ON2IT AND AMS-IX PRESENT: THREAT TALKS

threat-talks.com

Threat Talks
Breaking the bank
Financial sector cybersecurity threats

The financial sector faces a significant cybersecurity challenge, with nearly one-fifth of reported cyber incidents in the past two decades targeting financial institutions. This exposure is concerning, especially considering the sheer volume of attacks. Take JPMorgan Chase, the largest U.S. bank, for example. Despite a robust security posture, they experience a staggering 45 billion cyber events daily – a number that highlights the constant barrage these institutions face.

But what exactly is the impact of this reality on the business of the bank? Are humans the weakest link when it comes to financial cybersecurity? And how do you stop modern day bank robbers from targeting your financial institution?

In this **'Breaking the bank'** episode of Threat Talks we explore why the financial industry is such a popular target and what financial institutions can do to face this reality head-on. After all, surely robbing a bank shouldn't be as easy as the movies make it seem.

In this episode of Threat Talks we will discuss the following threats:

- Swift Gateway vulnerabilities
- Android Banking Malware (Vulture)
- Binance Hack

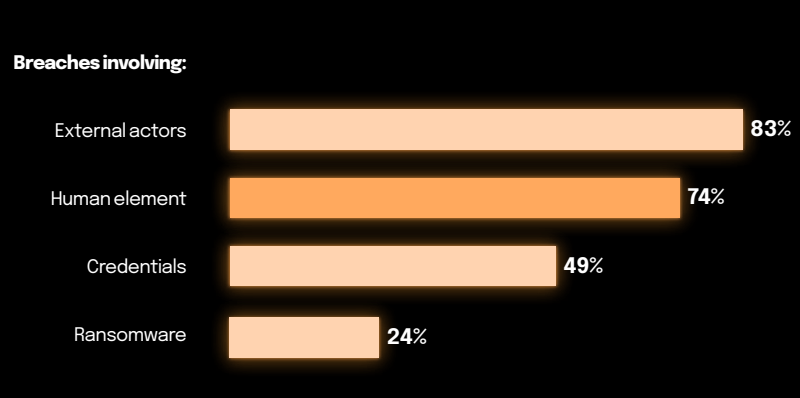
Nearly one-fifth of reported cyber incidents in the past two decades targeted financial instutitions.

Source: Advisen Cyber Loss Data; CISSM; International Telecommunication Union publication

The financial sector has suffered more than 20,000 cyberattacks, causing 12 billion in losses over the past 20 years.

Source: Advisen Cyber Loss Data and IMF staff calculations

74% of all breaches include the human element.



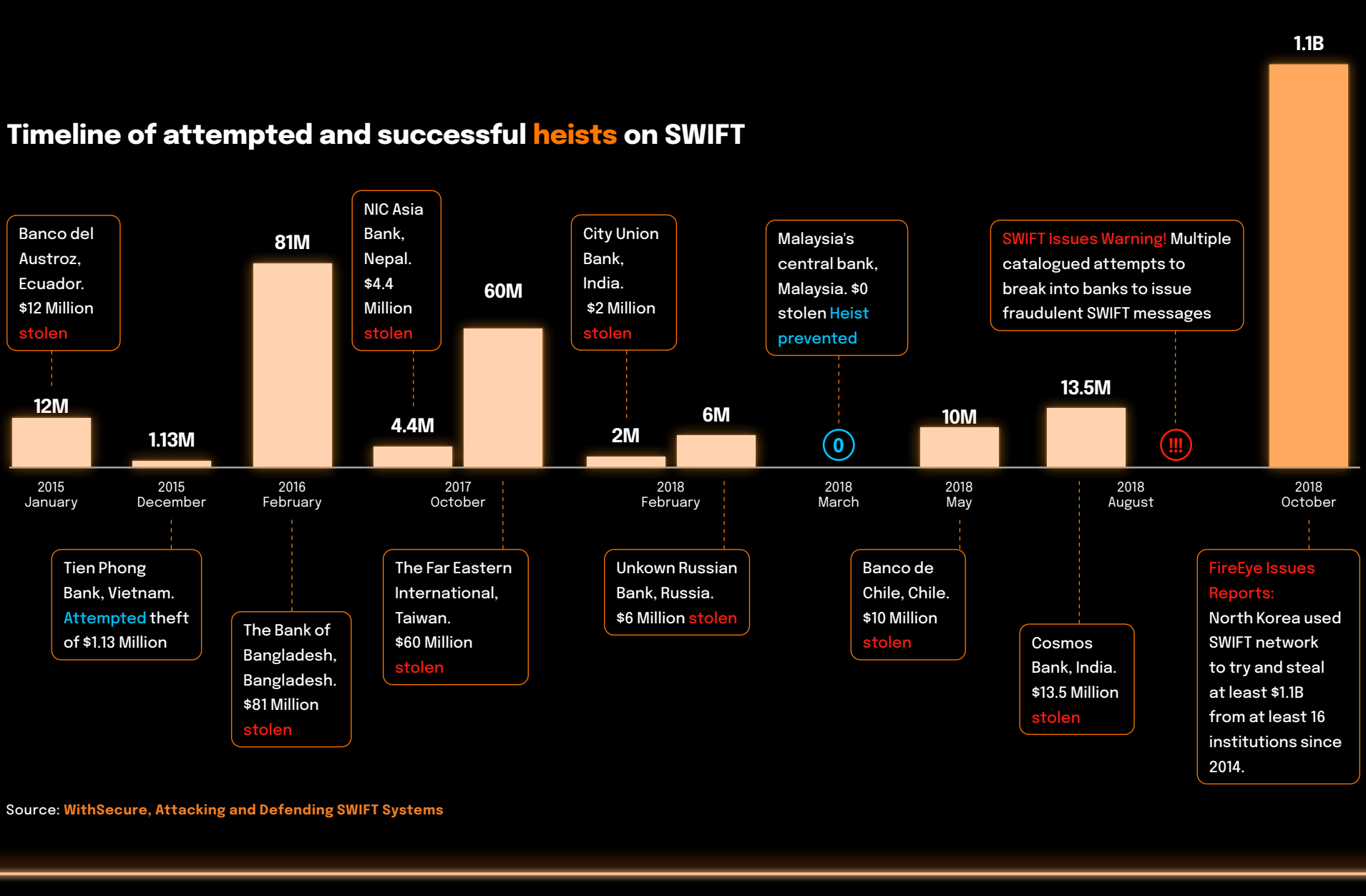
The human element risk cannot be understated.
74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

83% of breaches involved External actors, and the primary motivation for attacks continues to be overwhelmingly financially driven, at 95% of breaches.

Looking for access on multiple fronts.
The three primary ways in which attackers access an organization are stolen credentials, phishing and exploitation of vulnerabilities.

Source: Verizon's 2023 Data Breach Investigations Report: Finance Snapshot

Timeline of attempted and successful heists on SWIFT



Source: WithSecure, Attacking and Defending SWIFT Systems

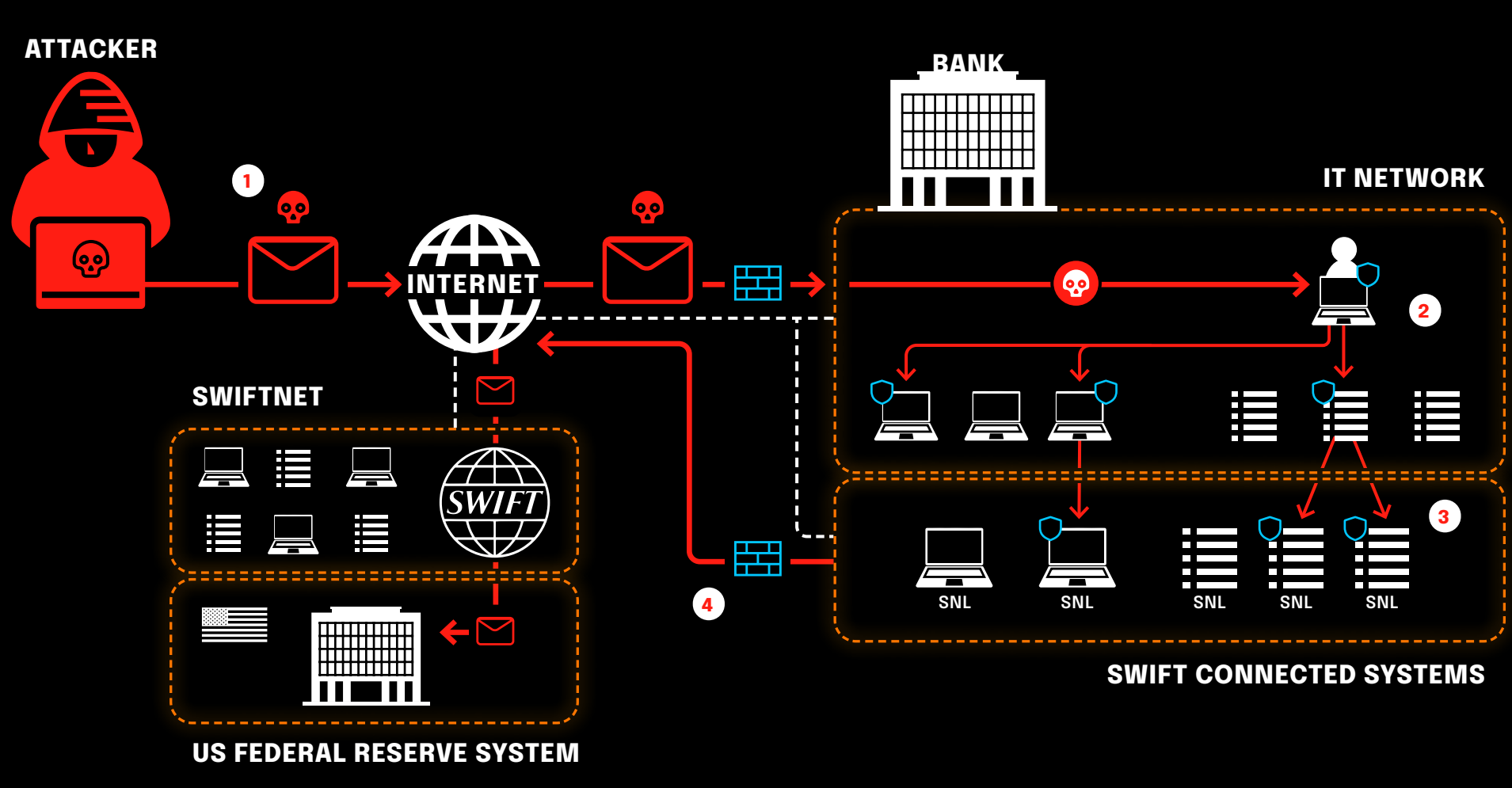
Bangladesh Bank SWIFT attack

On February 4, 2016, the Bangladesh Bank cyber heist resulted in the loss of $81 million from the bank's account at the Federal Reserve Bank of New York. Hackers initially aimed to steal $951 million using fraudulent SWIFT transfer requests. They used spear phishing, custom malware, and a secure file wiper to breach the bank's systems and launder money through Philippine casinos.

mSOC confidence score Confirmed
Threat category Cyber Attacks - Heist
Severity Critical

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1071 - Application Layer Protocol	Exploit SWIFT messaging system	Use of legitimate credentials	High	Financial Institution

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1037 - Filter Network Traffic M1031 - Network Intrusion Prevention	Malware Infection	Network Traffic Monitoring	High	Advanced Persistent Threats (APTs)



Spear phising

1. The attacker used spear phishing emails themed around job applications, which contained malicious zipped attachments. The initial foothold was gained in March 2015, almost a year before the attacker acted on their objectives.

M Implementing email filtering systems to detect and block malicious attachments before they reach the user can help mitigate these attacks. Additionally, employee training programs focused on phishing awareness can significantly reduce the likelihood of successful attacks. Multi-factor authentication (MFA) can add an extra layer of security, making it more difficult for attackers to gain access even if they obtain credentials. EDR solutions can monitor and respond to suspicious activities on endpoints and prevent malware executions. Some firewalls can prevent leaking credentials on phishing websites through "Credential Phishing Prevention."

Patient 0

2. After infecting the initial victim, the attacker began harvesting credentials and moving laterally within the bank's network. They infected new systems by installing additional backdoors, eventually gaining a foothold on SWIFT-connected systems. Command and control (C2) communications were camouflaged using a fake TLS protocol to evade detection.

M Network segmentation and a Zero Trust architecture can limit lateral movement and reduce the blast radius of an attack. Implementing strong password policies and monitoring for unusual login activities can help detect and mitigate credential harvesting attempts. The use of firewalls and network traffic monitoring can assist in detecting suspicious traffic activities.

Dwelling

3. At this point, the attacker managed to compromise local administrator accounts and installed legitimate software to monitor employee activities. This allowed them to learn how financial messages were sent, enabling them to capture SWIFT credentials.

M Removing local administrator rights from users can prevent attackers from easily escalating privileges and installing unwanted legitimate software. EDR solutions can help detect behaviors that deviate from the norm.

Act on objectives

4. After a long dwell time, the attacker deployed new malware specifically designed to target the SWIFT Alliance Access application. This malware bypassed security controls and removed evidence from printed SWIFT messages. It interacted with the process loading the liboradb.dll file, tampering with it by overwriting 2 bytes at a specific offset. This modification forced the application to always pass validity checks, allowing the malware to execute database transactions. The attacker used a secure file wiper to erase any traces of their activities from the systems they compromised.

B: Deploying advanced threat detection systems that can identify and respond to suspicious file modifications and unusual process activities is crucial. Regular integrity checks of critical system files and configurations help detect unauthorized changes. Additionally, implementing application whitelisting can prevent unauthorized applications and malware from executing.

Heist

5. The attackers were able to issue a total of 35 SWIFT transactions worth $951,000,000. Only $81,000,000 of this amount was successfully exfiltrated from the US Federal Reserve to fake bank accounts in the Philippines. The funds were then laundered through multiple private baccarat junkets in various casinos and ultimately extracted and transported to Macau, where the trail was lost.

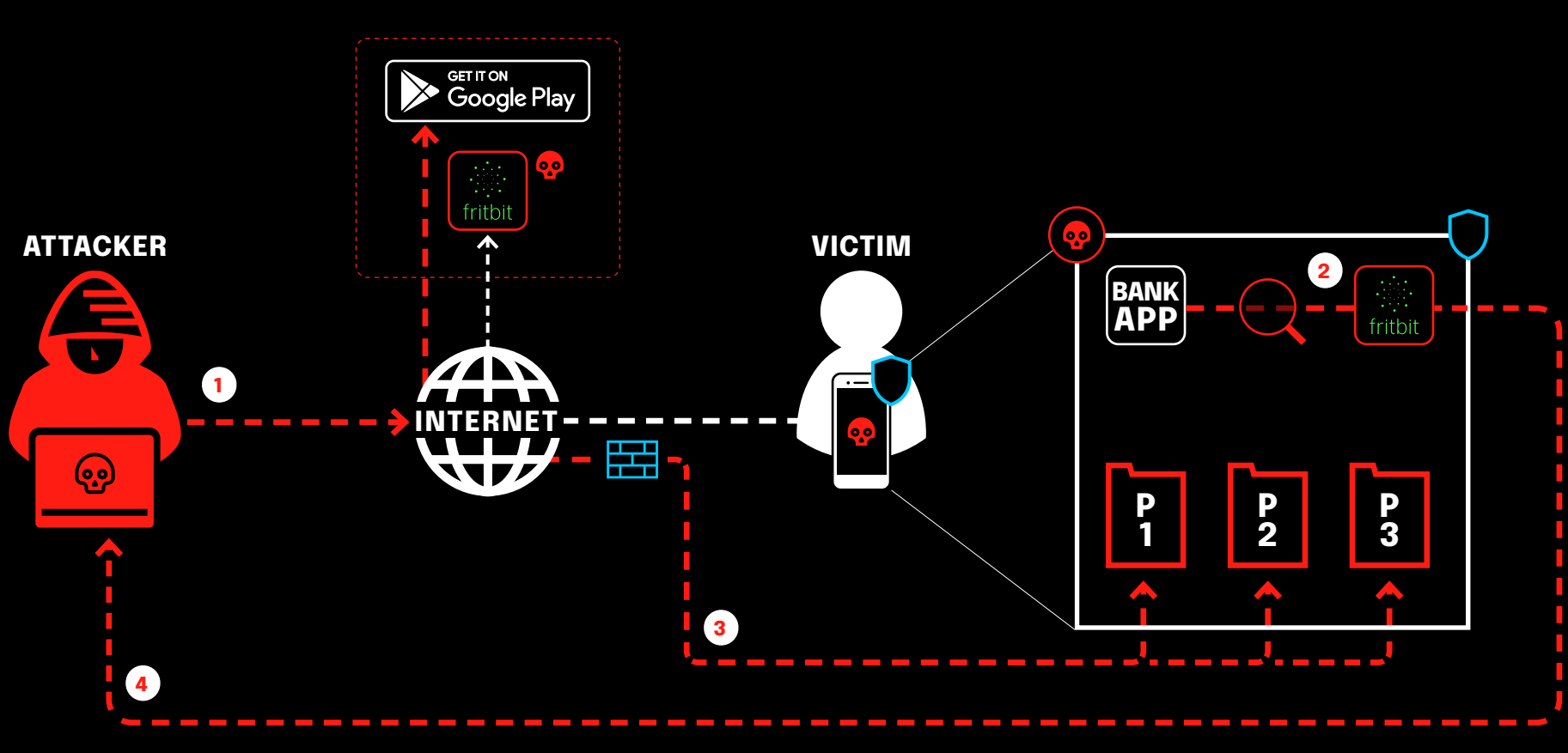
Vultur Android Malware

On March 28, 2024, NCC Group reported on the expansion of the Android malware Vultur, which has increased its capabilities and targets. Initially focused on keylogging, Vultur now employs screen recording and accessibility services to capture sensitive user data from banking and financial apps, posing significant risks to users' financial information.

mSOC confidence score Verified
Threat category Malware - Spyware information-stealing
Severity High

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
T1660 - Mobile Phishing	Install malicious app disguised as a legitimate application	Encryption and Tunneling	Medium	Individuals

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1058 - Antivirus/Antimalware	Malware infection	Network traffic	High	Cybercriminals



Dropper

1. The threat actor uploads the malicious app (dropper[1]) to the Play Store or, alternatively, uses social engineering to convince the victim to download the malicious app disguised as a legitimate application.

M Always make sure to download legitimate applications by carefully checking the names and the source.

Infection

2. The victim installs the malicious application and continues using their phone as usual without noticing any changes. Once the victim opens a banking app, the dropper detects it and contacts the C2 server to download the appropriate malware (Vultur in this case).

M Some EDR solutions provide support for Android and iOS devices, which may help prevent or detect infections. Steering traffic over a SASE or firewall solution can help detect malicious traffic or destinations.

Payloads

3. At this stage, the dropper decrypts and executes three different payloads, which provide the attacker with accessibility services privileges, set up ngrok[2]/alphaVNC[3], and implement C2 methods and FCM[4] (Firebase Cloud Messaging) commands. The payload is broken down into three stages to make analysis more complex.

M Some EDR solutions provide support for Android and iOS devices, which may help prevent or detect infections.

Communication and functionalities

4. The malware communicates with the C2 server using AES encryption and Base64 encoding, evading detection. At this point, the attacker can:
   - Download, upload, delete, install, and find files.
   - Control the infected device using Android Accessibility Services, enabling actions such as scrolling, swipe gestures, clicks, and muting/unmuting audio.
   - Prevent apps from running.
   - Display custom notifications in the status bar.
   - Disable Keyguard to bypass lock screen security measures.

This enables the threat actor to easily steal funds from the victim's bank account.

M Steering traffic over a SASE or firewall solution can help detect malicious traffic or destinations.

[1] A dropper is a type of malware designed to deliver and install other malicious payloads onto a target system.

[2] Ngrok is a tool that creates secure tunnels to localhost, enabling developers, or in this case, threat actors, to expose their local development servers to the internet through a secure URL.

[3] AlphaVNC is a remote administration tool that allows users to control and monitor Android devices remotely by providing a VNC (Virtual Network Computing) server interface. It enables full access to the device's screen and inputs over the network.

[4] Firebase Cloud Messaging (FCM) is a messaging service that allows developers to send notifications and messages to users across platforms, including Android, iOS, and web applications.

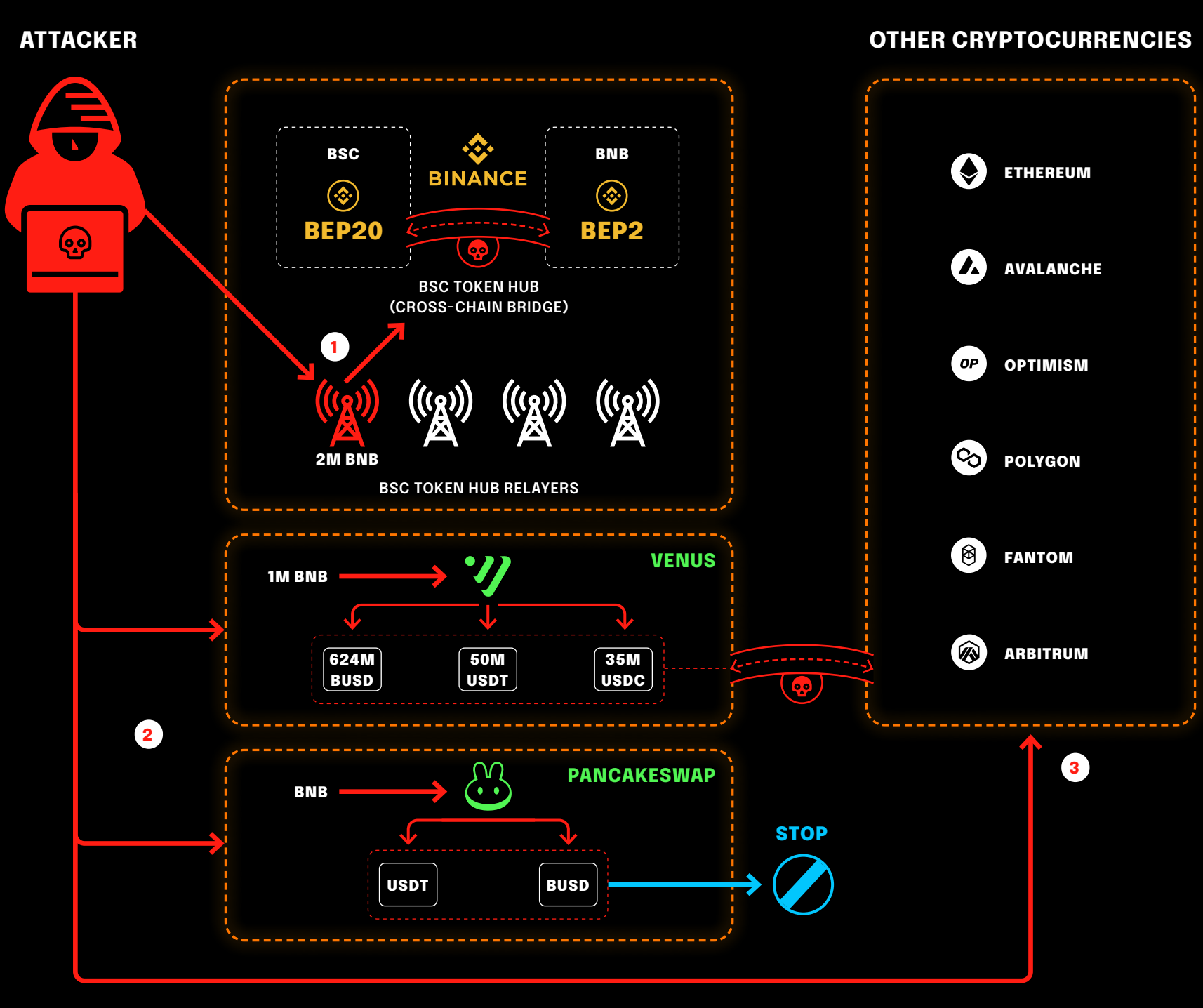
Binance Chain exploit

On October 6, 2022, BNB Chain, the blockchain of crypto exchange Binance, was temporarily paused due to a cross-chain bridge exploit. Attackers stole an estimated $110 million worth of cryptocurrency by exploiting a vulnerability in the BSC Token Hub. The incident led to the suspension of all deposits and withdrawals on the network.

mSOC confidence score Verified
Threat category Misconfigurations - insecure implementation
Severity High

ATT&CK Technique	Attack Strategy	Evasion	Complexity	Target Type
not applicable	Cross-chain bridge exploit	Use of Multichain routers and burner wallets	High	Enterprises

ATT&CK Mitigation	Attack vector	Detection	Threat level	Threat Actor Type
M1047 - Audit	Crosschain bridge vulnerability	Monitoring crosschain transaction	High	Cybercriminal



Relay registration and exploit

1. The attacker used 100 BNB to register as a relayer[1] for the BSC Token Hub[2]. At this point, the attacker was able to exploit a bug in the way BSC Token Hub verifies proofs, allowing them to forge messages and manipulate the bridge to create and withdraw 2 million BNB in two transactions.

M Regular audits and rigorous security testing of cross-chain bridges can help identify and fix vulnerabilities before they can be exploited.

Generate new tokens

2. The attacker used Venus Protocol to deposit 1M BNB as collateral and borrow stablecoins[3] (USDT, USDC, BUSD). At the same time, the attacker swapped some of the remaining BNB for USDT and BUSD using PancakeSwap. This last attempt was unsuccessful due to Binance halting all transactions on their blockchain.

M Implementing real-time monitoring and automated alerts for unusual activity can help detect and mitigate malicious actions quickly.

Evasion

3. The attacker used bridging services such as Stargate Finance and Multichain to move the newly obtained stablecoins across several blockchains, swapping coins and providing collateral using multiple different burner addresses. This obfuscation made it difficult to track and recover the stolen funds.

M Enhanced tracking of cross-chain transactions and cooperation with other blockchain networks can improve the chances of recovering stolen funds and identifying the attackers.

[1] A relayer is a node that facilitates cross-chain communication by forwarding transactions and messages between different blockchain networks, ensuring that actions on one chain are reflected on another.

[2] The BSC Token Hub is a cross-chain bridge that facilitates the transfer of assets between Binance Chain and Binance Smart Chain (BSC), enabling interoperability between the two blockchains.

[3] Stablecoins are a type of cryptocurrency designed to maintain a stable value by being pegged to a reserve of assets such as fiat currency (e.g., USD) or other stable assets.

Taxonomy

ATT&CK Technique
Which technique of the MITRE ATT&CK framework does the threat correspond to.

ATT&CK Mitigation
Which mitigation of the MITRE ATT&CK framework can be applied.

Attack Strategy
Plan devised by the attacker to exploit specific system vulnerabilities.

Attack Vector
What is the primary method of attack.

Evasion
Tactics used by the attacker to avoid detection or bypass security.

Detection
Mechanism to identify malicious activities or system anomalies.

Complexity
How easy it is to exploit the vulnerability or carry out the attack.

Threat Level
How severe the threat is.

Target Type
The category of organization that may potentially be targeted.

Threat Actor Type
What type of threat actor may be involved.

CONTACT US

mSOC score explanation:
We assign scores to both our sources and the news items. Sources are scored on a numeric scale ranging from 0 (untrustworthy) to 5 (verified), while news items are scored with a letter, ranging from E (unreliable) to A (reliable). By considering the scores of both the source and the news item and the quality of the available information, we classify the overall reliability into three categories: Confirmed, Verified, and Credible. Interested in learning more about our reliability scoring system for sources and news items? Our Threat Intelligence team would be happy to walk you through our procedure, so please don't hesitate to reach out.

threat-talks.com

ON2IT ZERO TRUST INNOVATORS amsix