An Overview of FinTech Threat Landscape

blog.cyble.com/2021/08/20/an-overview-of-fintech-threat-landscape/

August 20, 2021

Research shows that there has been a considerable increase in digital threats targeting financial firms since the onset of the pandemic. The statistical reports released between 2020-2021 show that cyber-attacks on financial firms and services have increased by 238%. Out of these attacks, nearly 75% of the victims were banks and insurance companies.

Attackers have been widely targeting financial institutions such as banks and insurance companies, which we observed more frequently since the onset of the pandemic. Attackers benefit monetarily by misusing and selling sensitive Personally Identifiable Information (PII) such as customer details, Social Security Numbers (SSN), driver's licenses, bank account details, and transactional records. Attackers gain access to the system by exploiting any security vulnerabilities that they can identify.

Attackers also leverage Advanced Persistent Threats (APT) campaigns towards financial institutions for sensitive data extortion. One such example, "APT34", is a suspected Iranian group targeting financial institutions.

A few banking botnets and spyware variants such as DanaBot and TrickBot, which initially targeted specific areas, have expanded into other regions like Europe and Asia.

Over 100 financial groups were targeted using Distributed Denial of Service (DDOS) attacks executed via their zombie networks. The US Department of Treasury's Financial Crimes Enforcement Network published a report stating that approximately a billion dollars were stolen from financial institutions each month because of cybercrime activity.

Interestingly, we observed a rise in attacks on mobile users using fake banking apps aimed at major financial institutions. Attacks on financial firms are often state-sponsored, aimed against a specific country's economic situation.

Some of the collective threats that target financial institutions are:

- Phishing
- Brute-Force
- Ransomware
- Stealer/Bot (Spyware)
- Trojan

Tactics:

After compromising the financial institution's data, the attackers use the sensitive information gathered to launch a more sophisticated attack on their consumers.

Another method used by attackers is to target the financial firms by identifying the loopholes in the services provided by these institutions, such as e-commerce, net banking, payment transactions online, and cryptocurrency services.

Around 94% of attacks observed targeting financial firms are performed using common cybercrime tactics such as spear phishing, social engineering, watering hole, etc. Attackers also combine and reuse old but effective malware variants such as the FakeSpy Android banking trojan, which spreads via smishing messages and steals sensitive information from the victim's device.

Telecommunication networks and companies also play a crucial role in financial transactions for security and 2-factor authentication mechanisms such as One-Time-Password (OTP).

Before attacking the customers, attackers utilize malicious applications which have already been installed on the victim's device to gain knowledge about the network service provider. They then employ this information to compromise and disrupt the OTPs required for verification of transactions and hijacking and rerouting the text messages.

Threats:

Attackers use open-source and social engineering tools to build customized malware for the specific purpose of targeting financial sectors. The attackers constantly refine malware variants by adding additional features to automate the exfiltration of stolen data and funds.

Banking malware is one of the best examples of an Automation Transfer System (ATS) engine and a web injection script to automate the fund-initiated bypassing authentication mechanism.

Some of the top cybersecurity threats that target financial services captured in our regular threat intelligence were analyzed, and information regarding these threats is shared below.

Endpoint Threats:

The threat landscape is growing day by day with various methods and techniques, which expands potential attack surfaces. Among many endpoints threats, the topmost persistent attacks that target financial sectors are phishing and ransomware attacks.

Based on our research, we've listed detailed information on endpoint threats below:

Phishing Attacks:

Attackers use phishing as the most common tool to targeting financial sectors. The ease of access and minimum technical knowledge required in building phishing campaigns to launch malware attacks make it the preferred method of attacking financial firms for several attackers.

Statistical reports published by the FBI and Statista reveal that about 40% of attacks that target financial firms use various phishing emails and URLs. The most impersonated cloud brand and social media brands are Microsoft and Google, respectively. Attackers routinely create fake Microsoft login pages to steal PII data.

Figure 1 depicts phishing attempts aimed at financial industries based on the services they provide. Financial and payment platforms are the most targeted services, accounting for 25% and 9% of the total.

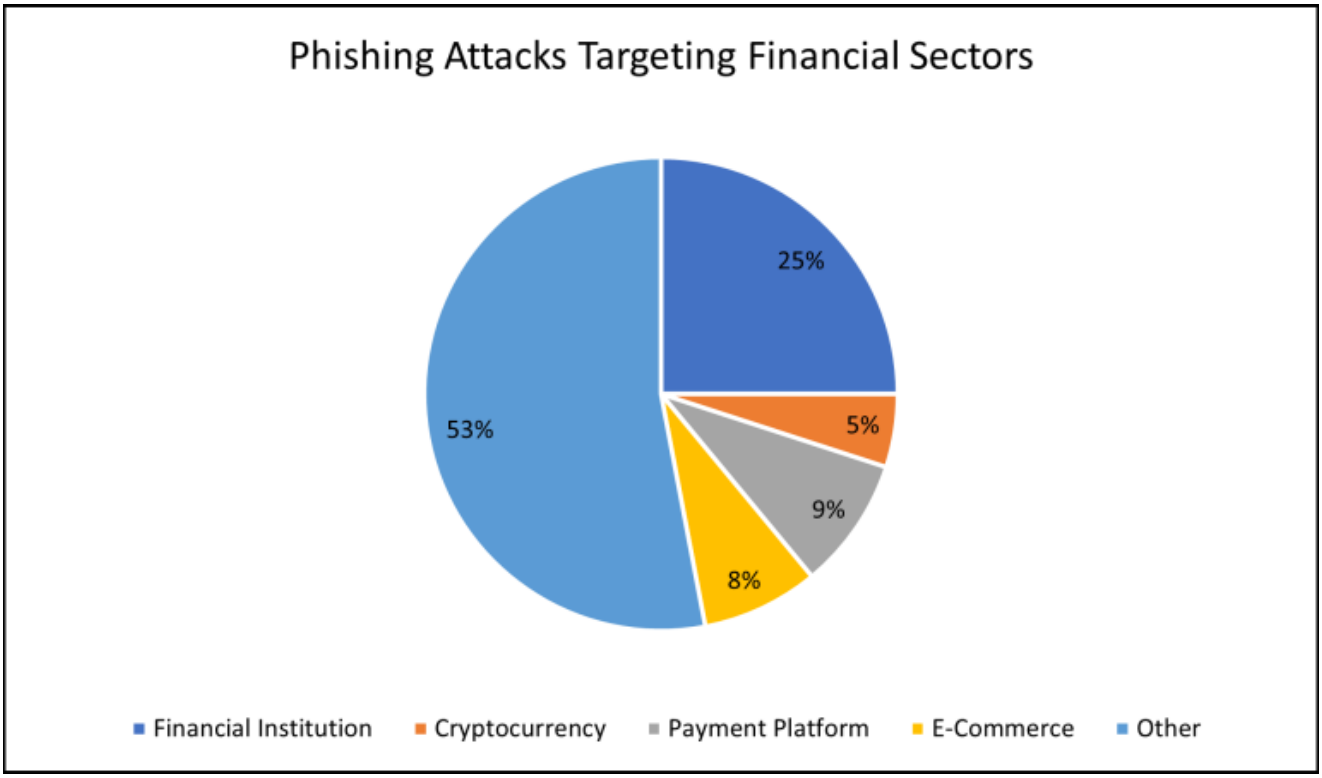

Figure 1 Phishing Attacks targeting Financial Sectors

The phishing webpage can be seen in comparison to a major financial portal in Figure 2.

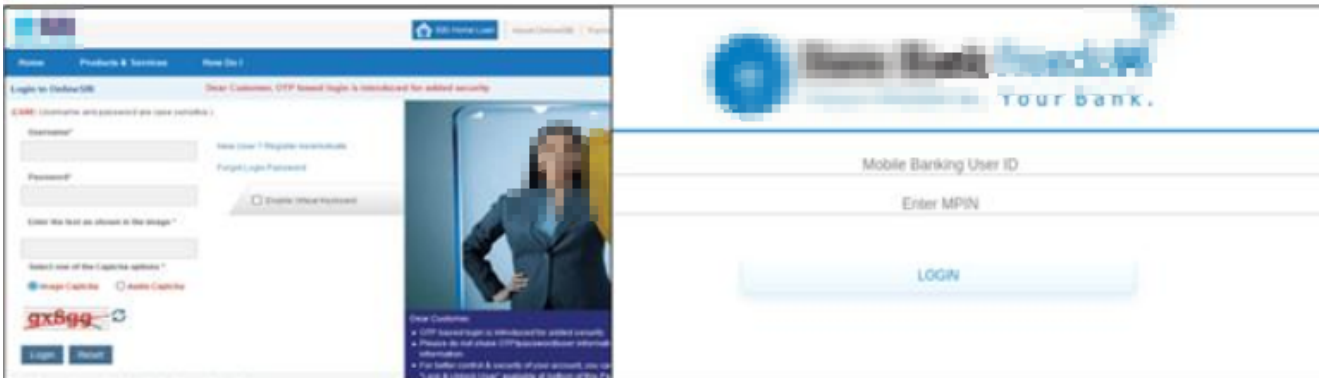

Figure 2 Comparison of a legitimate and a phishing page for a well-known bank

Note: To know more about our research on phishing and its types that are targeting various industries, please refer to our previous blogs:

- Trends In Phishing Attacks and The Industries Commonly Targeted
- Phishing Attack Trends Captured by Cyble Honeypots

Banking Malware:

Spyware is another commonly used tool to target financial sectors and steal credentials, identity, and sensitive data. Stealer and Bots are spyware variants that the attackers commonly use to target financial firms, and they are generically called Banking Malware. Banking malware targets personal computers (PCs) and mobile devices, which steals the credentials used to conduct online payments and transactions.

Some of the functionalities that banking malware can perform upon successful installation on the device are:

- Stealing usernames and passwords from online banking services
- Collecting data such as the user's banking information (cardholder name, card number, CVV, and expiration date)
- Gathering call logs and contacts
- Reading SMS content from the device and storing the data within the device
- Reading SMS notifications, such as financial transactions, received from the user's device.
- Collecting the machine's information
- Having a keylogger functionality

These variants of banking malware, which are also known as Banking Trojan or BankBot, frequently targeting financial firms are listed below:

- Cerberus
- Aberebot
- SpyEye
- TrickBot
- DanaBot

- Anubis

According to a recent report by Heimdal and Securelist – Zbot malware, commonly known as Zeus, is the most notorious trojan among the banking malware families, accounting for 25% of all attacks. SpyEye accounts for a further 15%, with TrickBot & DanaBot each accounting for 5% of all infections.

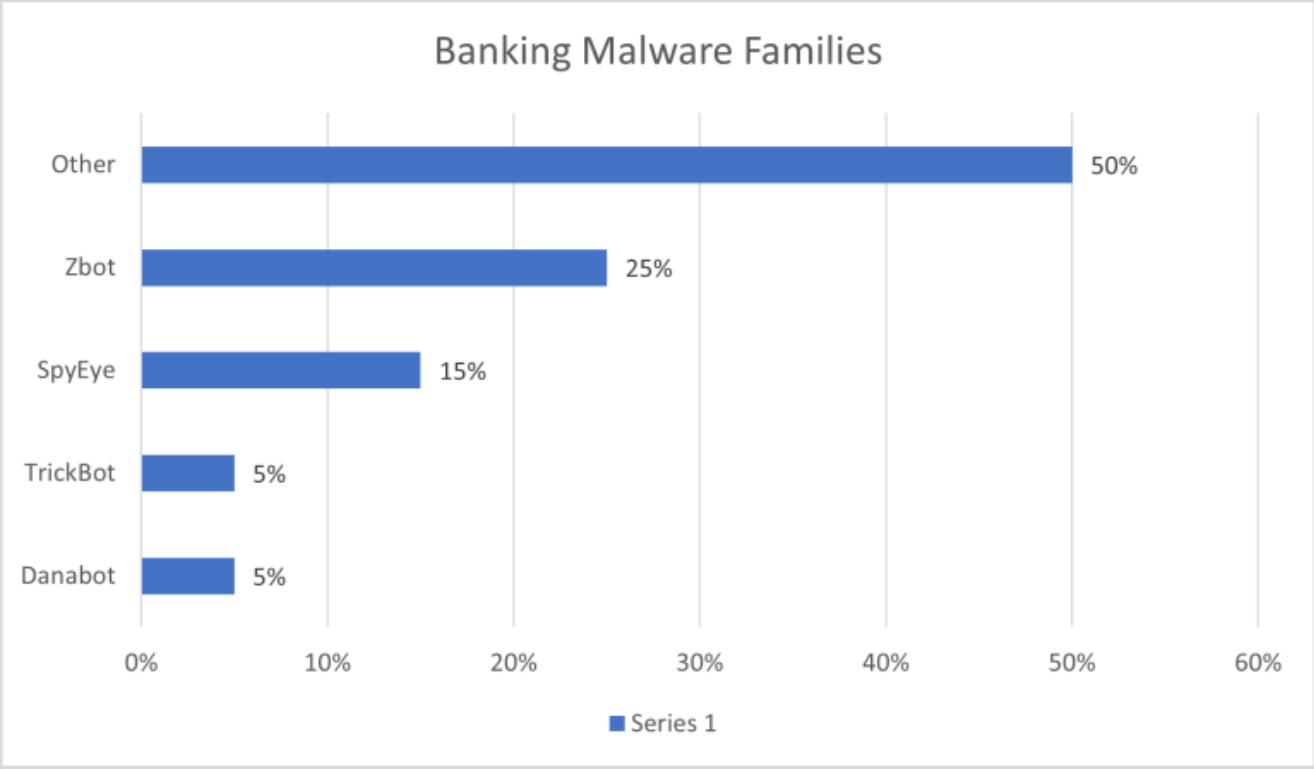

Figure 3 Banking Malware Families Targeting Financial Firms

Several cybercrime forums provide various services to cybercriminals that allow them to purchase the malware. Additionally, forum users also offer services to make the malware Fully Undetectable (FUD). Upon using the services from these cybercrime forums, the malware becomes undetectable by common scanning mechanisms such as antivirus programs. The figure below showcases one of the cybercrime forum posts about APK crypt/FUD service.

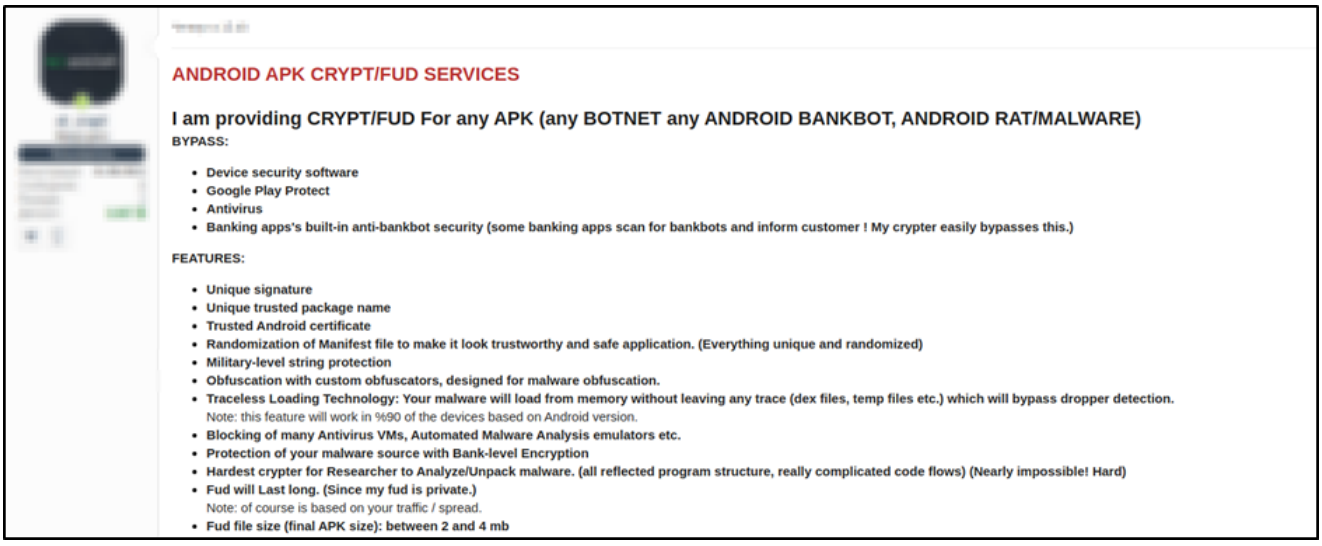

Figure 4 Crypt/FUD Sold through Cybercrime Forum to avoid BOTNET detection

Cybercriminals also sell the sensitive details they have extracted from various institutions and third-party services. These details include sensitive PII data and credit card numbers. In the below figure, a user is selling active credit card numbers on a cybercrime forum.

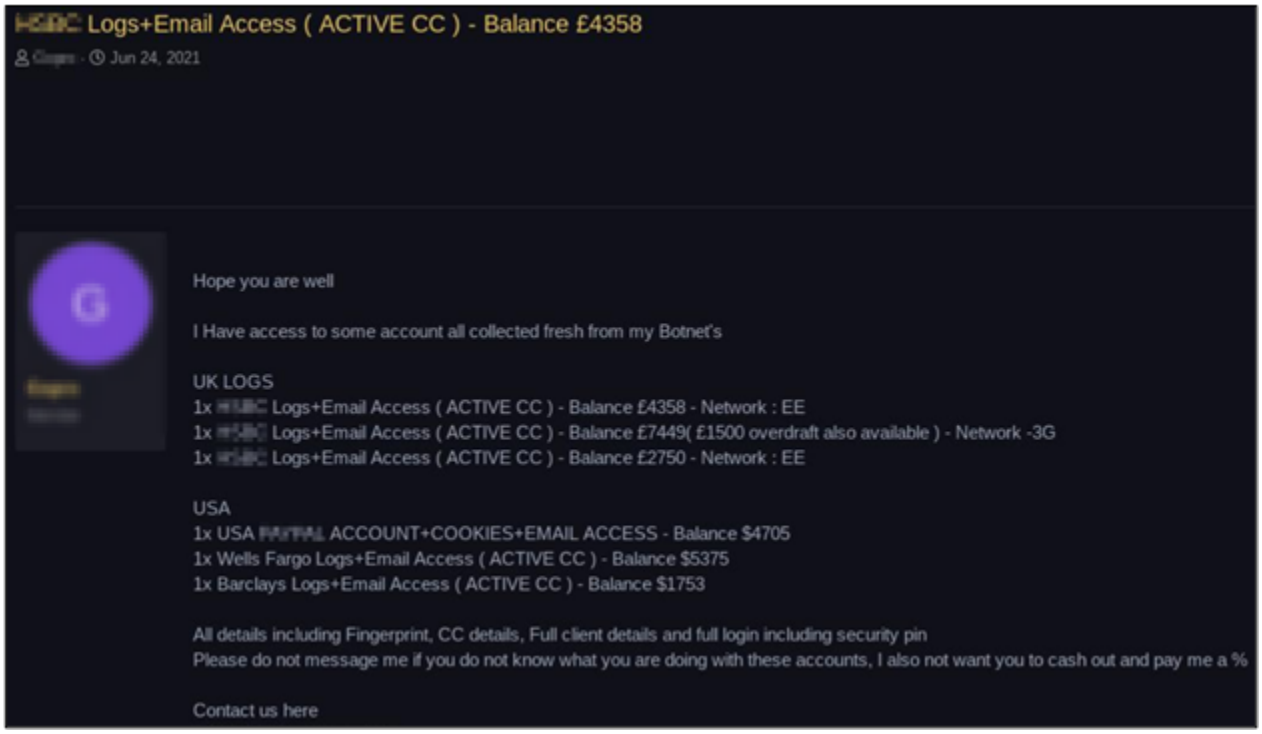

Figure 5 Collected Sensitive Information Sold through Cybercrime Forum

Note: Below, we have listed blogs covered by Cyble Research Labs related to banking malware that use Stealer/Bot to target financial firms.

ZLoader Returns Through Spelevo Exploit Kit & Phishing Campaign

Aberebot On the Rise: New Banking Trojan Targeting Users Through Phishing

DanaBot Banking Trojan Regains Its Foothold In The Threat Landscape

Mobile Malware App Anubis Strikes Again, Continues To Lure Users Disguised As A Fake Antivirus

Banking Trojan Variant Spreading Through Android App

Third-Party attacks:

Most financial institutions depend on third parties, vendors, or partners services like software services, analytics, web hosting, etc. Leveraging third parties for non-critical tasks allows financial firms to prioritize their primary business objectives.

The use of third-party services carries many perks; however, there are also some security risks associated with them. This quarter, we have seen how ransomware attacks on Kaseya impacted several businesses, and similar attacks can lead to attacks increasing the Maximum Tolerable Downtime (MTD).

Data breaches on service providers can impact their clients, as we recently observed in one of the Blackmatter ransomware attacks. This attack disrupted the victim's services and revealed sensitive information belonging to their clients.

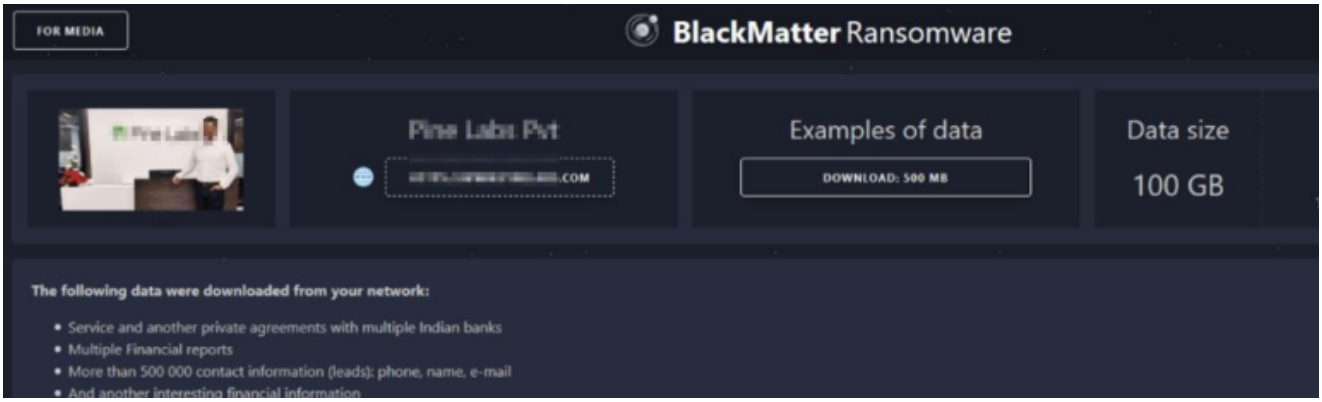

Figure 6 BlackMatter Ransomware Targeting Financial Service Provider

Note: A threat report covered by Cyble Research Labs related to third-party attacks that use ransomware to target various sectors is linked here:

Ransomware Threat Report Q2-2021

Trends:

A surge in ransomware attacks was observed in the year 2021 as a part of our research. Ransomware attacks typically encrypt the data on the targeted device. Before the encryption stage, however, these groups extract the sensitive data. The attacker then demands a ransom based on this sensitive data. If the victim is unable to pay the ransom, they extort the victim by leaking the collected sensitive data on public forums.

As a part of our research, the trend of the ransomware attacks and data leaks that affect financial sectors indicates that the LockBit ransomware group is the most active. LockBit has the most significant number of victims compared to other ransomware groups.

Figure 7 depicts the industries targeted by the LockBit ransomware group, with manufacturing accounting for 27.2% and financial services accounting for about 13.6%.

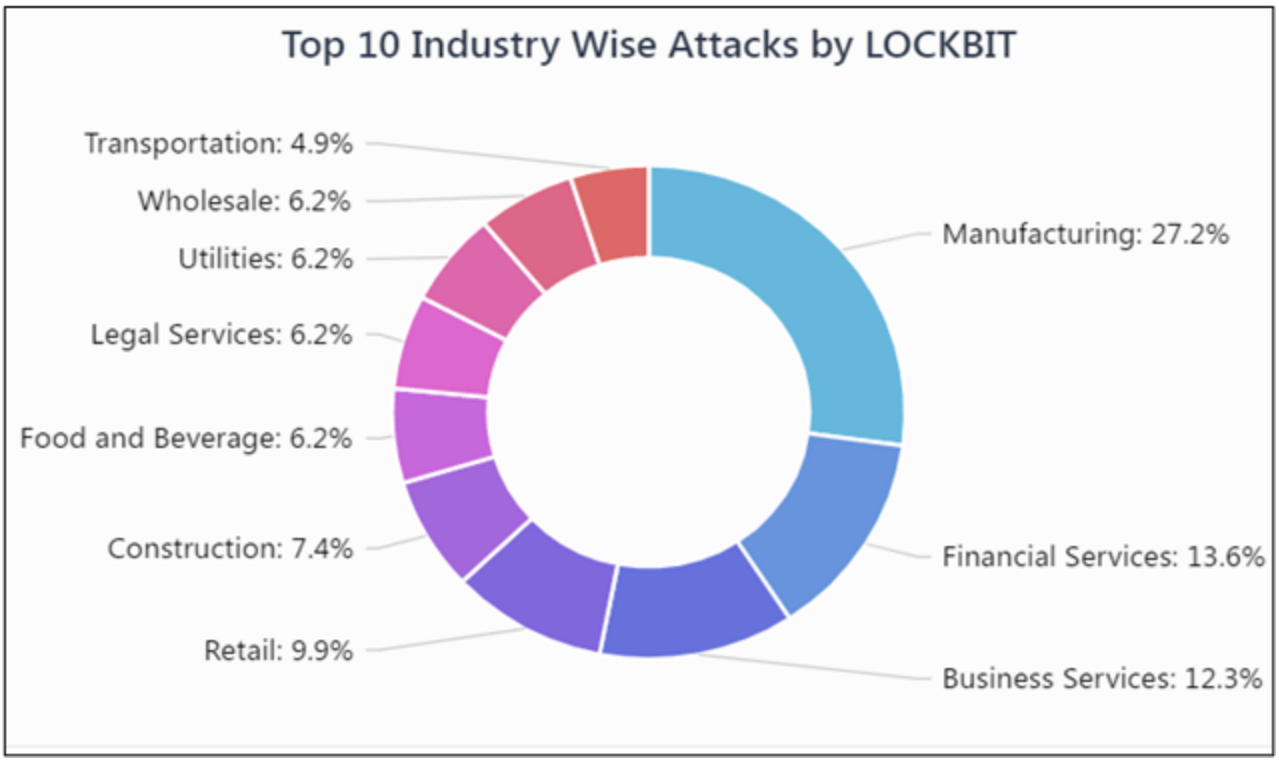

Figure 7 LockBit attacks by industry

Figure 8 depicts a statistical trend of ransomware organizations that target financial firms. LockBit tops the list based on the number of victims and recent attacks.

The trend also indicates that the second most active ransomware gang targeting financial firms is Sodinokibi (REvil), with eight victims. The third most active group is Avaddon, which has six victims.

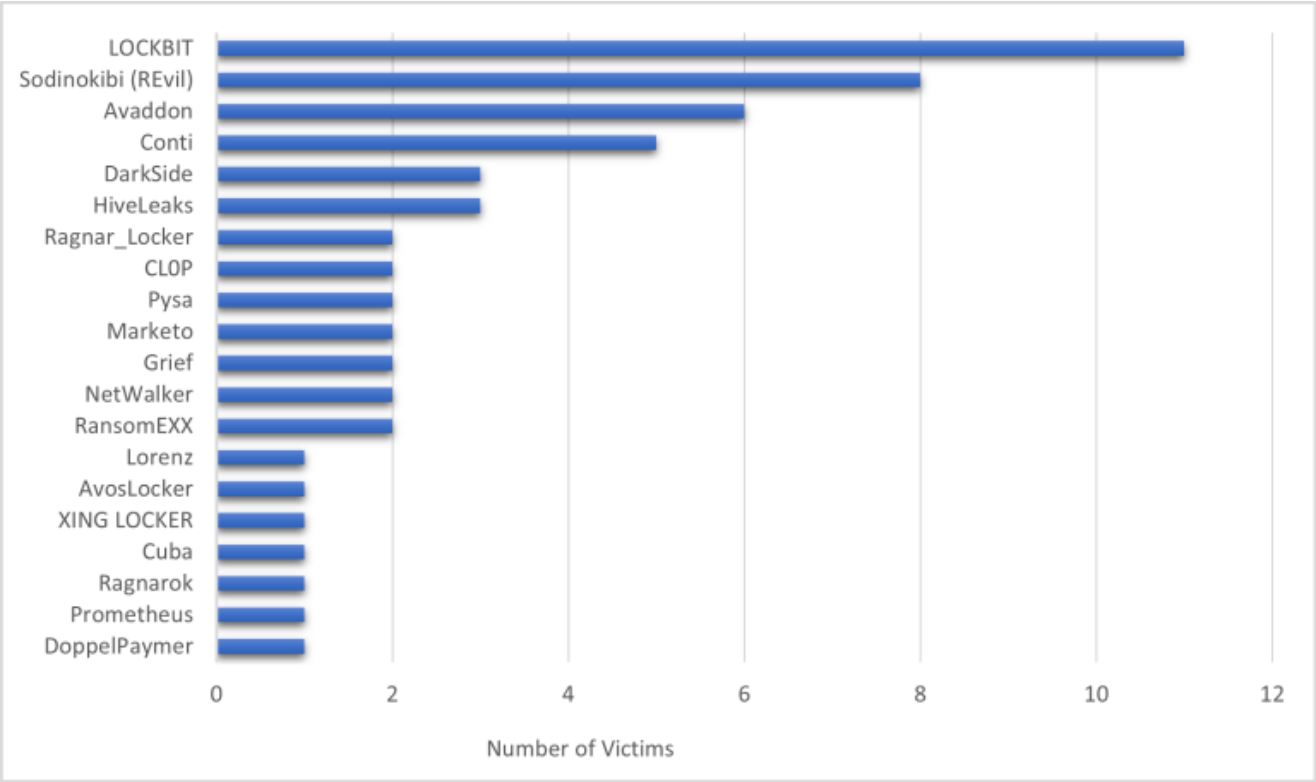

Figure 8 Number of Victims from the Financial Firms Targeted by Ransomware Groups

Figure 9 presents a heat map based on ransomware attacks targeting financial services around the world. The cumulative number of assaults targeting financial institutions is 59, with 20 ransomware groups involved.

The United States is the most frequently attacked country, followed by the United Kingdom, Canada, Australia, and France.

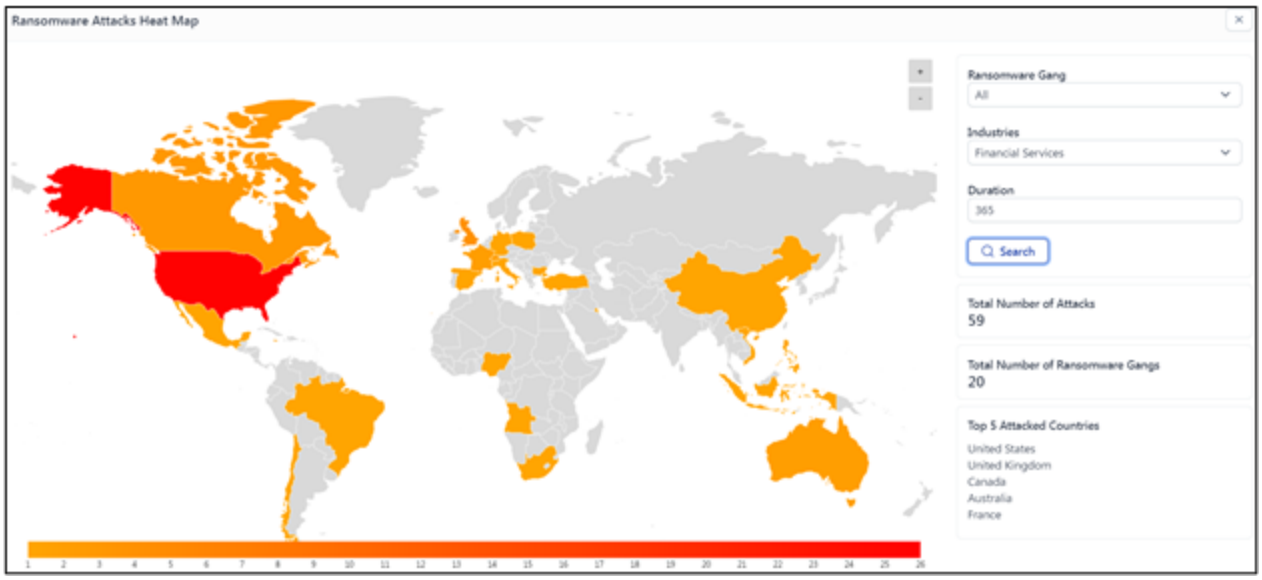

Figure 9 Heat Map on Ransomware Attacks

Conclusion:

Based on these findings, cybercrime, in general, has seen an increase with a focus on attacks targeting financial firms. Attackers use various social engineering tools to spread malware and use multiple techniques to evade detection mechanisms.

Along with enhancing the security methods used by financial organizations, the attackers simultaneously develop malware with customized techniques, such as automatically performing the malicious activity instead of relying on the manual commands pushed from the attacker's Command-and-Control Server.

Implementing a better endpoint security and threat intelligence platform by the organization could prevent them from becoming victims of malware targeting the financial sector.

Recommendations:

1. Impose strict identity and access management policies.
2. Keep track of vulnerabilities being targeted by attackers.
3. Identify the Tactics, Techniques, and Procedures (TTP) of the TAs.
4. Monitor TA activities on the web.
5. Use a reputed antivirus and Internet security software package on your connected devices, including PC, laptop, and mobile.
6. Refrain from opening untrusted links and email attachments without verifying their authenticity
7. Conduct regular backup practices and keep those backups offline or in a separate network.

About Us

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the Darkweb. Its prime focus is to provide organizations with real-time visibility to their digital risk footprint. Backed by Y Combinator as part of the 2021 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Start-ups To Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, and India, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com.