2024 SECTORAL REPORT

Attacks on the Financial Sector in the First Half of the Year

@echocti @echocti echocti.com

Contents

Executive Summary

This report provides a comprehensive review of cyber attacks on the financial sector in 2024. The increasing digitalisation of the financial sector and the growing sophistication of cyber threats make it imperative for financial institutions to review their cyber security measures.

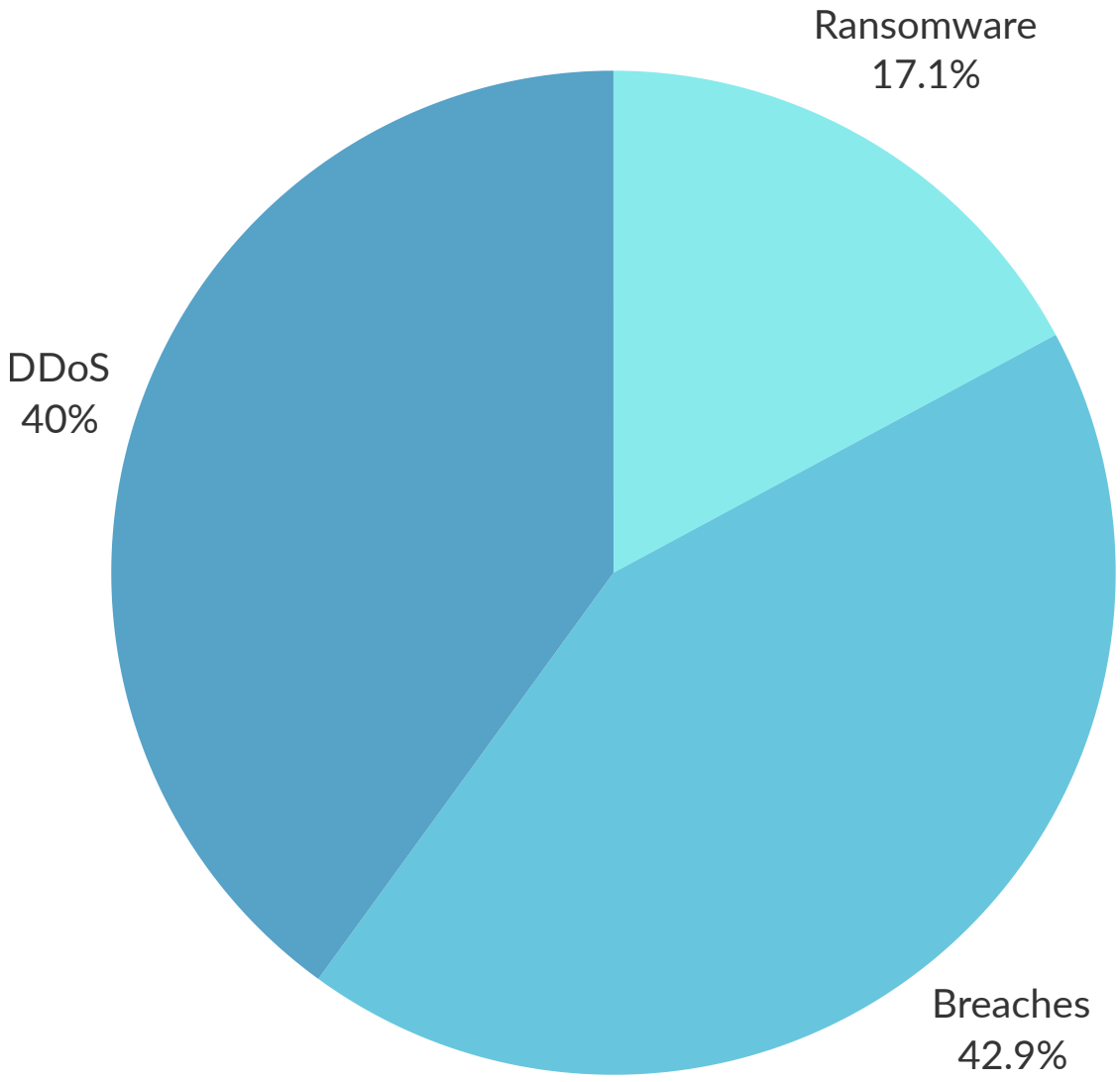
The report is an important resource for understanding these threats and the industry's strategies to stay safe. The report focuses on the types of cyber attacks seen in the financial sector in 2024 and the frequency of these attacks. It also discusses the identities and motivations of the actors behind cyberattacks. Prominent cyber attack incidents are analysed and their potential impact on the sector is evaluated.

Recommendations are provided for financial sector leaders to strengthen their cyber security measures and be prepared for future threats. Establishing emergency response plans and adopting cyber security best practices can increase the resilience of the financial sector against cyber attacks. Taking a proactive approach to future threats can help financial organisations protect their data and reputation.

This report is designed to guide financial sector leaders to strengthen their cybersecurity strategies and prepare for future cyber threats. The financial sector must increase seriousness about cybersecurity and ensure an effective defence against cyberattacks.

Cyber Threats in The Financial Sector

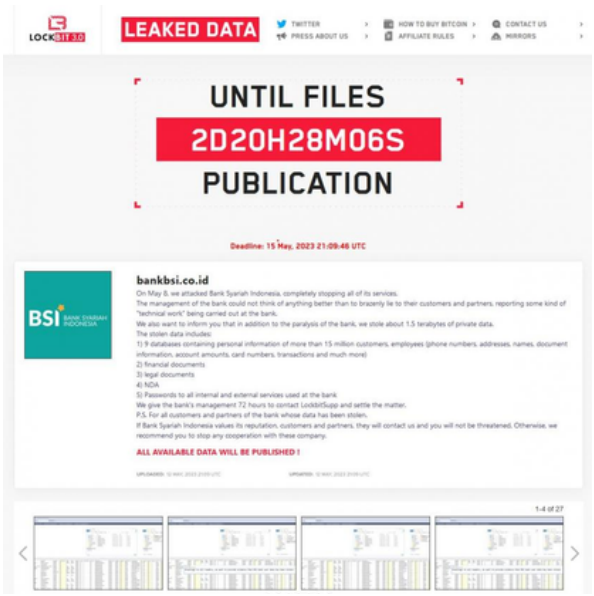
In the first half of 2024, the types of cyber attacks targeting the financial sector were analysed. The chart shows how cyber attack types contribute to attack trends in the financial sector.



Ransomware Attacks

LockBit Ransomware Claims to Have Leaked 1.5TB of Data from Bank Syariah Indonesia

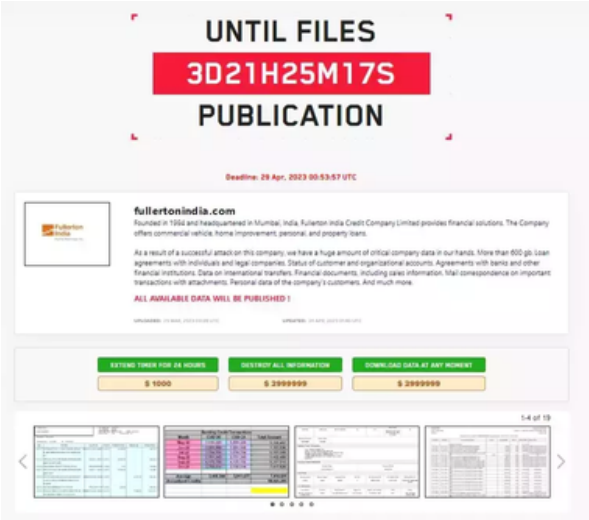
In May 2023, the LockBit ransomware group leaked 1.5 terabytes of personal and financial data from Bank Syariah Indonesia (BSI) after ransom negotiations failed.



The compromised data includes information on approximately 15 million customers and employees of Indonesia's largest Islamic bank. Although BSI initially attributed the service interruptions to IT maintenance, LockBit claimed responsibility for the cyberattack. Negotiation screenshots reveal that despite the bank's $10 million offer, LockBit initially demanded $20 million before stopping communications.

LockBit Ransomware Exposed 600 GB Fullerton India Data

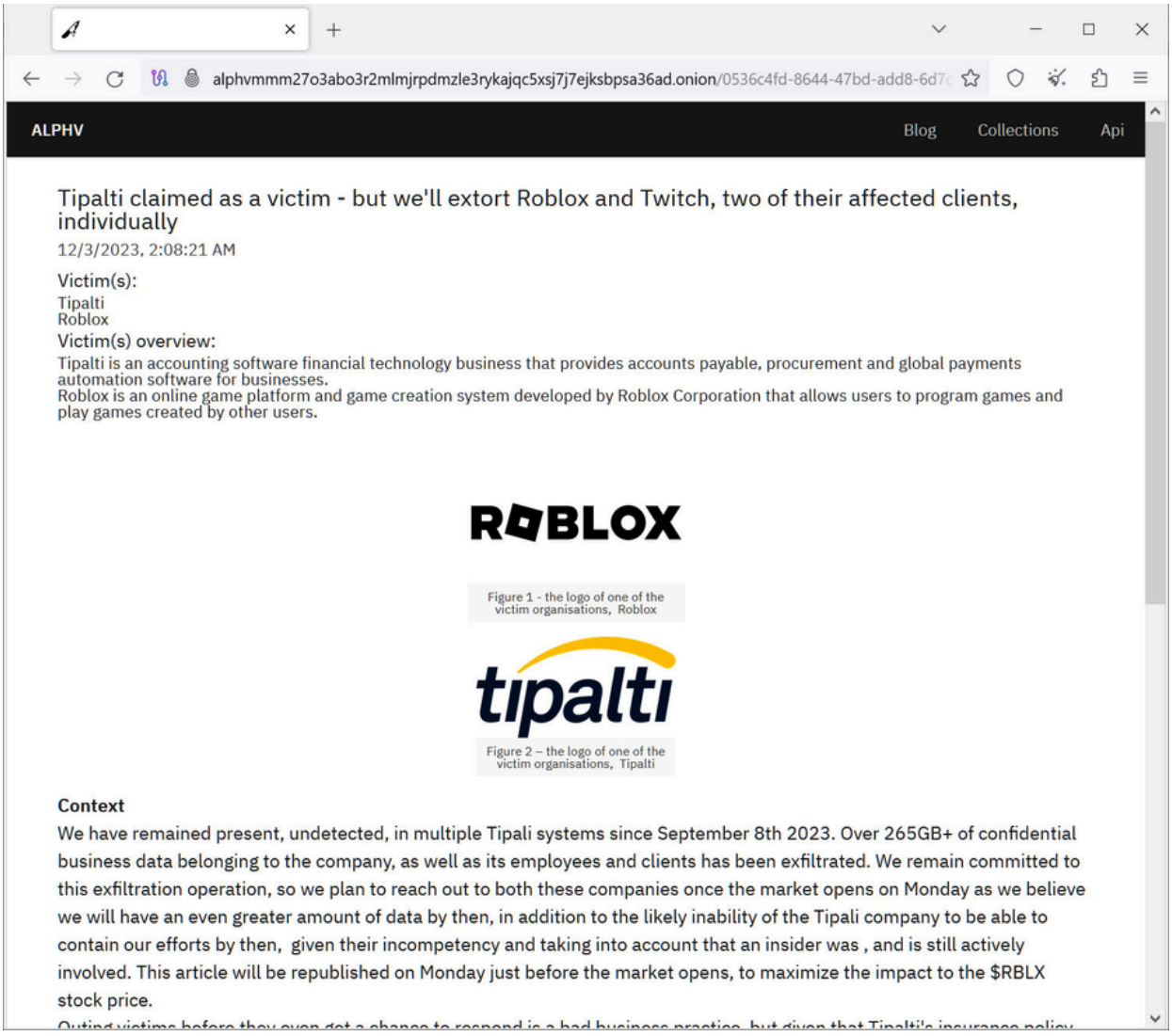
In May 2023, LockBit 3.0 claimed to have leaked 600 GB of data from Fullerton India after demanding a $3 million ransom.



Following the malware attack, Fullerton India briefly suspended operations, but enhanced cybersecurity measures enabled them to resume services. The ransomware group listed the bank on data leak sites, claiming to have stolen loan agreements. Fullerton India's refusal to pay led to triple extortion tactics. In a triple extortion attack, cybercriminals demand payment not only from the first target, but also from anyone affected by the exposure of the target's data.

Typical ALPHVM Attack

In December 2023, the ALPHV/BlackCat ransomware group, known for its sophisticated cyberattacks, targeted Tipalti, a leading FinTech company.



This alleged breach compromised Tipalti and threatened its high-profile customers, including Roblox, Twitch, and X.

ALPHV/BlackCat claimed to have accessed Tipalti's systems on 8 September 2023 and stole over 265 GB of sensitive data. The attack posed significant risks, especially for Roblox and Twitch, whose confidential information could be leaked or used for extortion.

Data Breaches

Latitude Financial Experienced Data Breach of 14 Million Records

In March 2023, Latitude Financial, an Australian financial services company, suffered a data breach in which hackers stole 14 million customer records. These records contained sensitive personal and financial information, including names, addresses, dates of birth, credit card details, driving licence numbers, passport numbers and financial statements.

TMX Experienced Data Breach Affecting 4.8 Million Customers

TMX Finance and its subsidiaries TitleMax, TitleBucks and InstaLoan experienced a data breach affecting 4,822,580 customers. However, this breach was discovered on 13 February 2023.

An investigation revealed that hackers stole sensitive customer data between 3-14 February 2023, including full names, dates of birth, passport numbers, driver's licence numbers, federal and state identification card numbers, tax identification numbers, Social Security numbers, financial account information, phone numbers, physical addresses and email addresses.

Mr Cooper Subjected to Cyber Attack Leaking Data of 15 Million People

In October 2023, Mr Cooper, the largest non-bank mortgage servicer in the US, suffered a cyberattack that exposed the personal information of 14.7 million people.

The breach occurred between 30 October and 1 November and included names, addresses, telephone numbers, Social Security numbers, dates of birth and bank account numbers. The incident also caused a technical outage in November that affected customer payments.

American Express Account Information Disclosed

In March 2024, American Express Co. informed Massachusetts regulators that a breach at an external company may have compromised cardholders' account information. While AmEx did not disclose the name of the hacked company or the number of potential affected individuals, in a letter it urged its customers to monitor their accounts for any suspicious activity.

LoanDepot Hit by Ransomware Attack Compromising Personal Data of 16.6 Million Customers

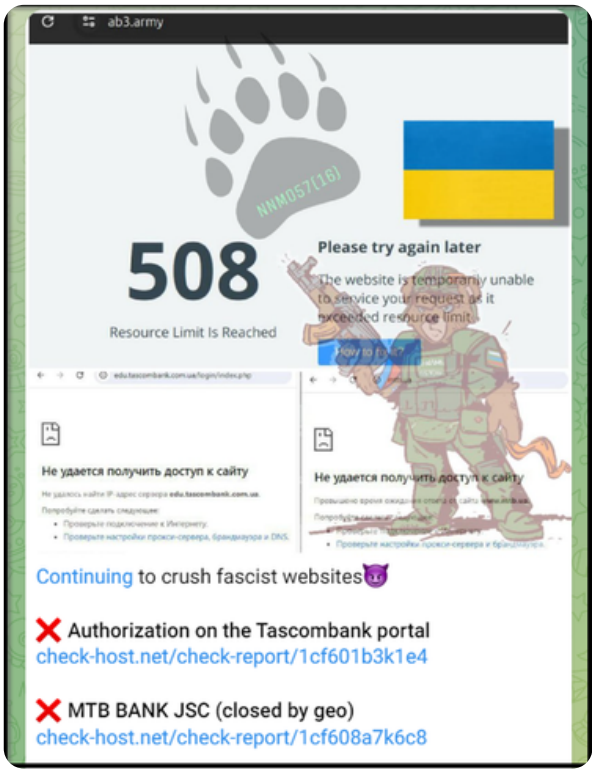
In January 2024, US-based mortgage and lending giant LoanDepot announced that it had been hit by a ransomware attack.

The company announced that they took some of their systems offline in response to the attack. LoanDepot announced that sensitive information belonging to 16.6 million customers was compromised. The stolen data included names, dates of birth, email and postal addresses, financial account numbers and phone numbers. LoanDepot also confirmed that Social Security Numbers were also stolen during the ransomware attack.

DDoS Attacks

NoName057(16) Claimed to Target Ukraine's Financial Sector

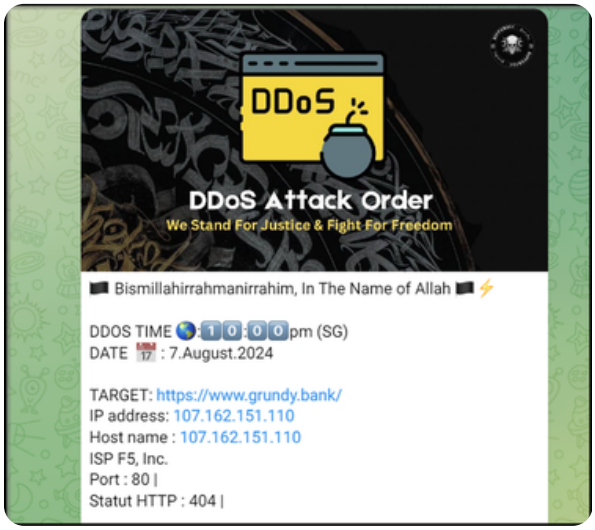
The relevant attack post was made by the hacktivist group NoName057(16) on the Telegram channel.



Russia-linked threat actor NoName057(16), who claimed to have attacked UKRSIBBANK and Accordbank yesterday due to the clashes between Russian and Ukrainian military forces in the Kursk Region, claimed to have attacked Tascombank and MTB BANK JSC today.

RipperSec Thedit Actor Claims to Target US Financial Sector

The relevant attack post was made by the hacktivist group RipperSec on the Telegram channel.



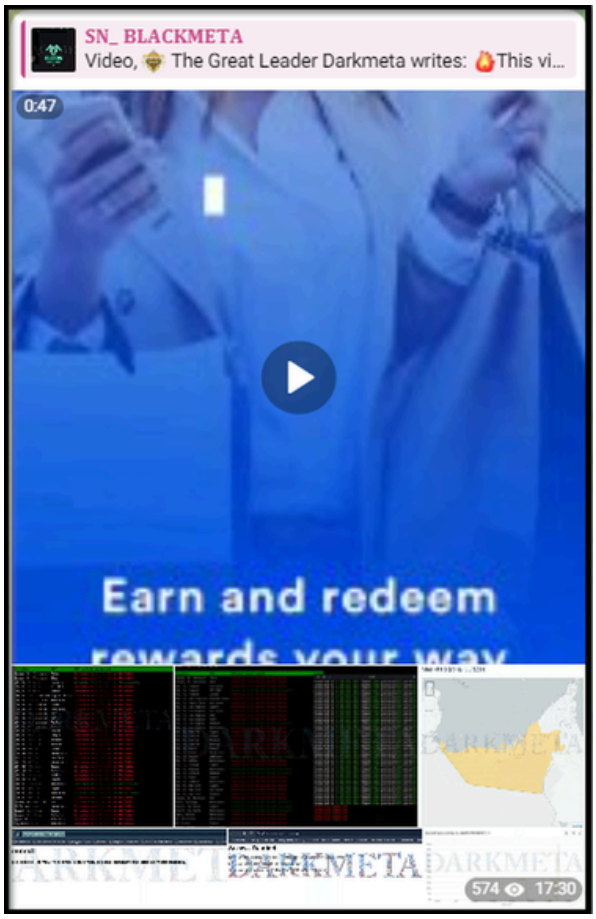
The threat actor claimed that it targeted Grundy Bank, one of the public banks in the state of Illinois in the United States and the 4th oldest bank in the state. As an attack method, he stated that they used Distributed Denial-of-Service (DDoS) attack, which is a common technique.

Threat Actor RipperSec Claims to Target Indian Financial Sector

The relevant attack post was made by the hacktivist group called RipperSec on the Telegram channel.

The threat actor named RipperSec, which has recently announced its cooperation with Russia-linked hacktivist groups, claimed to have organised a cyber attack on Bank of Baroda, one of India's leading financial institutions. He stated that he carried out a Distributed Denial-of-Service (DDoS) attack as a method.
Founded in 1908, Bank of Baroda is one of India's leading public banks with branch and office networks covering Europe, USA, Africa, Asia and Australia.

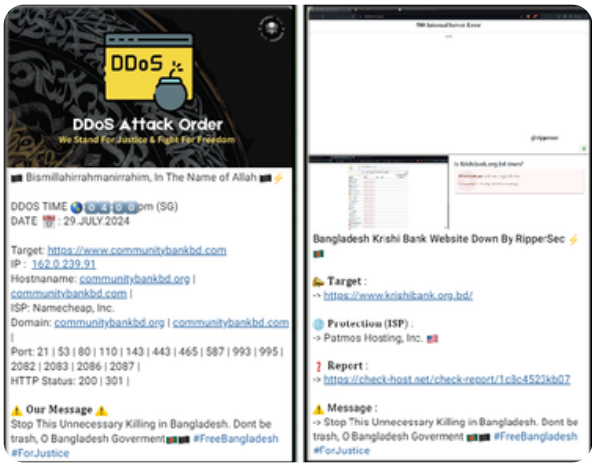
Russian Hacktivist Group Claims to Target UAE Financial Sector



Russia-linked hacktivist group SN_BLACKMETA claimed to have targeted First Abu Dhabi Bank, headquartered in the United Arab Emirates. The attack method was a Distributed Denial-of-Service (DDoS) attack. The attack was shared on a Telegram channel called "SN_BLACKMETA". In the related post, attacks on NATO and some organizations were also mentioned.

RipperSec Group Claims to Target Bangladesh's Financial Sector

The threat actor, RipperSec, claimed to be targeting Bangladesh's major financial institutions and shared the attack on its secret telegram channel.



In the related post, it was claimed that the websites of Krishi Bank, one of the banks with the largest service network in Bangladesh, and Community Bank, an organization of a foundation in the country, were targeted. As an attack method, it was stated that they used Distributed Denial-of-Service (DDoS) attack, a common technique.

Threat Actor NoName057(16) Claimed to Target Finnish Financial Institutions

The attack was posted by the hacktivist group "NoName057(16)" on a secret Telegram channel. The Russian-linked threat actor "NoName057(16)" claims to have targeted the "Finnish Chamber of Commerce and Industry" and "OP Financial Group". It says these attacks were in response to the military base agreement with the United States. It also claims to have targeted the "French Ministry of Economy, Finance, Industry and Digital Sovereignty" in the same attack. It says it used a Distributed Denial-of-Service (DDoS) attack, a common technique.

On July 1, the Finnish Parliament unanimously approved a military cooperation agreement with the United States. Under this document, Finland will open 15 military facilities for use by the U.S. armed forces. The US will be able to station its troops and equipment on Finnish territory. The agreement also strengthens cooperation between the countries in crisis situations.

We decided to "congratulate" the corrupt russophobic authorities of Finland on this event and in honor of it prepared DDoS gifts to local websites😈

❌ Finnish Chamber of Commerce and Industry (closed by geo)
check-host.net/check-report/1b909bbck479

❌OP Financial Group the largest financial group in Finland (dead on ping)
check-host.net/check-report/1b909dbfkdc7

❌ French Ministry of Economy, Finance, Industry and Digital Sovereignty's open data site (dead on ping)
check-host.net/check-report/1b90a9f1kc71

It's been a while since we've visited Croatia and we decided to "remind" ourselves😈

❌Ministry of Finance (dead on ping)
check-host.net/check-report/1b2fe713kf86

❌Tax Administration (dead on ping)
check-host.net/check-report/1b2fec0akec9

❌ Authorization on the Croatian National Bank portal (dead on ping)
check-host.net/check-report/1b2ff158kb35

❌Authorization on Croatian People's Bank portal (dead on ping)
check-host.net/check-report/1b2ffaadk9b1

❌Authorization on Croatian People's Bank portal (dead on ping)
check-host.net/check-report/1b2ffdb6k1f8

❌Authorization on the Economic Bank of Zagreb portal (dead on ping)
check-host.net/check-report/1b300083k86f

❌Zagreb Stock Exchange (dead on ping)
check-host.net/check-report/1b30050fkdf3

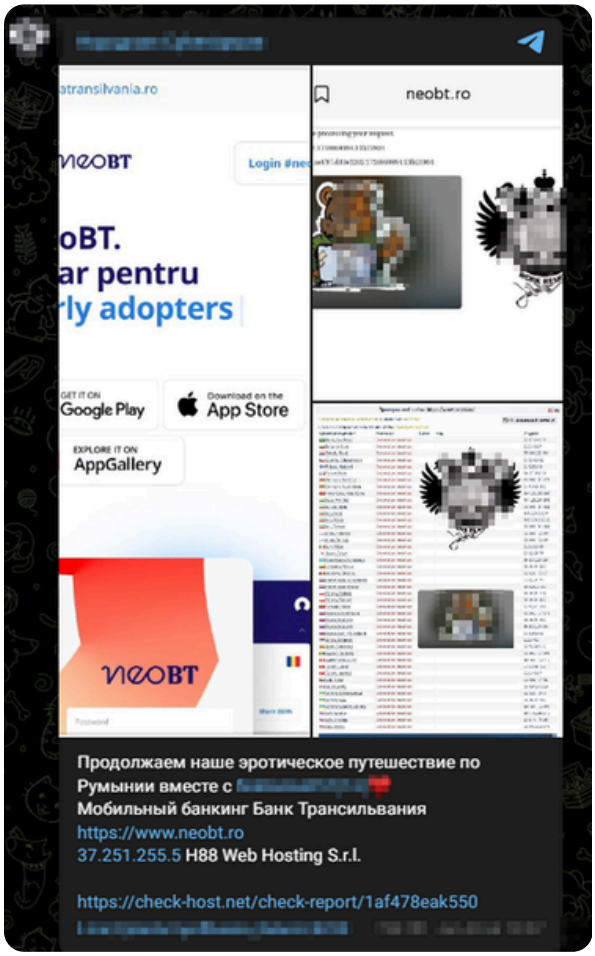
Russian Threat Actor NoName057(16) Claims to Target Croatia's Financial Sector

The attack was shared by the hacktivist group "NoName057(16)" on a secret Telegram channel.

The Russian threat actor "NoName057(16)" claims to have targeted important institutions and organizations in the Croatian financial sector. These institutions and organizations allegedly include "Ministry of Finance", "Tax Administration", "Croatian National Bank", "Zagreb Stock Exchange" and "Economic Bank of Zagreb". The threat actor states that the method of attack is a Distributed Denial-of-Service (DDoS) attack, which is a very common technique among threat actors.

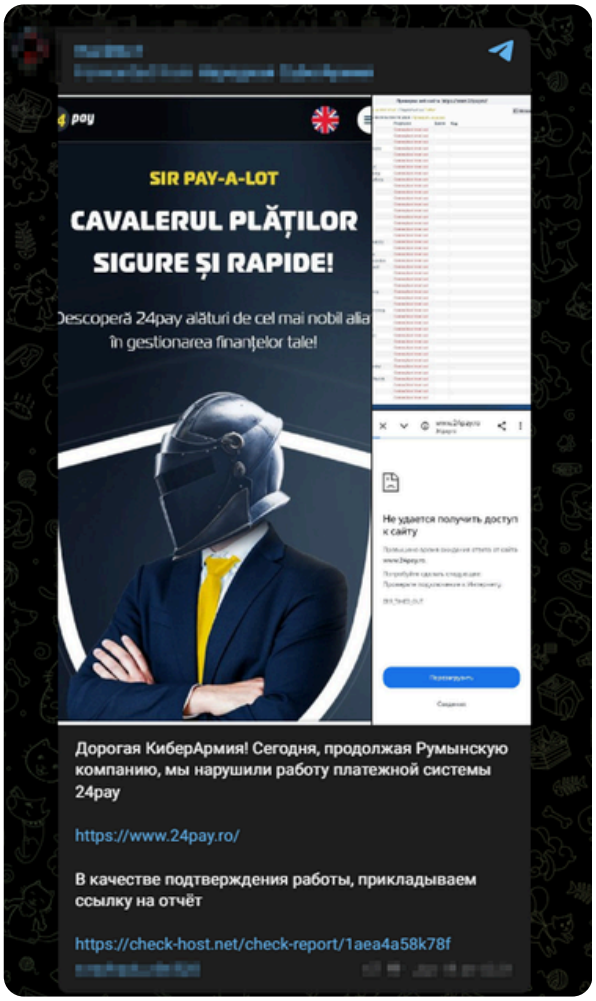
Russian Threat Actor Народная CyberАрмия Claims to Target Romania's Financial Sector

The attack was shared by the hacktivist group "Народная CyberАрмия" in secret Telegram channels. The Russian threat actor, in partnership with "Народная CyberАрмия" and "NoName057(16)", claims to be targeting "NeoBT", the next generation smart digital internet and mobile banking system of Banca Transilvania, which serves the Romanian banking sector. The threat actor states that they used Distributed Denial-of-Service (DDoS) attack, which is a very common technique among threat actors.



Russian Threat Actor HackNeT Claims to Target Romania's Financial Sector

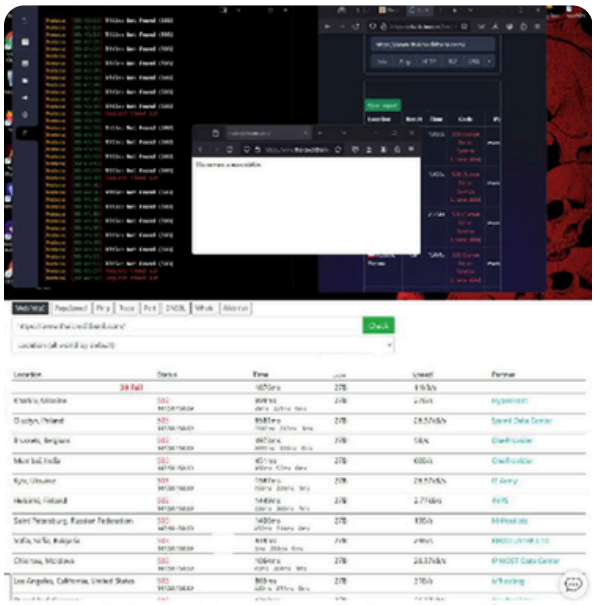
The attack was shared by the hacktivist group "HackNeT" on secret Telegram channels.



Russian threat actor "HackNeT" claims to have targeted "24pay", a Romanian financial services company. The threat actor states that they used a Distributed Denial-of-Service (DDoS) attack, which is a very common technique among threat actors.

Malaysian Threat Actor RipperSec Claims to Target Thailand's Financial Sector

The attack was shared by the hacktivist group "RipperSec" via secret Telegram channels.



Thai Credit Bank Website Down By RipperSec

Target :
-> https://www.thaicreditbank.com

Protection (ISP) :
-> CS Loxinfo Public Company

Report :
-> https://check-host.cc/report/rSaHgQtdC1t3gBc45NusQQ
-> https://check-host.net/check-report/1ab45f9ak816

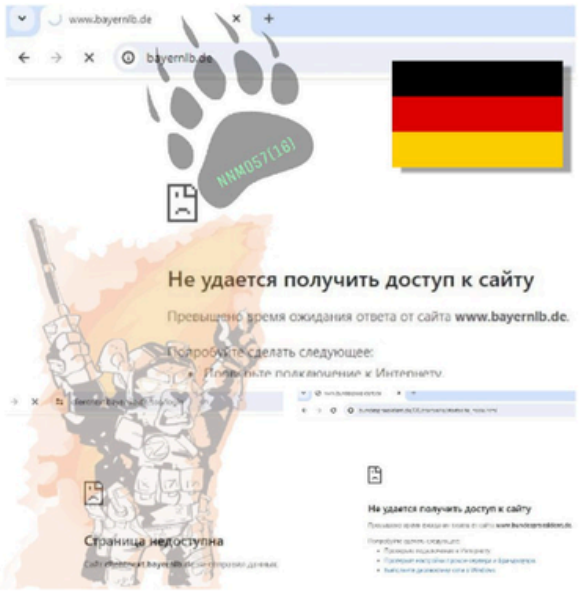
Message :
-> Patani Pasti Akan Merdeka
#FreePatani #OpsPutus #StandWithPatani

Malaysian threat actor "RipperSec" claims to have targeted "Thai Credit Bank Public Company", a banking service in Thailand. The threat actor states that they used a Distributed Denial-of-Service (DDoS) attack, which is a very common technique among threat actors.

Russian Threat Actor NoName057(16) Claims to Target German Financial Sector

Russian threat actor "NoName057(16)" claims to have targeted "Bayerische Landesbank", a commercial banking service in the German financial sector. The threat actor stated that they used a Distributed Denial-of-Service (DDoS) attack, which is a very common technique among threat actors.

The attack was shared by the hacktivist group "NoName057(16)" on their secret Telegram channel.



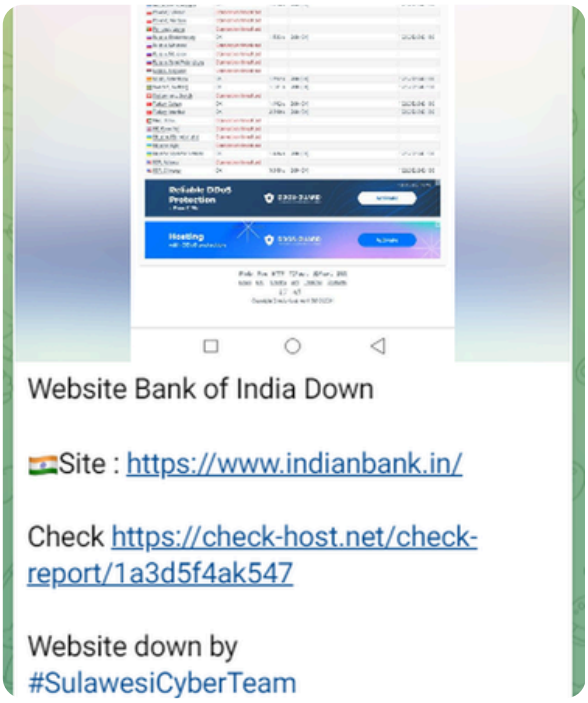
We continue to attack the German internet infrastructure and put down some websites😈

❌BayernLB (fully Bayerische Landesbank) - German commercial bank (dead on ping)
check-host.net/check-report/1aa38330k5e1

❌Lk Bayerische Landesbank (dead on ping)
check-host.net/check-report/1aa38489kf56

Indonesian Threat Actor Sulawesi Cyber Team Claims to Target Indian Financial Sector

The attack was shared by the hacktivist group "Sulawesi Cyber Team" via secret Telegram channels.



Website Bank of India Down

🇮🇳Site : https://www.indianbank.in/

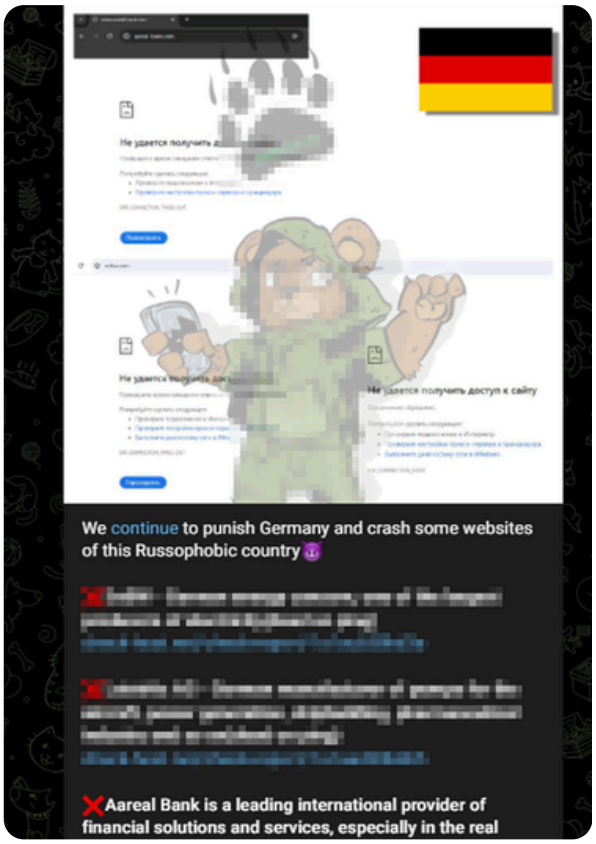
Check https://check-host.net/check-report/1a3d5f4ak547

Website down by #SulawesiCyberTeam

Indonesian threat actor "Sulawesi Cyber Team" claims to have targeted "Indian Bank", the 7th largest public sector bank in the Indian financial sector. The threat actors stated that they used a Distributed Denial-of-Service (DDoS) attack, which is a very common technique.

Russian Threat Actor NoName057(16) Claims to Target Germany's Financial Sector

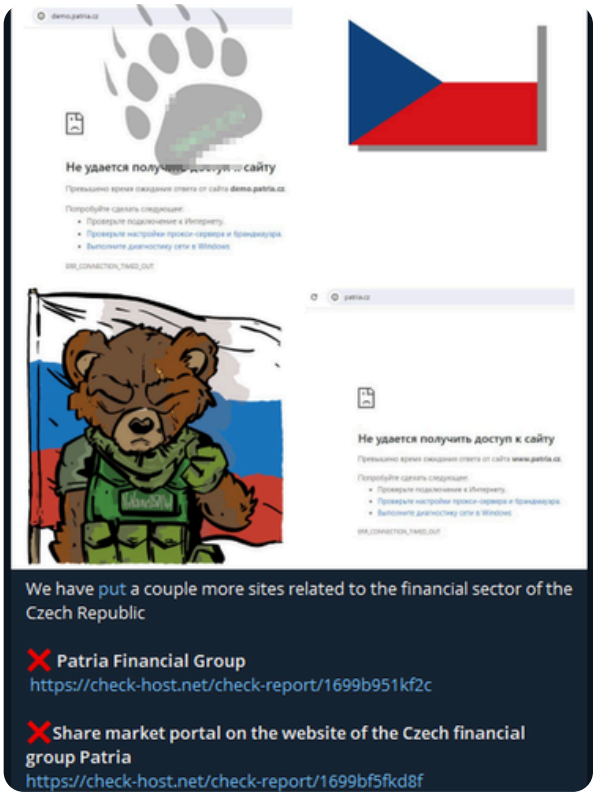
The attack was shared by the hacktivist group "NoName057(16)" on their secret Telegram channel.



Russian threat actor "NoName057(16)" claims to have targeted "Aareal Bank", a German financial services company that provides financing solutions and banking services, especially in the real estate sector. The threat actors stated that they used Distributed Denial-of-Service (DDoS) attack, which is a very common technique among threat actors.

Russian Cyber Threat Group NoName057(16) Claims to Target Czech Republic's Financial Sector

The attack was shared by the hacktivist group NoName057(16) on their secret Telegram channel.



Threat Actors Targeting the Financial Sector in 2024

LockBit Gang

LockBit Gang is a cyber threat actor that emerged in September 2019 with a ransomware-as-a-service (RaaS) model and is notable for its rapid spread capabilities.

Its attacks are based on automated processes that can quickly spread and lock down target systems.

1. Main Features

- **Fast Propagation:** LockBit 3.0, a family of ransomware that can quickly spread and lock down target networks through automated processes.
- **Targeting Various Industries:** LockBit Gang targets various critical infrastructure sectors such as finance, agriculture, education, Finance, government, healthcare, manufacturing and transportation.

2. Goals and Objectives

- **Ransomware Attacks:** Using LockBit ransomware, the data of target organizations is encrypted and ransom is demanded.
- **Double Extortion Method:** The LockBit Gang uses a double extortion method to pressure victims to pay ransom. This method is the use of encrypted data as well as stolen data as a threat.

for IoC see.

FROZEN SPIDER

FROZEN SPIDER, or Medusa ransomware team, is a cybercrime group that organizes ransomware attacks.

The group is known for spreading ransomware that locks computer systems, preventing access to data. The Medusa ransomware team largely targets institutions and organizations and is often known for its ransom demands.

Medusa ransomware is one of the most advanced ransomware families today. This ransomware gang mainly aims to infiltrate organizations with medusa ransomware.

As with any ransomware attack, the medusa group aims to undermine the reputation of the organization and gain financial resources through these attacks.

The Medusa ransomware group usually targets large organizations and institutions. These include corporations, government agencies, healthcare organizations and financial institutions. The group puts the targeted organizations at risk of massive data loss in order for the ransom demands to be taken seriously.

See also for IoC

MASKED SPIDER

MASKED SPIDER, also referred to as the BianLian ransomware group, is an advanced ransomware threat that has recently emerged and is rapidly gaining popularity in the attack scene.

This ransomware targets victims using unique encryption algorithms and sophisticated attack techniques and can cause severe data loss.

BianLian fidye yazılımı, genellikle kötü amaçlı e-posta kampanyaları, güvenlik açıklarından yararlanma ve kötü amaçlı web siteleri aracılığıyla yayılır. Kurbanların bilgisayar sistemlerine sızdıktan sonra, fidye yazılımı dosyaları ve verileri güçlü şifreleme algoritmalarıyla kilitleyerek erişimlerini engeller.

Bu fidye yazılımı grubu, genellikle Bitcoin gibi kripto para birimleriyle ödeme yapılmasını talep eder. Fidye ödendikten sonra, genellikle kurbanlara dosyalarını geri alma ve şifreleri çözme şansı verilir. Ancak, fidyenin ödenmesi bile dosyaların kurtarılmasını garanti etmez ve bazen veri kaybı kalıcı olabilir.

BianLian fidye yazılımı, özellikle büyük kuruluşları ve kurumları hedef alır. Bunlar arasında şirketler, devlet kurumları, sağlık kuruluşları ve finansal kurumlar bulunabilir. Bu tür kurbanların veri kaybı riski büyük olduğu için fidye taleplerine sıklıkla karşı gelinememektedir.

PUNK SPIDER

PUNK SPIDER is associated with the recently emerged next-generation Akira ransomware, which poses a serious cybersecurity threat.

This ransomware uses sophisticated encryption algorithms and effective attack techniques to target victims and demand ransom by locking their files.

Akira ransomware is usually spread via malicious email attachments, exploit kits and malicious websites. After infecting victims' computer systems, Akira encrypts files with strong encryption algorithms to prevent access and promises to unlock them in exchange for a ransom payment.

Akira ransomware specifically targets corporate and commercial organizations. Such victims often have large amounts of sensitive data, which can result in serious financial and reputational losses if the ransom is not paid.

How Can You Avoid Cyber Attacks?

If you want to ensure the security of your organization in the cyber realm, there are some important measures you should take.

Are There Vulnerabilities in the Software We Use?

If there are publicly known vulnerabilities in the software you use within your organization, it is essential to update these applications. If the software you're using hasn't received updates for a long time, you should consider switching to a competitor's product. Otherwise, attackers could exploit these vulnerabilities to access the network within your organization and perform malicious actions on endpoint devices, potentially causing significant damage to your system.

Have Personal Information of Our Employees Been Leaked?

Corporate account information, particularly that of your organization's management, can be leaked due to third-party software vulnerabilities. Attackers may use this leaked information to carry out phishing campaigns, or depending on the type and importance of the leaked information, they may target the individual to harm the organization. To prevent such situations, you can require employees to change their corporate account passwords periodically.

Are Our Employees Sufficiently Aware of Cybersecurity?

Perhaps the most crucial measure to take is raising human awareness. Employees who are less familiar with IT but still connected to the same network are often the primary targets for cyber attackers. To address this issue, it is essential to provide cybersecurity awareness training to these employees. By doing so, you can significantly reduce the risk of successful attacks.

In Summary,

Even if you take every precaution, your organization could still fall victim to a cyberattack. The key is to minimize the potential damage that such an attack could cause.

CYBER THREAT INTELLIGENCE