ECHO

CYBER THREAT INTELLIGENCE

FINANCE INDUSTRY

ATTACK REPORT

2023

@echocti

@echocti

echocti.com

Content

Executive Summary

This report provides a comprehensive review of cyber attacks on the financial sector in 2023. The increasing digitalization of the financial sector and the growing sophistication of cyber threats make it imperative for financial institutions to review their cybersecurity measures. The report is an important resource for understanding these threats and the industry's strategies to stay secure.

The report focuses on the types and frequency of cyberattacks in the financial sector in 2023. It also discusses the identities and motivations of the actors behind cyberattacks. Prominent cyberattack incidents are analyzed and their potential impact on the sector is assessed.

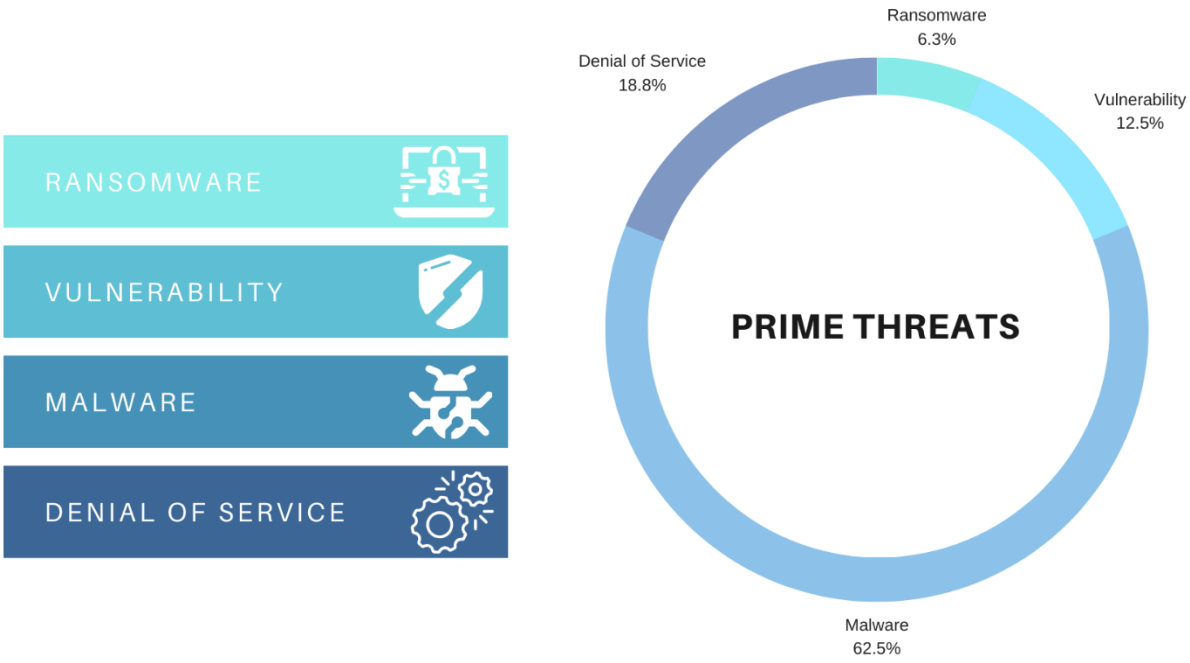
Recommendations are provided for financial sector leaders to strengthen their cybersecurity measures and be prepared for future threats. Establishing emergency response plans and adopting cybersecurity best practices can increase the resilience of the financial sector against cyberattacks. Taking a proactive approach to future threats can help financial institutions 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 get serious about cybersecurity and ensure an effective defense against cyberattacks.

Cyberattacks and Trends

Types of Cyber Attacks Observed in the Financial Sector in 2023

This report examines the types of cyber-attacks targeting the financial sector in 2023 and considers how these attack types are impacting threats to financial institutions. Furthermore, Chart 1 shows how cyber attack types contribute to the rising attack trends in the financial sector.



Grafik 1 Prime Threats

Ransomware

Ransomware is one of the biggest cyberattack threats that the financial sector faced in 2023. This type of attack is characterized by malicious software locking down the target system, blocking access to data, and usually not releasing the data until a ransom is paid. Ransomware attacks pose a great risk to financial institutions and a strong defense against such attacks is required.

Malware

Malware is a common component of cyberattacks targeting the financial sector. Malware has the ability to infiltrate the networks of financial institutions to steal information, monitor or perform malicious operations. Such attacks can lead to the leakage of sensitive financial data or disruption of financial institutions' operations. Typically, customers of financial institutions are targeted. All assets of the customers whose information is compromised are compromised in the organizations they receive services from.

Vulnerability

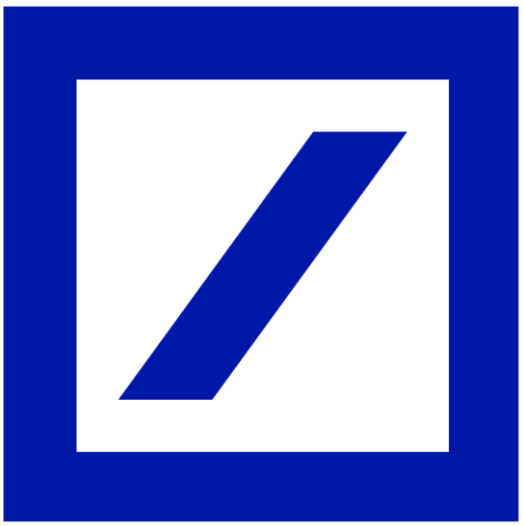
Cyber attackers can carry out cyber attacks by exploiting vulnerabilities in the technologies used by institutions. Such attacks aim to bypass the security systems of financial institutions or gain access to sensitive information.

Denial of Service

Denial of service attacks are a common cyber threat in the financial sector. Such attacks can disrupt the ability of organizations to provide services and even take their services offline. Denial of service attacks can damage organizations' reputation, customer satisfaction and operational continuity.

Cyberattacks in the Financial Sector in 2023

Deutsche Bank Confirms Customer Data Affected in Data Leak



Deutsche Bank has confirmed that a data leak at a service provider has affected customer data. The bank said it was hit by a possible MOVEit Transfer data theft attack and is investigating the incident to strengthen its cybersecurity measures. The incident, which is believed to have affected more than 100 companies across Germany, has been linked to the MOVEit attack wave of the Clop ransomware.

Level Finance Crypto Exchange Hacked Despite Two Security Audits

Level Finance has detected the theft of 214,000 LVL tokens (approximately $1.1 million) by hackers exploiting a vulnerability in its smart contract. The attack did not affect the liquidity pool and the DAO treasury, but it was observed to devalue the LVL token.

Lazarus Group Continues Cyberattacks on South Korean Financial Institution by Exploiting Zero-Day Vulnerabilities

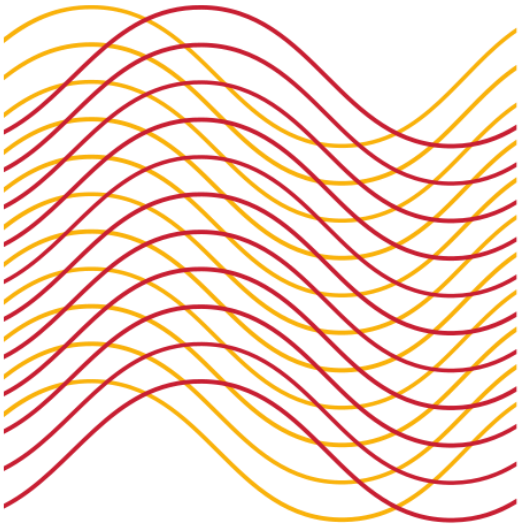
The North Korea-linked Lazarus Group attacked South Korean financial institutions twice in one year by exploiting zero-day vulnerabilities in classified software. In the first attack, the attackers used a vulnerable version of a certification software commonly used by government agencies and universities. A re-infiltration attempt in October 2022 was also found to involve exploiting another zero-day vulnerability in the same program.

Microsoft Warns of North Korean Attacks Exploiting JetBrains TeamCity Vulnerability

Microsoft reports that North Korean threat actors are attacking vulnerable servers using a critical vulnerability in JetBrains TeamCity. The attacks are being carried out by two threat groups that are part of the Lazarus Group, known as Diamond Sleet and Onyx Sleet, and target TeamCity servers using a variety of techniques.

German Financial Institution's Website Hit by DDoS Attack

The German Federal Financial Supervisory Authority (BaFin) announced in a statement that a distributed denial of service (DDoS) attack had impacted its website. BaFin is Germany's financial regulatory authority, responsible for supervising 2,700 banks, 800 financial and 700 insurance service providers. As a result of the attack, BaFin has decided to temporarily shut down its public website "bafin.de", but other important systems are running smoothly.

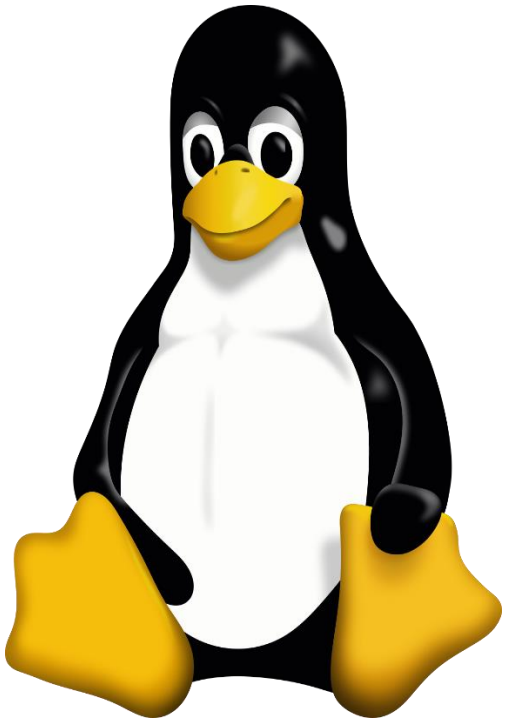


Ukrainian Hackers Disable Service Provider for Russian Banks

Ukrainian hacker group Cyber.Anarchy.Squad claimed responsibility for an attack that disabled Russian telecom provider Infotel JSC. Moscow-based Infotel provides connectivity services between the Russian Central Bank and other Russian banks, online stores and credit institutions. In the aftermath of the attack, several major banks across Russia lost access to their banking systems, making online payments impossible.

China's BlackTech Hacker Group Used Router Devices to Target US and Japanese Companies

Japan and US cybersecurity agencies have warned that BlackTech, a state-sponsored hacker group based in China, is attempting to secretly modify branch office routers to use them as access points to various companies' networks.



AitM Phishing and BEC Attacks Targeting Financial Giants Revealed

Banking and financial services organizations have been the target of a new multi-stage "AitM" phishing and business email conspiracy attack. The attack focused on the use of an indirect proxy that allowed attackers to flexibly tailor phishing pages to their targets and steal session cookies.

Scattered Spider Continues to Threaten with Ransomware Attacks

A dangerous threat group known as Scattered Spider has been found to interfere with normal hiring processes by pretending to be new hires at targeted companies and using a strategy to take over accounts worldwide. This financially motivated hacker group has been described as "one of the most dangerous financial crime groups". The group continues to pose a continuing threat as it has added SMS phishing, SIM swapping and help desk fraud to its operational flexibility and attack model.

FakeCalls Android Malware, New Version Detected

FakeCalls, the Android malware in the spotlight in South Korea, impersonates financial institutions and tries to steal credit card details from bank customers. Vishing, a well-established problem, cost victims in South Korea over $600 million in 2020. New versions of the FakeCalls malware have new techniques to circumvent analysis tools and have the ability to steal audio and video streams from attacked devices.

Xenomorph Android Malware Updated, Continues to Target Banks

The third version of Xenomorph Android malware has been released with an automated transfer system and the ability to steal data from 400 banks. Xenomorph is considered one of the most advanced and dangerous Android malware trojans, capable of performing automatic fund transfers and stealing credentials.

Bluebottle Hackers Using Signed Windows Driver Attack Banks

The hacker group Bluebottle, operating in French-speaking countries, carried out attacks against banks using a signed Windows driver. The signed malicious driver was used to disable security products. It is estimated that these attacks were orchestrated by a threat actor that stole over $11 million in assets from banks. As the Bluebottle group adopted the tactics of the OPERA1ER hacker group, it is thought that these groups may be the same.

An Iranian Cyber Espionage Group Targets Financial and Government Institutions in the Middle East

A group called Scarred Manticore is believed to be linked to Iran's Ministry of Intelligence and Security, which has orchestrated a sophisticated cyber espionage campaign against the financial, government, military and telecommunications sectors in the Middle East. The detected campaign used LIONTAIL, an unknown passive malware framework, and specifically targeted Windows servers. The group uses custom web shells, DLL backdoors and driver-based implants to carry out attacks.

New Financial Threat to Users in Latin America: JanelaRAT

Financial malware targeting users in Latin America, JanelaRAT, has been found to use DLL side loading techniques to compromise sensitive information from LATAM banks and financial institutions. JanelaRAT evades detection through DLL size loading and spreads via ZIP archives obtained from legitimate sources. The malware was also found to be capable of tracking mouse input, recording keystrokes and taking screenshots.

MMRat Android Trojan Revealed Using Accessibility Feature for Financial Fraud

Targeting Southeast Asia, the MMRat Android trojan has been hijacking mobile devices and committing financial fraud since June 2023. The malware uses a proprietary command-and-control protocol to perform large data transfers and targets users in countries such as Indonesia, Vietnam, Singapore and the Philippines. MMRat is spread through official-looking phishing sites and disguised as a government or dating app. The app uses tools such as the Android accessibility service and the MediaProjection API to perform malicious activities on devices.

LOBSHOT Finance Trojan Danger Spread via Google Ads

LOBSHOT is a financial trojan horse developed by a threat actor who publishes malware using Google Ads. The malware has the ability to secretly gain access to computers via the hVNC component, impersonating legitimate tools obtained from fake pages. Previously associated with the Dridex banking trojan, TA505 uses LOBSHOT to expand its malware tools for data theft and financial fraud.

Nexus Android Banking Trojan

Nexus, an emerging Android banking trojan, targets more than 450 financial apps for fraudulent activities. Nexus is designed to perform ATO attacks, with key features including stealing user credentials, intercepting SMS and integrating a ransomware module. Nexus is said to be particularly widespread in Turkey and poses a new threat to financial fraud.

PixPirate New Android Banking Trojan Targeting Brazil

An Android banking trojan called PixPirate has been uncovered that abuses the PIX payment platform by targeting Brazilian financial institutions. Researchers note that PixPirate has the ability to automate the malicious transfer of funds through its Automatic Transfer System (ATS) feature. PixPirate is notable for disabling Google Play Protect, intercepting SMS, and using no-objection ads.

2023 APT Groups Targeting the Finance Sector

As a result of the investigations conducted by our team, it has been determined that some APT groups have targeted the Financial Sector since the beginning of this year. For the informative purpose of this report, information on these APT groups is provided below.

BlackTech

BlackTech is an Advanced Persistent Threat (APT) group known for its covert operations and sophisticated attacks.

Operating mainly in the Asia-Pacific region, the group targets strategic sectors such as governments, technology companies and defense industries, particularly in countries such as Taiwan, Japan and South Korea.

Main Characteristics:

1. Precision Target Focused: BlackTech's attacks are often targeted at sensitive sectors such as government agencies, defense contractors and high-tech companies.
2. Customized Malware: The group develops and uses customized malware to suit its needs. This often includes advanced malware and spy tools.
3. Assassination Campaigns: BlackTech specializes in targeted attacks involving assassination campaigns against specific individuals or organizations. This often involves the use of social engineering tactics and advanced spyware.

Known Attacks:

One attack campaign by BlackTech, dubbed WaterBear, involves a complex attack vector involving exploited vulnerabilities to infect a target computer system with documents. It extends its capabilities to infiltrate target systems using malware called DinoDrop and uses this tool to steal information.

Aims and Objectives:

BlackTech's main objective is to obtain sensitive information from strategically important government and industry sectors. This information can often be on critical topics such as strategic plans, defense technologies or economic data. The group aims to use this information to gain political or economic advantages.

APT34

APT34, also known as OILRIG, is an advanced persistent threat (APT) group based in Iran.

This group is considered an intelligence unit that conducts cyber espionage and cyber attacks in support of Iran's strategic interests.

APT34 is capable of conducting cyber attacks against various sectors and is supported by the Iranian government.

Main Features:

1. 1. Iranian Government Connection: APT34 is a cyber espionage group closely associated with the Iranian government. The group operates in support of Iran's strategic interests.
2. 2. Target Diversity: APT34 conducts attacks against a range of sectors, including energy, defense, telecommunications, finance, and government. Targets often include foreign governments, companies, and strategic positions of hostile countries.
3. 3. Social Engineering Capabilities: The group uses social engineering tactics to infiltrate its targets. This can include manipulation and fraud to gain the trust of victims and spread malware.
4. 4. Malware: APT34 specializes in the use of malware. Specifically, it uses various types of malware to infiltrate its targets.

Known Attacks:

One of APT34's most notable attacks is the Phosphorus campaign against numerous government and private sector organizations around the world. This campaign involves cyber espionage and information gathering operations against targets.

Purpose and Target:

APT34 operates to protect and advance the strategic interests of the Iranian government. Its targets include foreign governments, the energy sector, military defense, and strategic information.

IoC için tıklayın.

Lazarus

Lazarus is an advanced persistent threat (APT) group that operates worldwide and has its origins in North Korea.

This cyberattack group is known for various cyber espionage, financial crimes and cyber sabotage operations.

Lazarus is known as a group that conducts highly sophisticated and targeted cyberattacks, focusing on high-profile targets among governments, financial institutions and large corporations around the world.

Main Features:

1. **North Korean Connection:** Lazarus APT grubunun kökeni, Kuzey Kore olarak belirtilir ve bu nedenle devlet destekli bir grup olduğuna inanılır.
2. **Cyber Espionage and Financial Crimes:** Grup, siber casusluk operasyonlarının yanı sıra finansal suçlar konusundaki yetenekleriyle de dikkat çeker. Daha önce banka soygunları, kripto para hırsızlıkları ve fidye yazılım saldırıları gerçekleştirmişlerdir.
3. **High Profile Targets:** Lazarus, hükümetler, finans kuruluşları ve büyük şirketler gibi yüksek profilli hedefleri hedef alır. Özellikle finans sektörüne yönelik saldırılar, grup için finansal kazanç elde etmenin bir yolu olarak öne çıkar.
4. **Complex Malware:** Grup, karmaşık kötü amaçlı yazılımlar ve siber casusluk araçları kullanır. Bu, saldırılarının tespit edilmesini zorlaştırır.

Known Attacks:

One of the most famous attacks by the Lazarus APT group is the Sony Pictures attack in 2014. The group has also carried out numerous large attacks targeting financial institutions. These include the Bangladesh Central Bank hack in 2016 and the WannaCry ransomware attack in 2017.

Aims and Objectives:

The main goal of the Lazarus APT group is to operate for various purposes of the North Korean government. These include financial gain, espionage, and protecting national interests. The group seeks to generate revenue by targeting the international financial system, while also focusing on gathering information by conducting espionage operations.

IoC için tıklayın.


ECHO
CYBER THREAT INTELLIGENCE