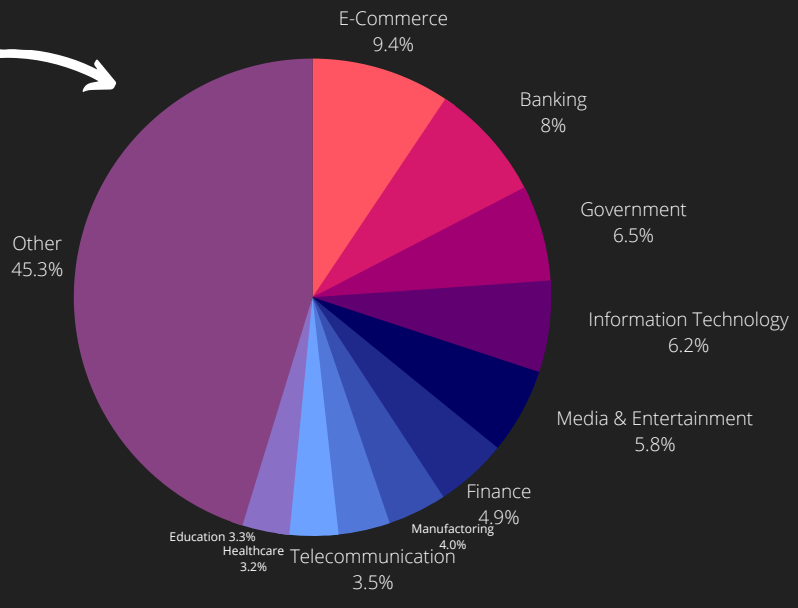
Deep Web Radar for Europe



The chatter aiming at Europe deviates from the global trend, especially with the excessive ransomware posts, 40% more than the worldwide average.

Threat actors targeted E-commerce and Banking in Europe even though Government and Information Technology Sectors focused on global trends.

Top 10 Industries - Europe



Asia & Pasific Deep Web Threat Analysis

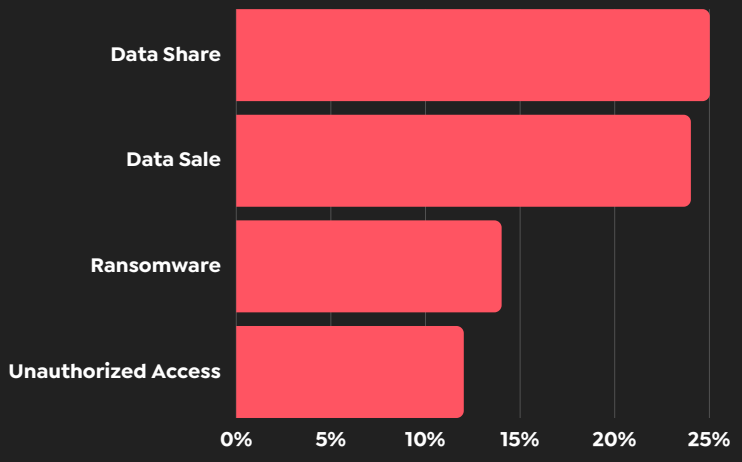
We focused on the posts and shares on darknet/ deep web forums and hacker channels to monitor trends on APAC.

The most targeted countries in 2021 on the deep web post and hacker channel shares.

Top 10 Countries - APAC

Country	%	Count
India	18.5%	476
China	14.4%	370
Australia	11.1%	285
Indonesia	8.7%	223
Thailand	5.0%	128
Japan	4.7%	120
Vietnam	4.2%	109
Malaysia	3.9%	100
Singapore	3.8%	97
South Korea	3.4%	87

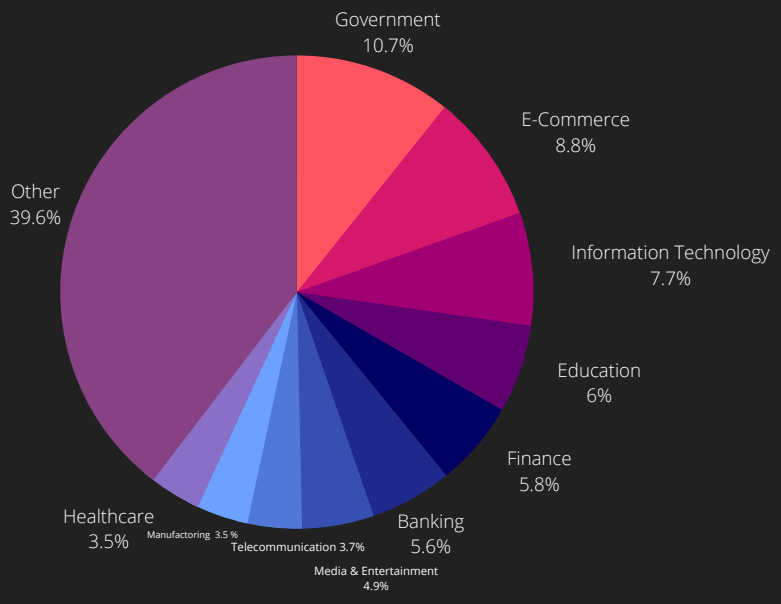
Deep Web Radar for APAC



The chatter aiming at APAC follows somewhat the global trends. Almost half of the chatter is about Data Sale and Data Share.

For APAC, threat actors targeted Government and E-commerce sectors. Education Institutions are also targeted more by the threat actors than the rest of the world.

Top 10 Industries - APAC



Middle East & Africa Deep Web Threat Analysis

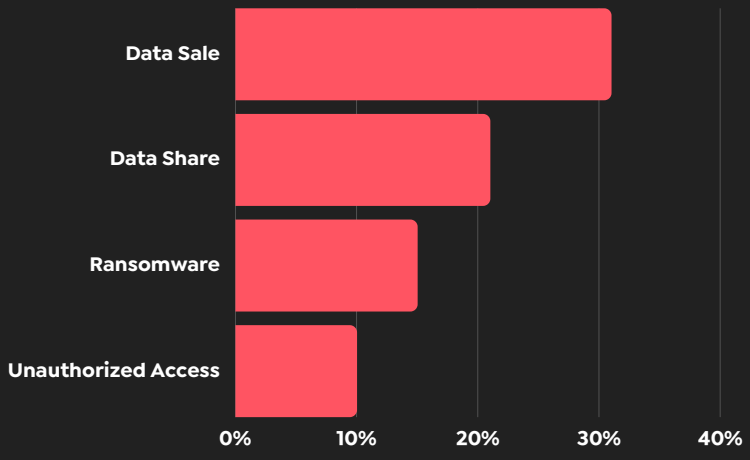
The SOCRadar team focused on the countries most mentioned in deep web posts and hacker channel posts in the MEA region.

The most targeted countries during 2021 on the deep web post and hacker channel shares.

Top 10 Countries - MEA

Country	%	Count
UAE	21.2%	181
Iran	15.0%	128
Israel	14.1%	120
Saudi Arabia	13.6%	116
South Africa	9.8%	84
Iraq	7.6%	65
Oman	6.6%	56
Egypt	6.3%	54
Qatar	4.6%	39
Kuwait	3.0%	26

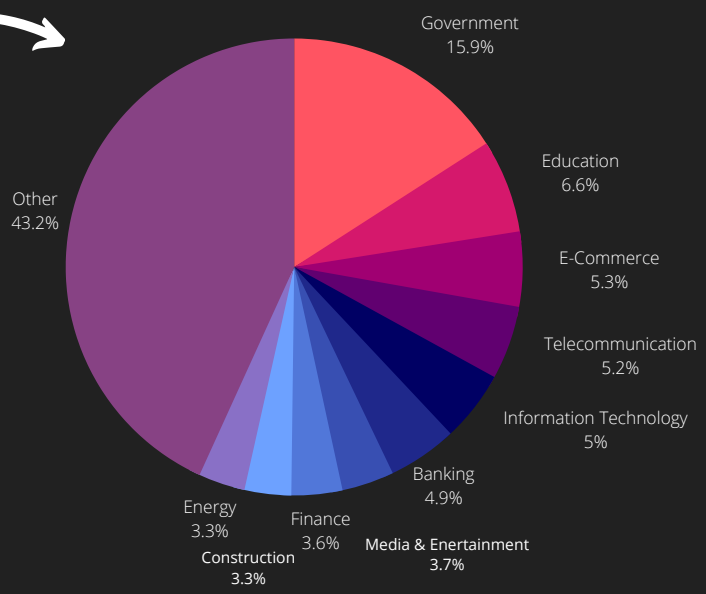
Deep Web Radar for MEA



The chatter about MEA is mostly about Data Leaks, and more than 30% of the posts are about Data sales.

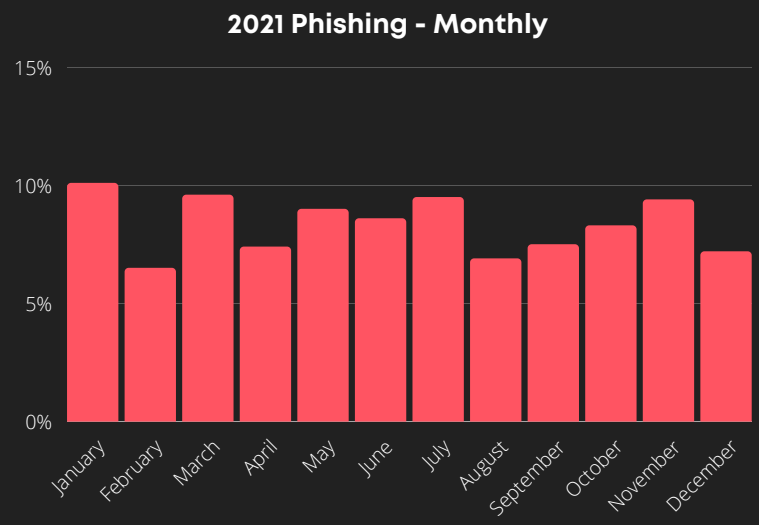
Threat actors targeted heavily Government Sector in the MEA region. There is more chatter compared to the rest about Education and Telecommunication sectors.

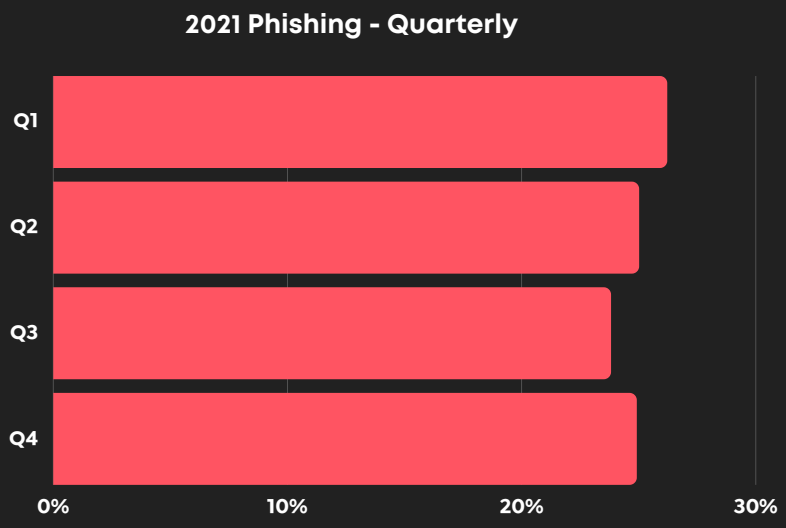
Top 10 Industries - MEA



Global Phishing Threats

Phishing is a tactic that targets victims primarily through emails. Emails appear to be from a legitimate source, but their main objective is to steal their personal information or login credentials by using impersonation.





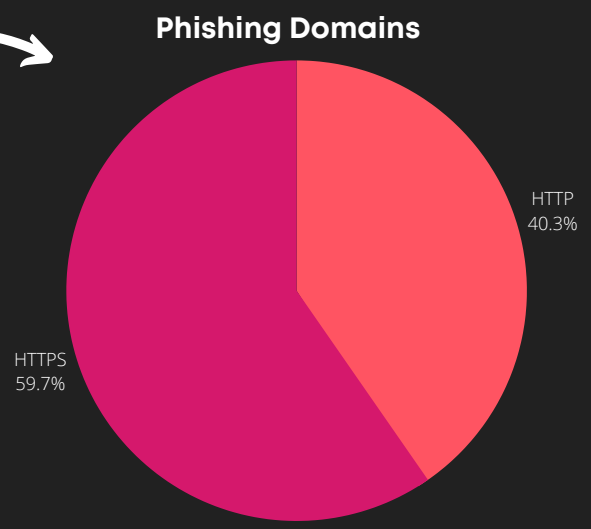
SOCRadar detected and collected almost 700,000 phishing domains impersonating websites in 2021 over the world. Threat actors use phishing domains to lure customers and employees into stealing their credentials and accessing the company systems.

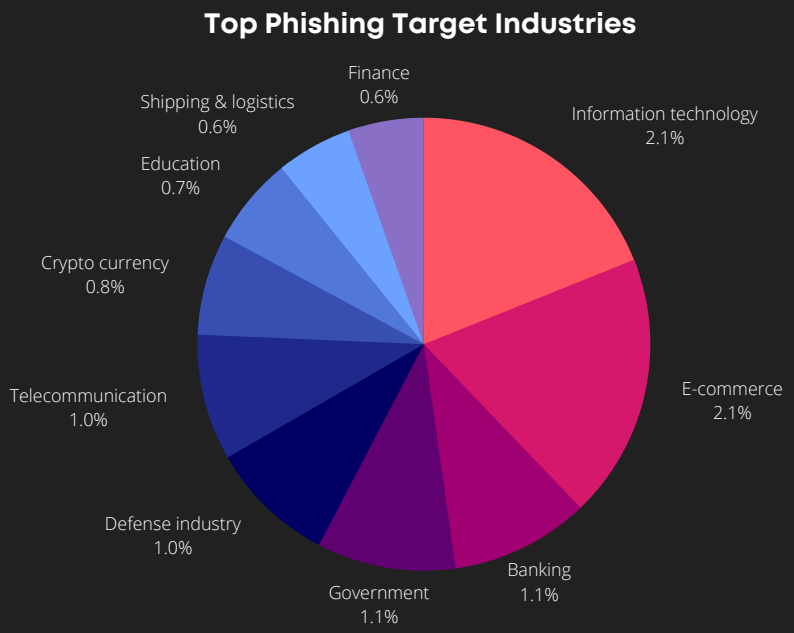
As seen in this table, there were months like February and August when the impersonating sites were significantly fewer. However, phishing attempts remained almost constant when each of the quarters of 2021 was considered.

Top 10 Phishing Target Countries

Country	%
United States	45.2%
Turkey	6.1%
Russia	4.7%
Germany	3.5%
Canada	2.1%
Netherlands	1.8%
Singapore	1.6%
United Kindgom	1.4%
France	1.3%
Hong Kong	1.1%

SOCRadar discovered that globally 60 % of the phishing domains impersonating legitimate sites have a valid SSL certificate.





The top sectors being targeted by phishing domains almost mirrors the sectors discussed dark and deep web posts and chatter. IT, E-commerce, banking, and the government are the most targeted sectors.

Rising Threat : Ransomware

- Ransomware groups have increasingly started to use a tactic called double-extortion, where they not only encrypt and steal a company's data but also exfiltrate it. Then they threaten the company with publishing in public for pressurizing the company to pay the ransom.
- Leading APT Groups in Ransomware: Conti, REvil/Sodinokibi, DarkSide, RagnarLocker, and MountLocker were the most prominent ransomware groups that extorted millions from the victims in 2021. Conti ransomware group received nearly $13 million using the double extortion technique. Russia-based REvil/Sodinokibi group extorted $12.13 million in 2021, and REvil is one of the leading ransomware-as-a-service providers (RaaS).
- On January 14, 2021, Russia's domestic security agency (FSB) arrested 14 alleged members of the REvil ransomware gang, including a hacker that U.S. officials say executed May's Colonial Pipeline attack.

- According to Sophos, 37% of all businesses and organizations will be hit by ransomware in 2021. Out of all ransomware victims, 32% pay the ransom, but they only get 65% of their data back. Only 57 percent of businesses successfully recover their data using a backup. Recovering from a ransomware attack costs businesses $1.85 million on average in 2021.

- The average ransomware payment climbed to a record $570,000 in the first half of 2021 from $312,000 in 2020.

- FinCEN identified 68 ransomware variants in 2021. The most common variants were REvil/Sodinokibi, Conti, DarkSide, Avaddon, and Phobos.

- In 2021, IT management software provider Kaseya became a victim of a ransomware attack. The hackers asked for $70 million – the most significant ransomware fee demanded.

- The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) has identified roughly $5.2 billion worth of outgoing Bitcoin transactions likely tied to the top 10 most reported ransomware variants. FinCEN identified 177 wallet addresses used for ransomware-related payments after analyzing 2,184 Suspicious Activity Reports filed between January 1, 2011, and June 30, 2021.

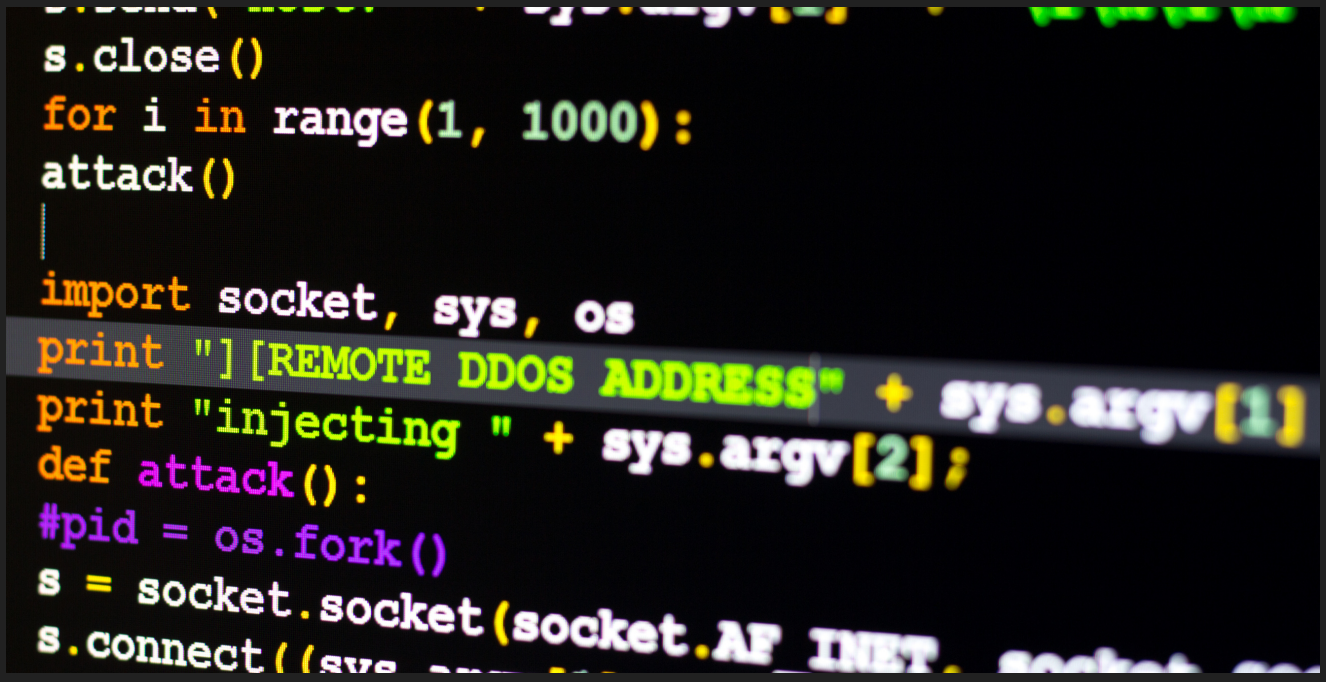
- Cybersecurity firm Coveware reported the most widely reported ransomware families in the first quarter of 2021: Sodinokibi (REvil) — 14.2%, Conti V2 — 10.2%, LockBit — 7.5%.

DDOS Attacks

- Denial of Service is a cyber-attack allowing threat actors to render the website unusable for legitimate users by sending an overwhelming traffic volume. In the case of a distributed denial of service (DDoS) attack, multiple sources of multiple bots from untraceable IP addresses send constant traffic to the target server to crash. As a result, it could cause business disruption, which could be a tremendous bother during the peak business periods. Threat actors use DDoS attacks to pressure ransomware victims or as an extortion tactic.

- According to Cloudflare, more than 20% of DDoS attacks were accompanied by an attacker's ransom note during 2021. This ratio went above 30% in December, just before the sale season for online retailers.

- DDoS attacks related to ransom increased by almost a third between 2020 and 2021. According to a survey by Cloudflare, in the last quarter of 2021, they increased 175% compared to the previous three months.



Meris: New Monster on the Block

- Meris (Latvian for plague) is the name of an active botnet behind a series of recent DDoS attacks. Russian security firm Qrator Labs discovered Meris, a new massive IoT botnet abused for DDoS attacks, in June 2021.

- The botnet size is estimated at around 250,000 infected routers and networking hardware manufactured by the Latvian company MikroTik. The Meris botnet broke the record for the most significant volumetric DDoS attack twice in the third quarter of 2021. This botnet has been primarily used for DDoS extortion campaigns against ISPs and financial institutions across several countries, including the US, UK, Russia, and New Zealand.

Malware

- Cisco defines malware as any intrusive software developed to steal data and damage or destroy computers and computer systems. Common malware includes viruses, worms, Trojan viruses, spyware, adware, and ransomware. Recent malware attacks have exfiltrated data in mass amounts.

- Cisco 2021 Cyber Trends Report explains that crypto-mining, phishing, ransomware, and trojans are the most active threats in the wild. These four threat types averaged internet query volumes of around 100 million each month, whereas the following dozen threat types hovered around 10% of that.

- As of December 2021, Trickbot is the most popular malware used by threat actors. According to Check Point, it impacts 4% of organizations worldwide, followed by Emotet and Formbook, both with a global impact of 3%.

- According to hackmageddon.com, malware is the leading attack technique with 39.4%.

- Web Arx Security reported that 300,000 thousand new pieces of malware are created daily.

- Trend Micro reports that email is responsible for around 94% of all malware.

Vulnerability of the year: Log4J

On December 9thof, 2021, a remote code execution (RCE) vulnerability was reported in the Apache logging package Log4j 2 versions 2.14.1 and below (CVE-2021-44228). Apache Log4j is the most popular Java logging library with over 400,000 downloads from its GitHub project. It is used by many applications to enable logging in applications.

Exploiting this vulnerability is simple and allows threat actors to control java-based web servers and launch remote code execution attacks. The Log4j library is embedded in almost every Internet service or application we are familiar with, including Twitter, Amazon, Microsoft, Minecraft, and more. Log4J could stay with us for years to come because of the complexity in patching it and the easiness of exploitation. CVEs related to Log4j are:

CVE Number	Vulnerability Type	CVSS Score
CVE-2021-44228	Remote Code Execution	10.0 (Critical)
CVE-2021-45046	Remote Code Execution	9.0 (Critical)
CVE-2021-45105	Denial of Service	7.5 (High)
CVE-2021-44832	Remote Code Execution	6.6 (Medium)

RECOMMENDATIONS

1. Keeping Track of the Vulnerabilities on Digital Assets

There are particular vulnerabilities, and sometimes zero-days that threat actors exploit. SOCRadar discovers almost all of your digital assets and their vulnerabilities. SOCRadar's External Attack Surface Mapper tracks your digital assets and the software versions installed on the support and their vulnerabilities. Therefore, you stop attacks before they start.

2. Identifying and Monitoring Threat Actors

Social engineering and phishing are still the starting attack vectors for many cyber attacks. In addition to your company's training for not clicking untrusted links and email attachments without verifying their authenticity, SOCRadar can discover impersonating and typo-squatting domains which could be used for phishing campaigns against your customers and employees.

3. Phishing Control

Many organized threat actors like APTs have signature Tactics, Techniques, and Procedures (TTPs). Some of them are only actives and specific regions and sectors. Monitoring the threat landscape and threat actors will make your defenses stronger. SOCRadar's threat intelligence threat feeds, IOCs, IOAs will give you the proactive readiness you need.

4. Dark Web and Deep Web Awareness

Threat actors often find their way into systems by purchasing credentials or intelligence from dark and deep web forums and chatter channels. SOCRadar monitors these channels and creates alarms and incidents for anything related to your company.

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!

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