



Top Cyber Threats for Financial Institutions

2021

Quarterly Threat Landscape Report

OCTOBER 2021

CONTENTS

Introduction	03
Executive Summary & Key Findings	03
Threats to Financial Institutions on the Rise	04
Deep Web Radar for Financial Institutions	05
Ransomware Threats	07
State-Sponsored APT Groups	08
Malware Targeting Banks and Their Customers	10
Phishing Domains Impersonating Financial Institutions	11
Top 5 Software Vulnerabilities Exploited by Threat Actors	12
The Rising Threat: DDoS Attacks	14
Third-Party/Suppliers Pose a Significant Cyber Risk	14
Recent Major Cyber Attacks Targeting Financial Institutions	15
Recommendations	17
How Can SOCRadar Help	18
References	20

Executive Summary

Financial institutions, especially banks, are always one of the significant targets of threat actors. The number of cyber threats against financial institutions that appeared on the darknet and the deep web has increased in 2021. We analyzed more than 10,000 deep web posts, thousands of chatters on hacker channels, ransomware attacks targeting financial institutions, banking trojans in the wild, DDoS threats, vulnerabilities, and supply-chain threats for financial institutions.

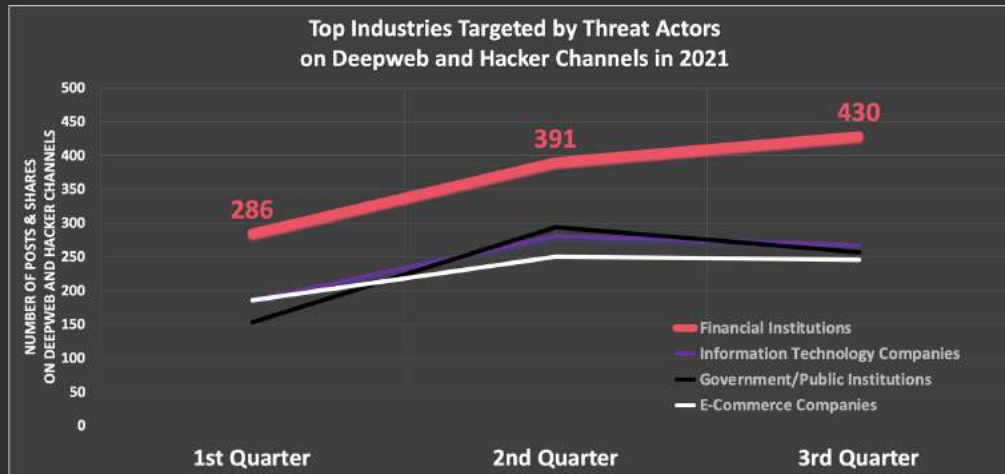
The threat landscape of finance is growing every day, with threat actors' adaptiveness to new technologies and automated tools that enable them to target multiple institutions with one click. Money is always the primary motivation of cybercriminals. To achieve this objective, they steal and sell sensitive data, or they choose extortion, by holding the data encrypted with ransomware, by threatening data sharing, or by executing DDoS attacks. Exploiting vulnerabilities on the supply chain is also an effective method for threat actors to gain access.

Key Findings

- Finance is the top industry targeted based on the number of posts on deep web forums and hacker channels. **11%** of the posts are related to financial institutions in the third quarter of 2021.
- **66%** of posts, targeting finance, belong to threat actors who want to sell or share sensitive data of financial institutions.
- Around 50 ransomware attacks, **Lockbit 2.0** is the ransomware group targeting financial institutions most.
- **14.6** million credit card information is sold on the black market so far in 2021.
- The spread of banking trojans is on the rise.
- The use of DDoS attacks for extortion against financial institutions has increased.
- Threat actors registered more than **2,300** phishing domains in 2021, all impersonating financial institutions. Around **60%** of those phishing domains have a valid SSL certificate.

Threats to Financial Institutions on the Rise

SOCRadar Research Team analyzed around ten thousand posts and shares on darknet/ deep web forums and hacker channels on different mediums.

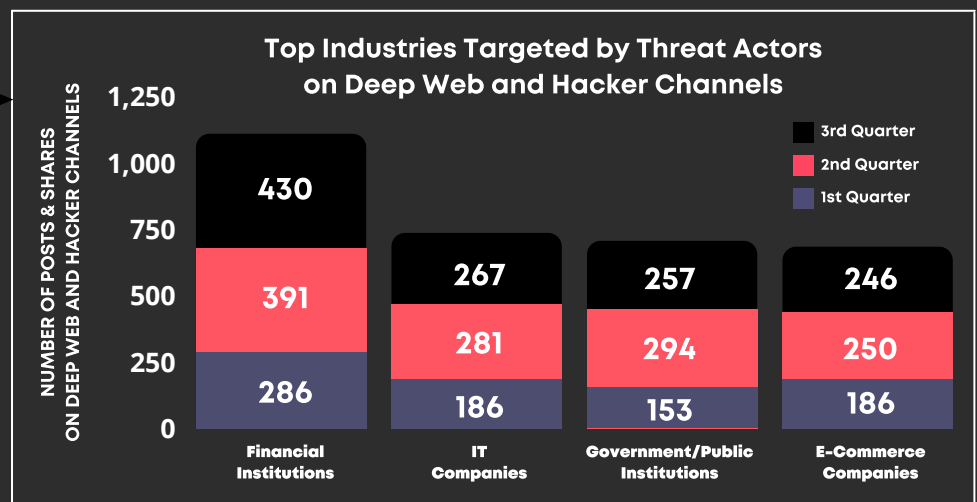


50%

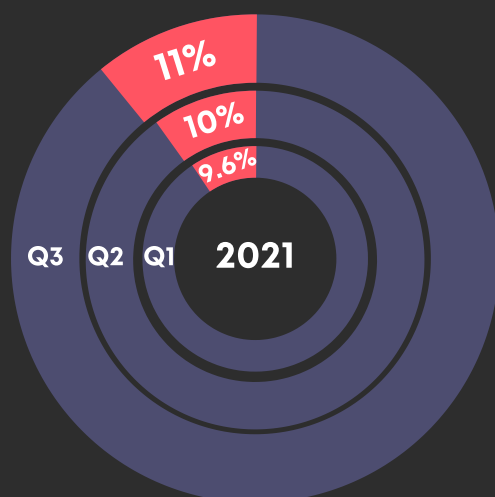
The number of posts targeting financial institutions increased by **50%** in the third quarter of 2021 compared to the first quarter.

TOP INDUSTRY

Finance is the **top industry** targeted by threat actors for the total number of posts and shares on deep web and hacker channels. It is followed by IT firms, government/public institutions, and e-commerce companies.



The Ratio of Deep Web Posts Targeting Financial Institutions



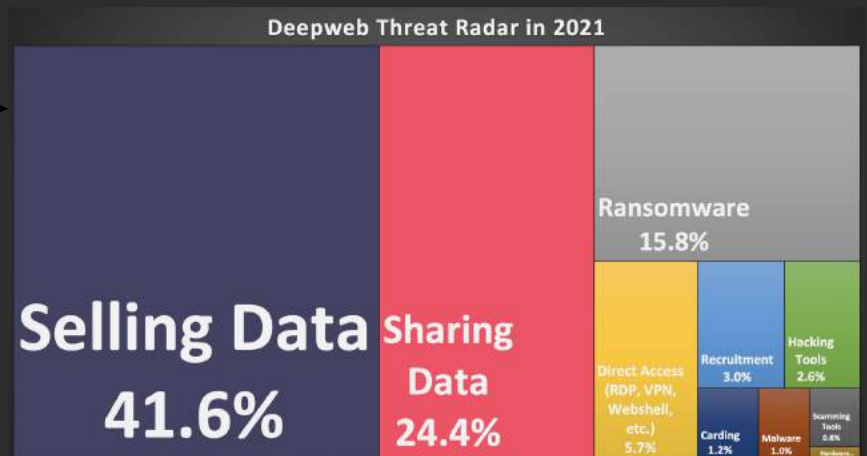
11%

The ratio of deep web posts targeting financial institutions has reached **11%** in the third quarter of this year.

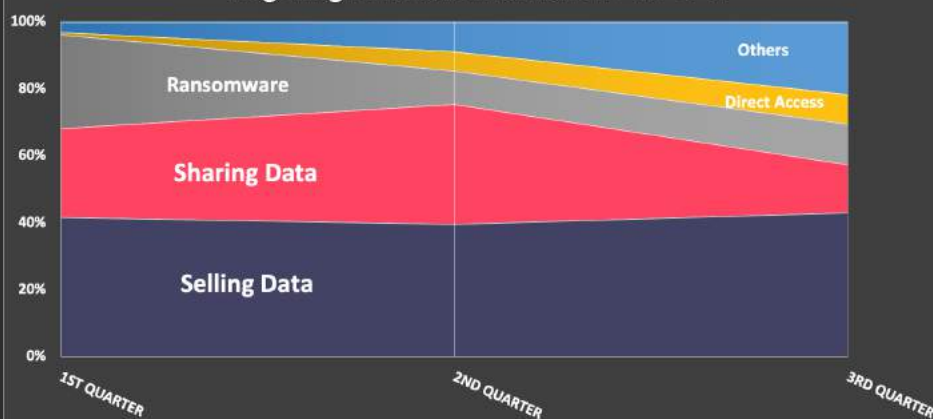
Deep Web Radar for Financial Institutions

Most deep web posts targeting financial institutions are related to sensitive data sold by threat actors. The exposed data on sale includes credit card information, employee PII data, and customer databases.

Data sales are almost **42%** of deep web posts targeting financial institutions in the third quarter of 2021.

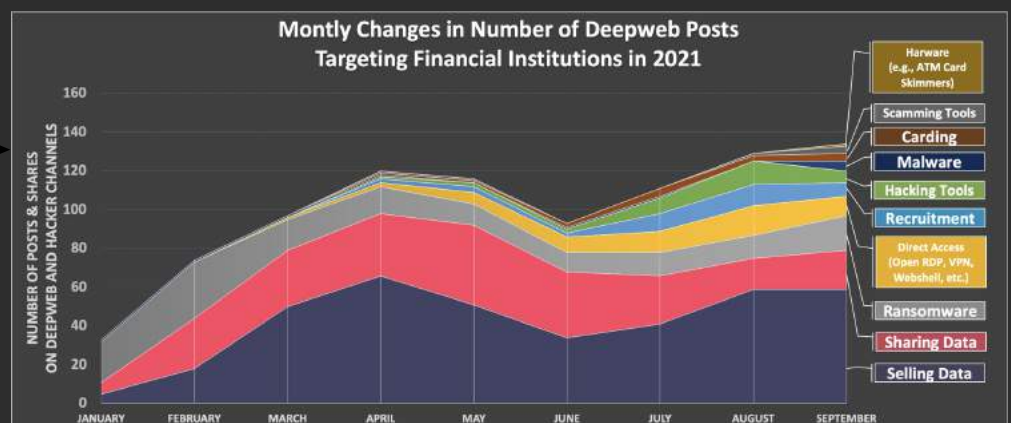


Quarterly Changes in the Ratio of Deepweb Posts Targeting Financial Institutions in 2021



Ransomware groups, still a significant threat to financial institutions, target companies in other industries (especially manufacturing) more in the third quarter compared with the first quarter.

Financial institutions face many other threats. Threat actors exchange hacking tools and malware to target these companies and also share their experience on how to cash out stolen credit cards.



Companies need to work with the right cyber threat intelligence solutions to gain visibility under the surface web.

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

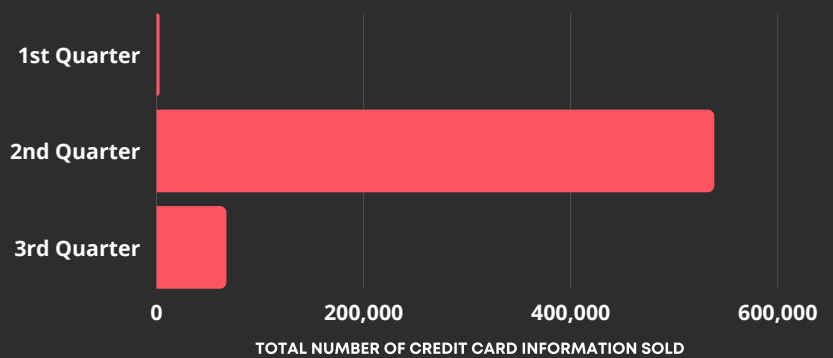
[Request a free deep web report](#) today to see what threat actors post about your company.



14.6 Million Credit Card Information Sold on Black Markets

The total number of credit card information sold on Black Markets and deep web hacker forums in the first three quarters of 2021 is 600 thousand. Even though the validity ratio is at most 10% for these shares, it is still a pretty large number affecting banking customers.

PCI Shared on Black Markets and Deep Web Hacker Forums



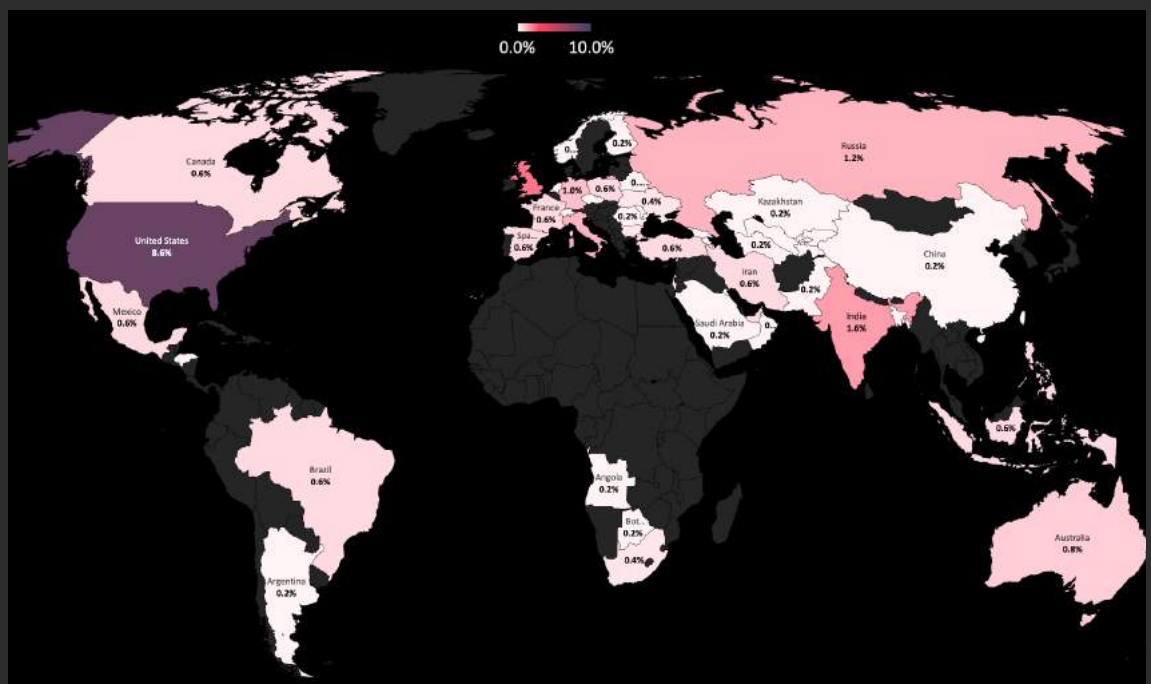
The posts in October so far set another bar with more than 14 million credit card data to be sold on the black markets. Half of them are from a single list posted on October 12.

[SOCRadar](#) closely monitors the black market where credit card information is sold in bulk. If shared, SOCRadar can identify the country and the bank it belongs to and send alarms accordingly.

Most Targeted Countries

Concerning the deep web post and hacker channel shares targeting financial institutions, the most targeted countries in the first three quarters of 2021 are;

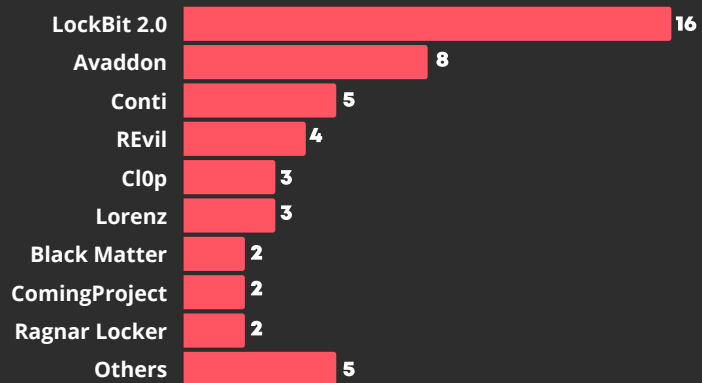
- USA
- UK
- India
- Italy
- Russia
- Germany
- Australia
- Brazil
- Canada
- France
- Turkey
- Spain
- Iran



Ransomware Threats

Various ransomware groups targeted financial institutions in 2021. Lockbit 2.0, Avaddon, Conti, ReVIL, and Cl0p are the head runners. Ransomware groups target fifty financial organizations around the globe.

Ransomware Attacks Targeting Financial Institutions in 2021



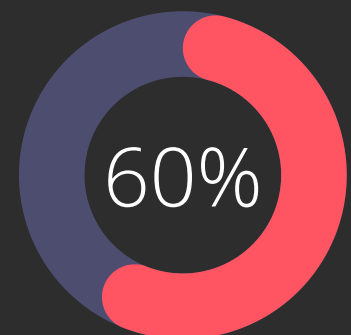
Most Concerning Threat Actor: LockBit 2.0

Many significant ransomware gangs' online presence tends to be limited to affiliate recruitment and their private networks. Over the years, LockBit ransomware operations have been active online, with gang representatives promoting the operation and providing support in hacker forums. Like most Ransomware, the LockBit Group maintains forums on topics that are known as underground web boards to advertise their products. [1, 2]

LockBit is a new ransomware family that exploits widely available protocols and tools such as SMB and PowerShell. Lockbit Ransomware group launched its operations in September 2019, and LockBit Ransomware is recruited by penetrating networks of encrypted devices. In these operations, ransomware services threaten actors to be recruited by breaking through networks of encryption devices.

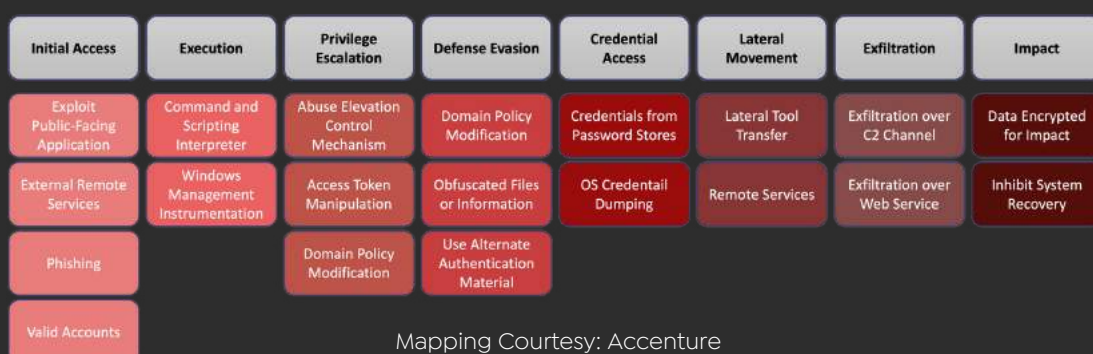
LockBit 2.0 is the most concerning ransomware threat actor for financial institutions, considering two-third of ransomware victims in finance hit by this group in the third quarter of 2021.

Attacks to Financial Institutions by LockBit 2.0 in 2021 Q3



Techniques, Tactics, and Procedures (TTPs) of LockBit 2.0

The new variant of LockBit 2.0 Ransomware can encrypt Windows domains with Active Directory Group Policies. It automates the interaction and subsequent encryption of Windows domains with Active Directory group policies. It adds a novel approach to interact with Active Directory to spread rogue malware to local domains by creating an updated global policy that disables antivirus, making it easier for new malware operators to engage in operations. The below diagram shows the TTPs of the Lockbit 2.0 ransomware group mapped to MITRE's ATT&CK Framework.



Mapping Courtesy: Accenture

State-Sponsored APT Groups

State-Sponsored Advanced Persistent Groups (APTs) and financially motivated threat actors are more organized groups in cyberspace targeting several industries, including finance, with sophisticated attacks. We list three significant threat groups that are active in 2021 and target financial institutions directly or indirectly.

Lazarus

Lazarus (also tracked as HIDDEN COBRA by the United States Intelligence Community), the North Korean state-sponsored cyber threat group, has been an active military hacking group since 2009. They target high-profile organizations such as Sony Films in Operation Blockbuster and multiple banks worldwide and coordinate the 2017 global WannaCry ransomware campaign.

Google spotted Lazarus in January while targeting security researchers in social engineering attacks using elaborate fake "security researcher" social media personas and in a similar campaign in March. [3]

THREAT ACTOR ID CARD

Lazarus

(Hidden Cobra)

Aliases: Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, TG03

SOCRadar®

Type : State-Sponsored (N. Korea)

Motivation : Information theft and espionage, Sabotage and destruction, Financial crime

Tools : Various Malware including BLINDINGCAN

Methods : Ransomware, supply-chain attack, EoP exploits

Target Industries : Aerospace, Engineering, Financial, Government, Media, Shipping and Logistics, Technology and BitCoin exchanges.

Target Countries : Australia, Bangladesh, Brazil, Canada, Chile, China, Ecuador, France, Germany, Guatemala, Hong Kong, India, Israel, Japan, Mexico, Philippines, Poland, Russia, South Africa, South Korea, Taiwan, Thailand, UK, USA, Vietnam and Worldwide (WannaCry)



In late October, researchers discovered that the threat group expanding its supply-chain attack capabilities. The group, by using a new variant of the BLINDINGCAN backdoor for its attacks after deploying to IT vendors. [4]

Companies targeted by the group (including financial institutions) should be aware of IT supply chain risk by monitoring their third parties and gathering intelligence to avoid such attacks.



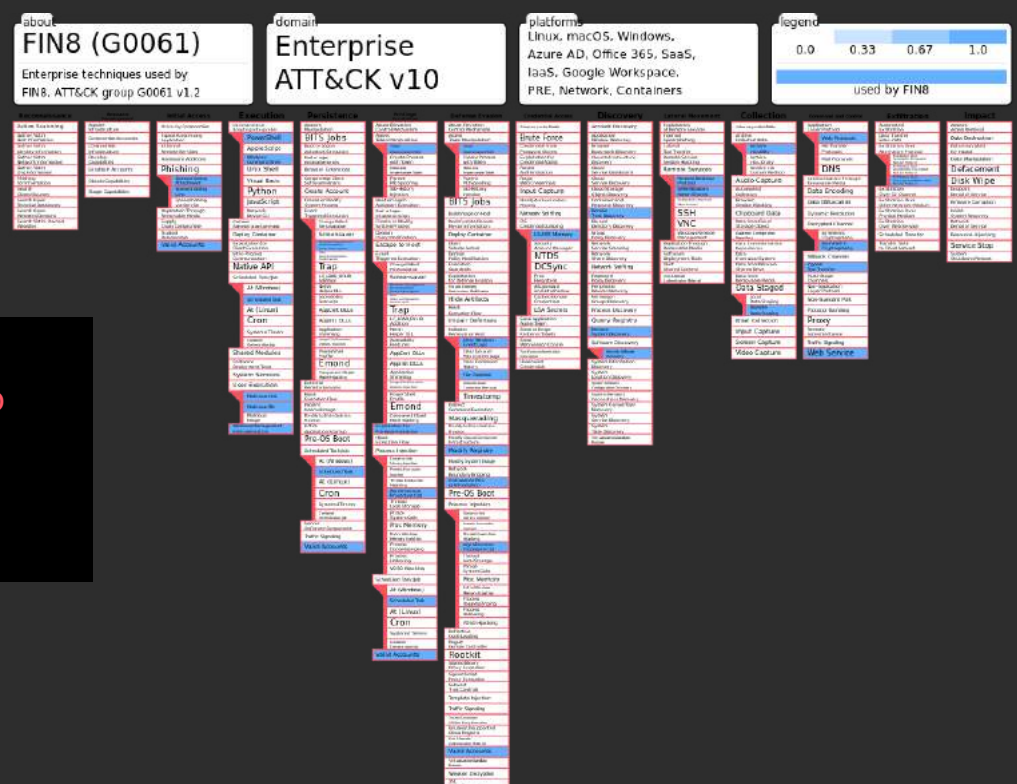
TTPs of Lazarus Mapped to MITRE's ATT&CK Framework

FIN8

FIN8 (aka ATK113) is a financially motivated group targeting the retail, hospitality, entertainment industries, and, recently, financial institutions. The actor had previously conducted several tailored spear-phishing campaigns using the downloader PUNCHBUGGY, backdoor BADHATCH, and POS malware PUNCHTRACK.



In August 2021, researchers discovered an improved version of the BADHATCH backdoor used by FIN8. The new backdoor, dubbed as Sardonic, was deployed during a recent attack against an unidentified financial institution in the US. FIN8 used a three-stage process to deploy and execute the Sardonic backdoor: A PowerShell script, a .NET loader, and downloader shellcode. Researchers stated that the new malware is exceptionally potent as threat actors can leverage various capabilities on the fly without updating components. [5]



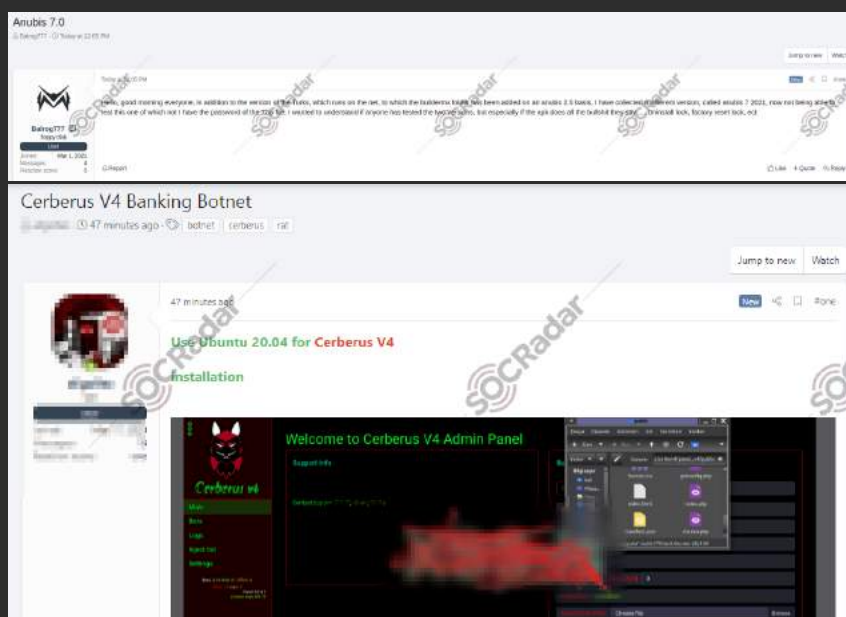
TTPs of FIN8 Mapped to MITRE's ATT&CK Framework

Both ransomware and APT groups pose a significant threat to financial institutions. Threat actor tracking and grasping their TTPs are essential arsenal for security teams of such institutions.

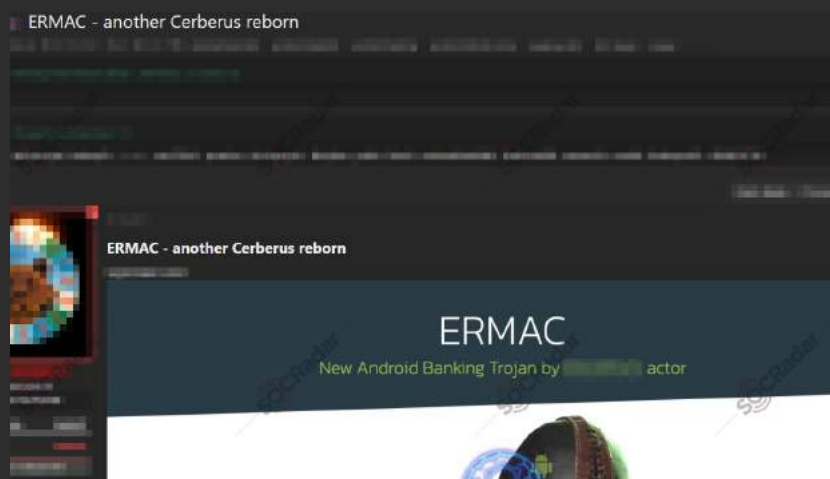
Malware Targeting Banks and Their Customers

With the increase in mobile banking users, we see an increase in banking trojan spreads. The source code leaks of two very effective bots, namely Anubis 2.5 and Cerberus, also contributed to the rapid rise in the number of banking trojans in the wild. With these leaks, threat actors created multiple private trojan versions actively targeting regions such as Poland, Spain, Turkey, and Italy (local actors).

Recent malware families, including Alien or Medusa, developed an approach for advertising by limiting their exposure on public forums and using side channels for the customers to communicate directly with the vendor. [6] On top of that, threat actors can upload the infectious apps by impersonating the legitimate apps to official mobile app stores such as Google Play Store. All these new adaptations enable cybercriminals to spread banking trojans more professionally.



Recent Banking Trojans



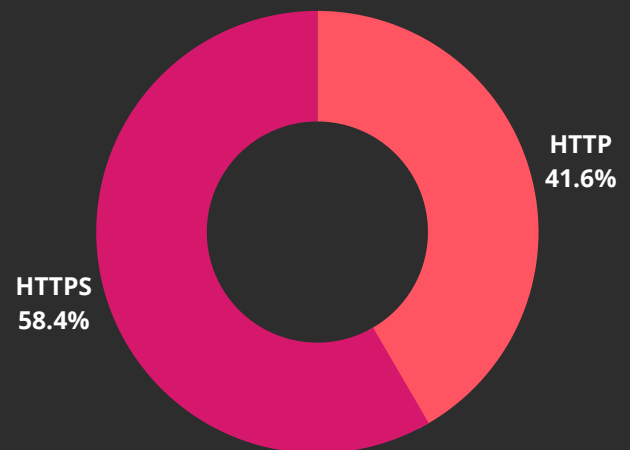
ERMAC: A new banking trojan called Ermac was introduced on a hacker forum in October. Ermac is almost entirely based on the well-known banking trojan Cerberus. The researchers believe that the operator behind this banking trojan is the BlackRock actor(s). BlackRock is another android malware that appeared in 2020 and can "steal" banking and other confidential data of a user.

S.O.V.A.: In August, a new banking trojan dubbed SOVA was introduced in a Russian-speaking hacker forum. The creators of the Android malware claimed that there are already multiple overlays available for different banking institutions from the USA and Spain. The malware is capable of overlay attacks, keylogging, notification manipulation, and also session cookies theft.

Phishing Domains Impersonating Financial Institutions

SOCRadar detected more than 2,300 phishing domains impersonating financial institutions registered in 2021. Threat actors use phishing domains to lure customers and employees into stealing their credentials and accessing the company systems.

While threat actors prefer free registrars to register these phishing domains, they also might get an SSL/TLS certificate to convince the victims about the website's legitimacy. Seeing the HTTPS at the beginning of the URL with a nice padlock sign next to it gives a false sense of security to the users.



SOCRadar discovered that almost 60% of the phishing domains impersonating financial institutions have a valid SSL certificate. It is a very high ratio not observed in phishing domains impersonating companies in other industries.

Top countries targeted by these phishing domains include;

- United States
- Russia
- Turkey
- Germany
- Australia



Takedown of the phishing domains is as important as the detection of them. Thus, a unified extended threat intelligence solution should offer the takedown services on behalf of the customers.

Do you know that on [Gartner's "Competitive Environment: Digital Risk Protection Services"](#) report, SOCRadar is recognized among the [Digital Risk Protection Services](#) and described as a vendor that offers "remediation support beyond standard takedowns or takes a managed service-oriented approach"?



Gartner
peer insights™

4.9
★★★★★

Top 5 Software Vulnerabilities Exploited by Threat Actors

Different threat actors, from APT groups to ransomware operators, from initial access brokers to average hackers, actively exploit software vulnerabilities. Companies disclosing the service version in use are always on the radar of cybercriminals to see whether the service has critical exploitable vulnerabilities or not.

In 2021, some critical 0-day vulnerabilities are exploited by threat actors to attack companies in many industries, including financial institutions. Here are the top 5 critical vulnerabilities widely used by threat actors this year so far:

MS Exchange Server ProxyLogon and ProxyShell Vulnerabilities

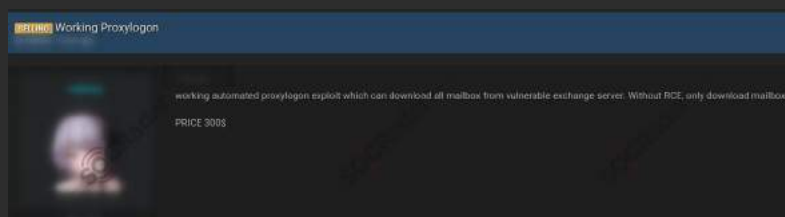
Microsoft Exchange Server users experienced cyber-attacks due to critical ProxyLogon in March and ProxyShell vulnerabilities in April. With the product's wide use in many different industries, threat actors did not lose time to share PoC exploits. Microsoft released patches and security updates for both ProxyLogon and ProxyShell vulnerabilities several days, even weeks later. [8, 9]

ProxyLogon vulnerabilities were chained together to access Microsoft Exchange servers, steal email, and deploy further malware to increase network access. Some ransomware groups such as BlackKingdom and DearCry actively exploited ProxyLogon vulnerabilities to execute their attacks.

ProxyLogon Vulnerabilities
CVE-2021-26855,
CVE-2021-26857,
CVE-2021-26858, and
CVE-2021-27065

ProxyShell Vulnerabilities
CVE-2021-34473,
CVE-2021-34523,
and CVE-2021-31207

SOCRadar detected that working ProxyLogon exploits were still on sale on deep web hacker forums in August.



ProxyShell vulnerabilities consist of three vulnerabilities to bypass pre-authentication, elevate privileges, and post-auth arbitrary-file-write leads to remote code execution (RCE). Even after the patches are available, there are tens of thousands of MS Exchange Servers vulnerable.

Microsoft MSHTML Remote Code Execution Vulnerability (CVE-2021-40444)

In September, the remote code execution (RCE) security flaw, tracked as CVE-2021-40444, was found in the MSHTML Internet Explorer browser rendering engine used by Microsoft Office documents. The PoC exploits appeared on the deep web the same day. Microsoft released a patch two days later. [10]

Windows NTLM PetitPotam Vulnerability (CVE-2021-36942)

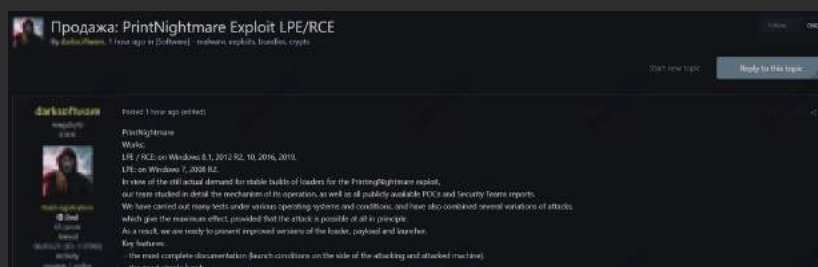


A new NTLM relay attack called PetitPotam was discovered in July. It allows threat actors to take over a domain controller and thus an entire Windows domain. [11]

LockFile ransomware gang actively used the vulnerability to deploy ransomware to target systems. Microsoft published a security update in the second week of August. [12]

Windows Print Spooler PrintNightmare Vulnerability (CVE-2021-34527)

In June, another vulnerability that allowed domain takeover was PrintNightmare. It is a remote code execution vulnerability affecting all Windows versions. Microsoft published multiple mitigations about the vulnerability. [13]



VMWare vCenter Server Vulnerability (CVE-2021-22005)

VMWare vCenter Server, a widely-used server management solution to manage virtualized hosts and machines in enterprise environments. Attackers can exploit vulnerability, that appeared in September to execute commands and software on unpatched vCenter Server deployments by uploading a specially crafted file. VMWare published a security update a few days later. BlackMatter ransomware group targeted vulnerable VMWare servers to deploy ransomware. [14, 15]

Gartner states that only roughly one-eighth of all vulnerabilities in the past decade were exploited in the wild. Many are frequently reused and leveraged in a wide range of threats, such as Remote Access Trojans (RATs) and ransomware. Taking external-facing vulnerable services into perspective, SOCRadar is committed to providing you with actionable insights and context while speeding up the prioritization process.

The Rising Threat: DDoS Attacks

Threat actors execute DDoS attacks against financial institutions, especially banks, with various objectives. Considering that a DDoS attack experienced by a bank can cost millions of dollars to the company, threat actors mainly use DDoS as an extortion tool. According to [a recent report published by FS-ISAC](#) in February, more than 100 financial services firms were hit by a DDoS extortion attack conducted by the same actor last year. [16]

The second reason for DDoS attacks is to create a distraction. While executing a DDoS attack by using a botnet and keeping the security team busy, threat actors infiltrate the company's systems by other means.

Recent DDoS Attacks on Financial Institutions

[A top European bank experienced a DDoS attack](#) in June. The attack reached over 200 gigabytes of volume in total. The threat actors hit the company with three waves of DDoS attacks in one hour. The motivation behind the attack was unknown. [17]

In September, [a massive DDoS campaign](#) against the New Zealand companies resulted in service outages for businesses including ANZ New Zealand and Kiwibank. The internet banking app and website were offline for several hours. It was not the first time New Zealand became the victim of large DDoS attacks. Last year, threat actors forced New Zealand Stock Exchange to be offline for almost an entire week and asked for ransom to stop the DDoS attacks. [18]

Third-Party/Suppliers Pose a Significant Cyber Risk

Financial institutions' digital ecosystem includes many vendors in different industries. SWIFT Companies, First-party Collection Vendors, Credit Reporting & Specialty Agencies, Financial Software Vendors, Identity & Technology Firms, Interbank Network Providers, Know Your Customer/Anti-Money Laundry (KYC/AML) Vendors, and Payment Providers are some of the vendors of interest. Threat actors usually aim for the weakest link in the vendor ecosystem to gain access to or obtain sensitive data of multiple financial institutions with one hack.

[A recent report](#) showed that the top 5 vendors of financial institutions that can cost millions of dollars in case of a cyberattack due to their poor cybersecurity posture are [19];

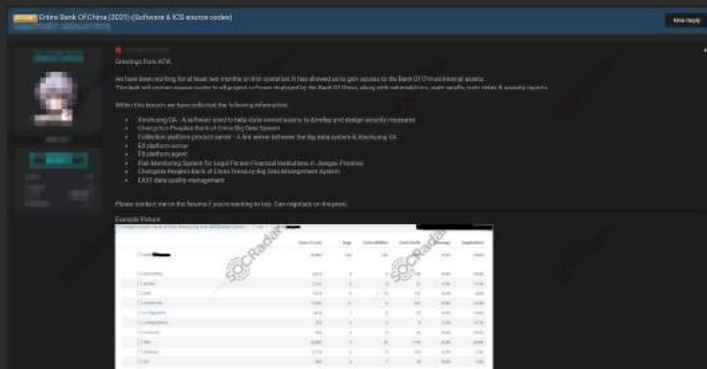
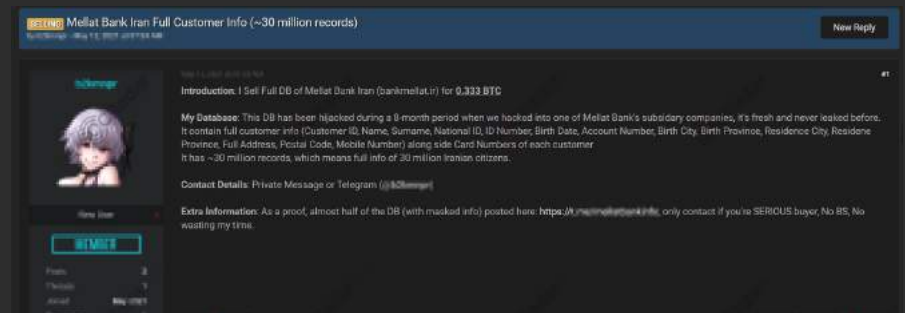
- Financial Software Vendors,
- Credit Reporting & Specialty Agencies,
- Payment Providers,
- Financial Data Vendors, and
- Interbank Network Providers.

Recent Major Cyber Attacks Targeting Financial Institutions

In the last year, the deep web was filled with threat actors sharing or selling data that belong to financial institutions. We list some major claims by threat actors below.

Mellat Bank

In May, SOCRadar detected a threat actor selling a database allegedly belonging to an Iranian bank. The database includes sensitive information of 30 million citizens of Iran.

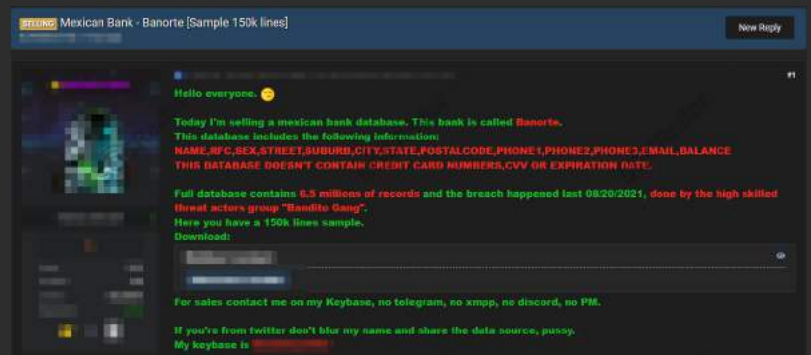


Bank of China

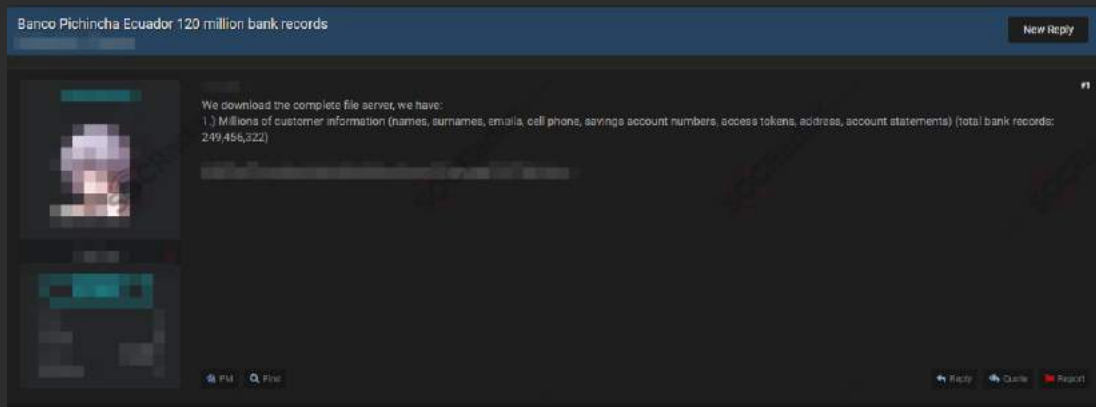
In this particular post published in October, threat actors claim that they worked on this attack for two months to gain access to the bank's internal assets. They allegedly obtained source codes to all project software deployed by the Bank of China, including "vulnerabilities, code smells, code debts, and security reports."

Banorte

In August, a threat actor posted a sale of a Mexican bank's database. A hacker group called Bandito Gang allegedly breached the database that contains 6.5 million records. The threat actor also shared sample data that consists of 150 thousand lines.



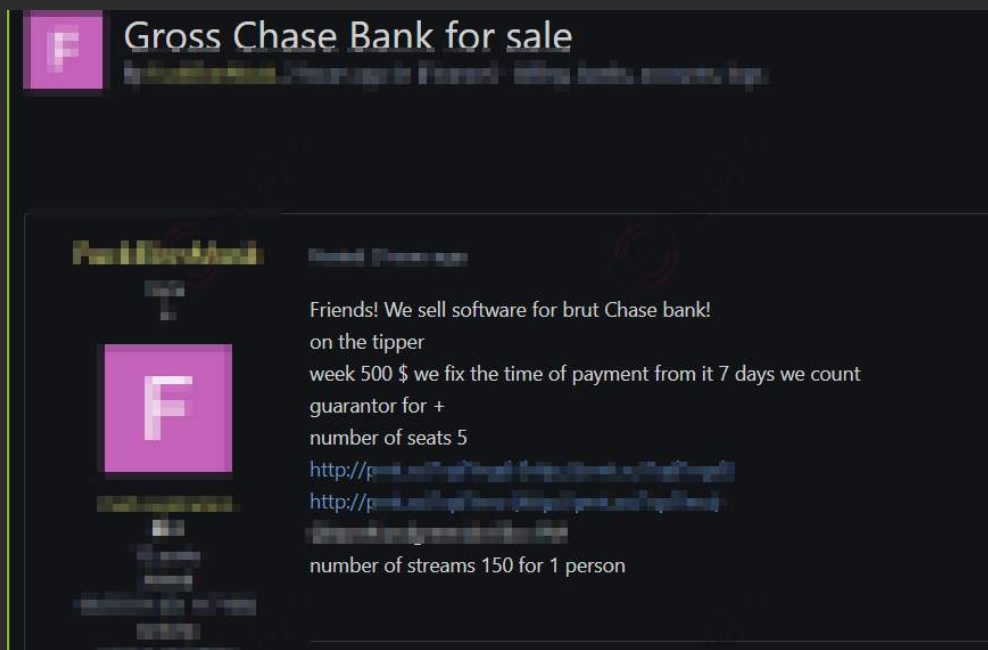
Banco Pichincha



In July, on a hacker forum monitored by SOCRadar, threat actors claimed that they have 120 million bank records allegedly belonging to Banco Pichincha of Ecuador.

Chase Bank

Some leaks are just because of technical errors or some misconfiguration. On August 17, Chase Bank admitted to having a technical bug on its online banking website and app that allowed accidental leakage of customer banking information to other customers. Chase Bank sent a notice to its customers on the following days. [20]



Interestingly enough, three days later, SOCRadar detected a software to execute brute force attacks on Chase Bank is on sale on a deep web hacker forum. If a company is on the news because of a leak, even if the leak is due to an error, cybercriminals may target the company because it may look to have a poor cybersecurity posture.

RECOMMENDATIONS

As all criminals, cybercriminals target financial firms because that is where the money is. And they are not going to stop anytime soon. Plain and simple. However, defending financial institutions against cybercrime needs to happen on many levels. As the European Central Bank (ECB) president, Christine Lagarde, put it, a well-organized cyber-attack on major financial institutions could lead to a financial crisis. Therefore, a global effort is needed against cyber threats in terms of international collaboration among governments, financial institutions, and technology and cyber security firms.

When we are expecting global collaboration, some precautions could be taken. For those, SOCRadar can help. Cyber-attacks are not a matter of "if" but "when" for financial firms.

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 and updates your assets and their vulnerabilities.



2. Identifying and Monitoring Threat Actors

Many organized threat actors like APTs have signature Tactics, Techniques, and Procedures (TTPs). Some of them are only active in 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.

3. Phishing Control

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



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.

In addition to these steps, there are more things to protect yourself, such as:

- You could create strict identity and access management policies by utilizing multiple-factor authentication (MFA) and one-time-password (OTP) technologies.
- You could protect your endpoints using trusted security software as much as possible.
- You must have backup policies and practices. In addition, you should have multiple recent copies (preferably at least one offline) of your critical data and settings and configurations of your security devices.

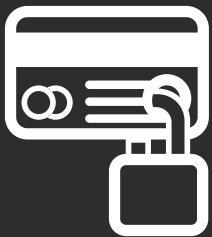
SOCRadar provides extended cyber threat intelligence (XTI) that combines,

- [Cyber Threat Intelligence](#),
- [Digital Risk Protection](#), and
- [External Attack Surface Management Services](#).

SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the era of transformation.

Darknet and Deep Web Monitoring

SOCRadar's fusion of its unique dark web Recon technology with the human analyst eye achieves further to provide in-depth insights into financially-targeted APT groups and threat landscape.



Credit Card Monitoring

Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

Protecting Customers' PII

Scan millions of data points on the surface web, deep web, and darknet to accurately identify the leakage of your customers' personally identifiable information (PII) in compliance with regulations.



360-Degree Visibility

Achieve digital resiliency by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

See SOCRadar in action!

Free Access Now



HOW CAN WE HELP?

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

 +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

 +1 (571) 249-4598



4000 Legato Road, Suite 1100
Fairfax, VA 22033 USA

References

- [1] [The Story of Lockbit Ransomware](#)
- [2] [What Is Ransomware-as-a-Service \(RaaS\)?](#)
- [3] [New campaign targeting security researchers](#)
- [4] [APT trends report Q3 2021](#)
- [5] [FIN8 Threat Actor Spotted Once Again with New "Sardonic" Backdoor](#)
- [6] [The Rage of Android Banking Trojans](#)
- [7] [SOCRadar Recognized as DRPS Vendors in Two Gartner Reports](#)
- [8] [Automatic on-premises Exchange Server mitigation now in Microsoft Defender Antivirus](#)
- [9] [Description of the security update for Microsoft Exchange Server 2019, 2016, and 2013: April 13, 2021 \(KB5001779\)](#)
- [10] [Microsoft MSHTML Remote Code Execution Vulnerability](#)
- [11] [CVE-2021-36942 Detail](#)
- [12] [KB5005413: Mitigating NTLM Relay Attacks on Active Directory Certificate Services \(AD CS\)](#)
- [13] [CVE-2021-34527 Detail](#)
- [14] [CVE-2021-22005](#)
- [15] [VMSA-2021-0020.1](#)
- [16] [MORE THAN 100 FINANCIAL SERVICES FIRMS HIT WITH DDOS EXTORTION ATTACKS](#)
- [17] [Quarterly Threat Intelligence Report: Q1, 2021](#)
- [18] [ANZ New Zealand back online after outage from DDoS attack](#)
- [19] [2020 BLACK KITE FINANCIAL RISK REPORT](#)
- [20] [Chase bank accidentally leaked customer info to other customers](#)