ANALYZING ENDPOINT VULNERABILITIES AND NETWORK EXPLOITATION IN MODERN BANK CYBER HEISTS

Vijayaraghavan K, LLM, School of Criminal Law and Criminal Justice Administration, Tamil Nadu Dr. Ambedkar Law University, School of Excellence, Taramani, Chennai 600113, Tamil Nadu, India

ABSTRACT

The evolution of financial crime has culminated in highly sophisticated cyber heists targeting global banking infrastructures, moving away from physical bank robberies toward digital, transnational operations. The article examines three pivotal case studies that redefined the threat landscape of financial technology: Bangladesh Bank heist, Carbanak heist and Cosmos Bank heist. The 2016 Bangladesh Bank heist underlines the compromised the central bank's local SWIFT terminal. In contrast, the Carbanak heist (2013–2015) highlighted a prolonged, multi-institution assault targeting internal banking networks rather than external payment rails. The 2018 Cosmos Bank heist exemplified a hybrid approach, combining infrastructure manipulation with coordinated, real-world execution. Attackers targeted the cooperative bank by creating a malicious proxy server that intercepted and isolated the bank's central switching system from its core banking backend. Cumulatively, these three heists underscore a critical paradigm shift in banking security. They expose how modern cybercriminals exploit the weakest links in the financial ecosystem, utilizing temporal gaps, internal human vulnerabilities, and isolated network infrastructures. In response, the global banking sector has been forced to abandon perimeter-based defences in favour of Zero Trust architectures, advanced behavioural analytics, and stringent endpoint monitoring for cross-border financial routing systems.

Keywords: Malware reconnaissance; Bangladesh bank heist; Carbanak heist; Cosmos bank heist; cybersecurity.

1 Introduction

The landscape of bank robberies has transformed fundamentally due to technological advancements. An analysis of bank heists spans across three distinct dimensions: the modern evolution of real-world financial crimes, the mechanics of popular tabletop/video games, and their portrayal in cinematic pop culture. The modus operandi of bank robberies transformed from physical to digital nature. Traditional, armed bank heists have sharply declined globally. Physical bank branches no longer hold massive reserves of unallocated cash or gold. Security features like time-release vault mechanisms, GPS-tracked dye packs, and immediate silent alarms limit a physical robber's window of success to under 45 seconds. Consequently, organized crime has shifted heavily toward cyber heists and tactical displacement, such as targeting isolated ATMs or armoured transport trucks. To stop hackers from moving horizontally across their internal networks after an initial breach, modern banks rely on a zero trust architecture that isolates critical environments, continuously verifies user identities, and automatically blocks suspicious internal traffic. Cyber bank heists almost always fail to reach their full potential or get exposed due to a mix of human operational errors, system-level design flaws, and unexpected timing mismatches. While hackers often spend months executing highly sophisticated network intrusions, the ultimate collapse of their plans generally stems from simple tactical mistakes, automated defensive triggers, or cross-border procedural discrepancies.

2. General Bank Cybersecurity Mechanisms

The primary cybersecurity defences banks use to prevent lateral movement include the following structural protections:

2.1 Network Micro-Segmentation

Banks have abandoned traditional "flat networks" where a breach on a receptionist's computer grants visibility over the entire organization.

- **Granular Isolation:** Networks are sliced into tiny, isolated zones based on business functions (e.g., separating standard HR workstations from SWIFT transaction terminals).
- **Next-Generation Firewalls (NGFWs):** Traffic moving *between* these internal zones

must pass through strict firewalls that inspect packets for malicious payloads.

- **Default Deny Policies:** Internal communication rules are set to block all traffic by default, only allowing explicitly approved connections between specific server pairs.

2.2 Identity and Access Management (IAM)

Once inside, attackers try to escalate privileges by stealing passwords or administrative tokens. Banks prevent this using strict access controls:

- **The Principle of Least Privilege (PoLP):** Employees are only granted the absolute minimum network permissions necessary to complete their specific tasks.

- **Just-In-Time (JIT) Access:** Administrative privileges are temporary, expiring automatically after a short, predefined window.

- **Phishing-Resistant MFA:** Hardware-based multi-factor authentication security keys are required to access critical segments, ensuring stolen passwords alone cannot grant deeper network entry.

2.3 Endpoint Detection and Response (EDR) & XDR

Because attackers attempt to blend in with legitimate user behavior, banks monitor endpoints constantly.

- **Behavioral Analytics:** EDR agents installed on all workstations flag actions like an accounting PC suddenly trying to scan network ports or running PowerShell commands.

- **Deception Technology:** Security teams deploy "honeypots"—fake servers or decoy databases that look attractive to hackers. If an intruder interacts with a honeypot, an immediate, high-priority alarm is triggered.

- **Automated Isolation:** When an anomaly is detected, Extended Detection and Response (XDR) systems can instantly isolate the infected machine from the network, containing the threat before it can move.

3. Bangladesh Bank Heist

The 2016 Bangladesh Bank Heist falls out to be a classical piece of information that focuses on cyber theft orchestrated by the state-sponsored Lazarus Group. On 4th and 5th of February 2016 the cybercriminals executed the audacious digital robbery that targeted the central bank of Bangladesh and resulted in the theft of $81 million, and they further attempted to siphon a total of $951 million from the bank's foreign exchange account held at the Federal Reserve Bank of New York. While a typo ("fandation" instead of "foundation") and timing discrepancies flagged the security teams, the attackers successfully made away with $81 million, transferring it from the bank's account at the Federal Reserve Bank of New York to accounts in the Philippines. Unlike traditional robberies, the hackers did not breach the core SWIFT Global Network, instead they hijacked the bank's local endpoints to manipulate transactions. The attack targeted the internal interfaces, logs, and database structures that connect a local institution to the broader financial ecosystem.[1] By scheduling the attack over a weekend across disparate time zones, the hackers bypassed immediate scrutiny to issue 35 fraudulent transfer orders summed to $951 million to the Federal Reserve Bank of New York. While automatic fraud filters flagged a typo and halted most transactions, $81 million successfully routed to the Philippines, where it was rapidly laundered through casinos. This heist demonstrated that trusted international financial communication protocols are highly vulnerable if the local endpoints are compromised.[2]

3.1 Defence Evasion Mechanisms

The attackers deployed customed Trojan termed as evtdiag.exe a highly targeted malware suite. The malware was specifically designed to bypass the bank's local network defences and was deployed to cover their tracks.[3]

- **Database & Ledger Manipulation:** The malware was targeted to directly modified the local Oracle database of the bank's SWIFT Alliance Access software. The malware was designed to intercept the database search results, thereby dynamically deleted

[1] https://www.bbc.com/news/stories-57520169
[2] Mazumder Md., and Sobhan Md., Bangladesh Bank Cyber Heist: Incident Analysis, 2021. https://repository.gatech.edu/bitstreams/df3d1c19-47be-4738-a855-9c049b709d52/download
[3] Samima Nasrin S. Combating Cybercrime in the Financial Sector: A Study on Problems, Preventions, and Cyber Laws of Bangladesh, Woxsen Law Review, 2023. https://woxsen.edu.in/woxsen-law-review/wlr-papers/Combating-cybercrime-in-the-financial-sector-A-study-on-problems-preventions-and-cyber-laws-of-Bangladesh/

traces of the fraudulent transfer confirmations.

- **Disabling Forensic Logging:** The malware also bypassed standard logging mechanisms by into hooking system APIs. Due to the systematic deletion of transaction logs i.e .dat files and registry entries, so that no suspicious movement in traffic was detected by security teams while looking at the system history as it appeared as a normal operation.

- **Hardware Interception (Printer Sabotage):** The bank relied on real-time automated physical printer configured to print confirmation receipts of all SWIFT transactions. The malware was specifically programmed to block the system's printing queue, thus it appeared as a hardware "glitch" that delayed bank employees from analysing the outgoing transactions for nearly over 24 hours.

- **Blending via Stolen Credentials:** The malware harvested legitimate admin login credentials during the espionage phase, thus the transaction commands appeared entirely authorized to security algorithms. Due to absence of "exploit payloads" flying over the firewall, it did not trigger signature-based Intrusion Detection Systems (IDS).

3.2 Intruder Mode & Operational Matrix

The Lazarus Group designed their internal tools to step through different "modes" of operation over a multi-month period reconnaissance which ensured them to garner credentials and intelligence before initiating the heist.[4,5]

- **Initial Access & Lateral Movement Mode:** The access and lateral movement was triggered through targeted spear-phishing emails which contained malware disguised as job applications. Once a single employee machine was compromised, the intruder payload scanned the local area network, looking for the highly specific subnet holding the bank's SWIFT terminal.

[4] Mohammad Sami A Kabir, *Lessons Learned From the Bangladesh Bank Heist*. ISACA Journal, 2023. https://www.isaca.org/resources/isaca-journal/issues/2023/volume-6/lessons-learned-from-the-bangladesh-bank-heist

[5] Mazumder Md., and Sobhan Md. The Spillover Effect of the Bangladesh Bank Cyber Heist on Banks' Cyber Risk Disclosures in Bangladesh, Journal of Operational Risk, 2020. DOI - 10.21314/JOP.2020.249

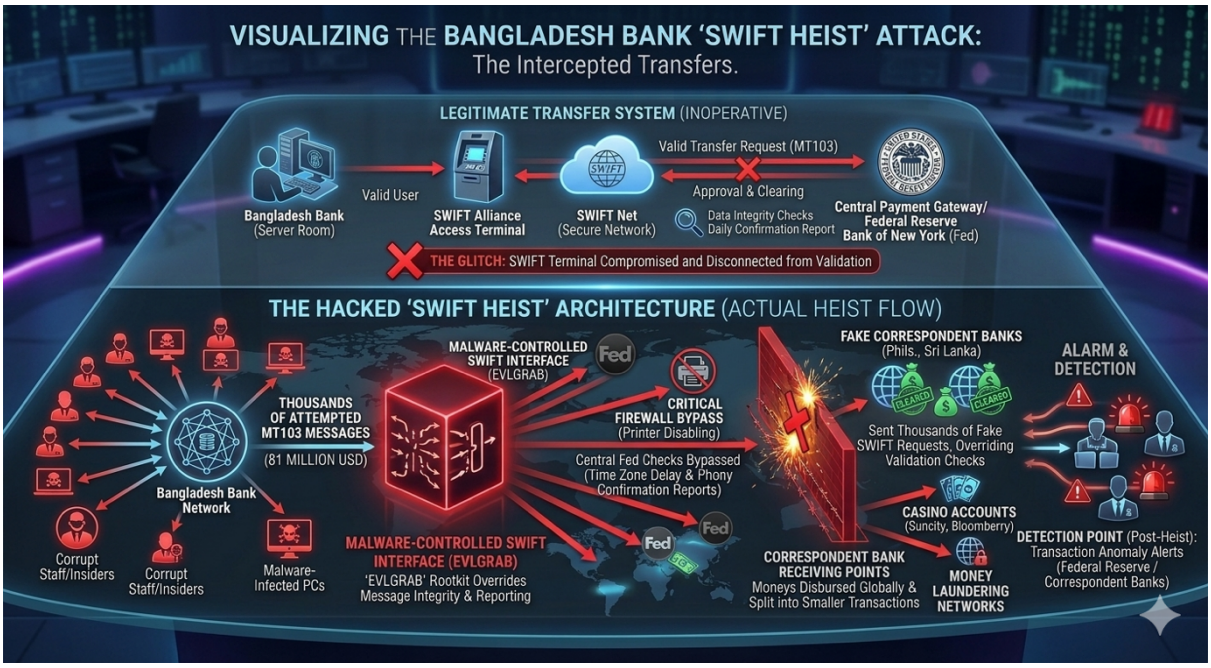

Fig 1. Bangladesh Bank SWIFT Heist Attack

- **Passive Watcher (Reconnaissance Mode):** Once inside the SWIFT-connected segment, the intruder stayed completely passive. Instead of firing heavy commands, it recorded keylogs and mapped the workflow. The hackers monitored the precise layout of financial messages known as MT103 messages and learned the strict dual-authorization steps used by bank managers. The attackers did not just use the stolen credentials to manually type in requests. They deployed a highly specialized tool known as the evatg.exe malware, which was later identified by BAE System Applied Intelligence.[6]This malware sat actively inside the local SWIFT server architecture to alter financial messages in real-time. The MT103 and MT202 Issuance, armed with administrative authorization, the attackers dispatched 35 fraudulent MT103 messages (Single Customer Credit Transfers) and MT202 messages (General Financial Institution Transfers) to the Federal Reserve Bank of New York. The malware actively intercepted and watched the bank's internal database which was specifically running on Oracle tables tracking the SWIFT environment. It was designed to run automated database queries that searched for, altered, and deleted confirmation lines containing the exact tracking numbers of the fraudulent transactions.

[6] https://www.bankinfosecurity.com/report-swift-hacked-by-bangladesh-bank-attackers-a-9061

- **Active Interception & Emulation Mode:** On Thursday, February 4, 2016, the intruder payload activated its weaponized features. It intercepted the session, injected the pre-staged fraudulent transfer commands, and simulated real employee keystrokes.

- **Timing Matrix Mode:** The intruder systematically capitalized on global time zones. They initiated the attack on a Thursday evening in Bangladesh (their weekend start), which rolled into Friday morning in New York (processing time), which then led to the Chinese New Year weekend in the Philippines—ensuring that banks on three separate continents were non-operational or delayed when trying to communicate stop-payment orders.

3.3 After Attack

Following international forensic investigations, it was revealed that the hackers belonging to the Lazarus Group successfully moved laterally through the Bangladesh Bank's internal infrastructure due to following factors viz: the network was completely flat, unmonitored, and relied on cheap, unmanaged network switches. This structural flaw allowed the attackers to pivot from a low-security endpoint that was compromised through a phishing email directly onto the high-value local server hosting the SWIFT Alliance Access software. The Bangladesh Bank and the global SWIFT network was completely rebuilt by enhancing their security architectures. SWIFT established the mandatory Customer Security Programme (CSP), forcing all participant banks to implement strict controls to block internal lateral migration.[7,8]

The following primary cybersecurity defenses were implemented to prevent lateral movement in bank network following the Bangladesh Bank heist:

3.3.1 Eliminating Flat Networks via Micro-Segmentation

The attackers' ability to map out and access the SWIFT server room from a standard office workstation was the single biggest failure point of the original architecture.

- **Physical and Logical Air-Gapping:** The SWIFT Alliance Access terminal environment was completely isolated from the bank's general local area network

[7] Scribd Case Database, Bangladesh Bank Heist Case Study, 2024. https://www.scribd.com/document/724862038/Bangladesh-Bank-Heist-Case-Study
[8] Mohammad Tanvir Hossain, An Overview of Cybersecurity Threat Evaluation in Banking Systems. Science and Engineering Research Journal, 2024; 12(1); 1-13

(LAN). The SWIFT is now located behind the multi-layered dedicated hardware firewalls.

- **Strict IP Access Control Lists (ACLs):** Only a tiny, predefined number of authorized internal administrative IP addresses are allowed to communicate with the SWIFT gateway. All horizontal traffic coming from standard office workstations, email servers, or guest networks is blocked by default.

3.3.2 Implementation of Privileged Access Management (PAM)

In 2016, the attackers managed to harvest legitimate credentials to log into the SWIFT software and send 35 fraudulent MT103 money transfer requests summing to nearly $1 billion.

- **Two-Factor Authentication (2FA) for All Core Systems:** Multi-factor authentication was made strictly mandatory for accessing any machine within the payment processing zone. Static, reusable passwords alone can no longer grant access.

- **Session Recording and Credential Vaulting:** Administrators must now log into a secure PAM "jump server" to access critical environments. This server randomizes administrative passwords continuously and records all terminal sessions in real time, preventing hackers from scraping permanent access tokens out of local memory.

3.3.3 Endpoint Detection and Threat Hunting (EDR)

The hackers lived inside Bangladesh Bank's network undetected for nearly a year, deploying a customized rootkit (EVLGRAB) that modified the local SWIFT database software and deleted confirmation logs to hide their tracks.

- **Behavioral File Integrity Monitoring (FIM):** Modern defenses employ FIM tools on financial transaction servers. If any unauthorized process or piece of malware attempts to modify system libraries, database schemas, or printer log queues, the system instantly triggers a critical alert and locks down the environment.

- **Continuous Behavioral Analytics:** Legacy signature-based antivirus applications were replaced with Endpoint Detection and Response (EDR) agents. These agents analyze real-time system behaviors, immediately flagging and killing processes if a

machine begins unusual internal network scanning, port probing, or credential-dumping activities.

3.3.4 Hardware Hardening and Ledger Synchronization

A critical operational failure during the heist occurred when the malware corrupted a local script, breaking the physical printer that generated paper confirmation logs of transfers.

- **Decentralized, Tamper-Proof Log Streaming:** Financial reporting logs are no longer just stored locally where malware can modify or delete them. They are securely streamed in real time to immutable, off-site SIEM (Security Information and Event Management) systems that cannot be modified by an internal network intruder.

- **Out-of-Band Validation:** Banks implemented secondary, out-of-band verification systems that check ledger changes against independent, external payment paths to catch anomalies even if the primary local network is entirely compromised.

3.4 Structural Defensive Overhaul

[Phishing Entry Point] ──> [Office LAN Segment] ──X── [Next-Gen Firewall / PAM Gateway] ──> [Isolated SWIFT Terminal] (Blocked by EDR & Real-Time SIEM)

The 2016 Vulnerability in Bangladesh Bank was directed on a single compromised PC that gave the attackers an unrestricted network-level access to the SWIFT core infrastructure. The modern defense mechanism focuses on zero-trust framework mandating network micro-segmentation, behavioral EDR surveillance, and strict multi-factor authentication loops.[9]

4. The Carbanak Heist

The Carbanak Heist is considered the largest cyber bank robbery in history, where an Advanced Persistent Threat (APT) group stole up to $1 billion from over 100 financial institutions worldwide. The bank heist was discovered by Kaspersky Lab in 2014, the Carbanak group flipped the traditional cybercrime playbook: instead of targeting banking customers, they hacked the banks directly. When global financial institutions deployed

[9] Micael L.Y., Melissa G.R.G, Kimberly G.M. The Bangladesh Cyberheist: How compliance programs can help protect against cybercrime, *thehedgefundjournal*, 2016; 114 https://thehedgefundjournal.com/the-bangladesh-cyberheist/

countermeasures to stop Carbanak's signature lateral movement tactics, they targeted the group's highly specific methodology: spear-phishing an administrative workstation, stealing credentials via video/keylogging, and migrating horizontally to domain controllers to compromise the SWIFT and ATM infrastructure.[10] The Carbank defense evasion mechanisms and its "intruder" operational modes are being dealt herewith. The Carbanak Heist was not a single-day event but an ongoing, highly sophisticated cyber campaign that actively stole money from banks from late 2013 through early 2015, peaking in June 2014. The full scale of the heist was publicly uncovered and reported on February 16, 2015. The group siphoned approximately $1 billion through diverse vectors, including manipulating account balances, utilizing e-payment systems, and remotely commanding ATMs to dispense cash to waiting mules at specific times. Carbanak proved that prolonged internal network persistence could yield catastrophic, systemic financial losses.[11]

4.1 Modus Operandi

The attackers did not breach the core, global SWIFT network. Instead, they manipulated the target banks' internal workflows, endpoints, and credentials to send completely authorized instructions.[12]

4.1.1 Silent Reconnaissance and Workflow Mapping

- **Video and Screen Capture:** Unlike quick "hit-and-run" malware, the Carbanak backdoor featured advanced video-recording, desktop streaming (VNC), and keylogging plugins.

- **Learning Human Behavior:** Once the attackers pivoted into the restricted SWIFT subnet, they spent months secretly recording the screens of bank clerks, administrators, and operators. They studied exactly how a legitimate worker structured, validated, and

[10] EPC-European Payment Council, Payment Threats and Fraud Trends Report, EPC183-22/Version 1.0: 23 November 2022.
https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2022-12/EPC183-22%20v1.0%202022%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf

[11] Mike L Hackers Hit 100 Banks in 'Unprecedented' $1 Billion Cyber Heist: Kaspersky Lab, Cybercrime, February 15, 2015 https://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab/

[12] Boston University Department of Computer Science, Carbanak Technical Workflow Analysis, https://www.cs.bu.edu/~goldbe/teaching/HW55815/presos/carbanak.pdf

approved a wire transfer.

4.1.2 Exploiting the Local SWIFT Terminal Interface

- **Endpoint Control:** Instead of writing complex scripts to interface with SWIFT APIs directly, Carbanak relied on impersonating a legitimate operator via the compromised local terminal.

- **Credential Harvest:** They captured passwords and session tokens used by authorized personnel to access the local SWIFT Alliance Access (SAA) system.

4.1.3 Generating Fraudulent Message Types (MT)

- **MT103 Standard Execution:** Using the captured user accounts and mimicking the observed workflows, the attackers drafted and approved standard MT103 messages (used for single customer international credit transfers).

- **Legitimate Structure Alignment:** The fraudulent messages used correct syntax, routing tags, and matching cryptographic authentication signatures natively applied by the bank's own local SWIFT terminal modules.

- **Routing to Mule Accounts:** Because the messages appeared fully authorized and correctly formatted, the global SWIFT network smoothly transmitted the instruction to correspondent banks in the US, China, and Europe, routing the funds directly into overseas money-mule accounts.

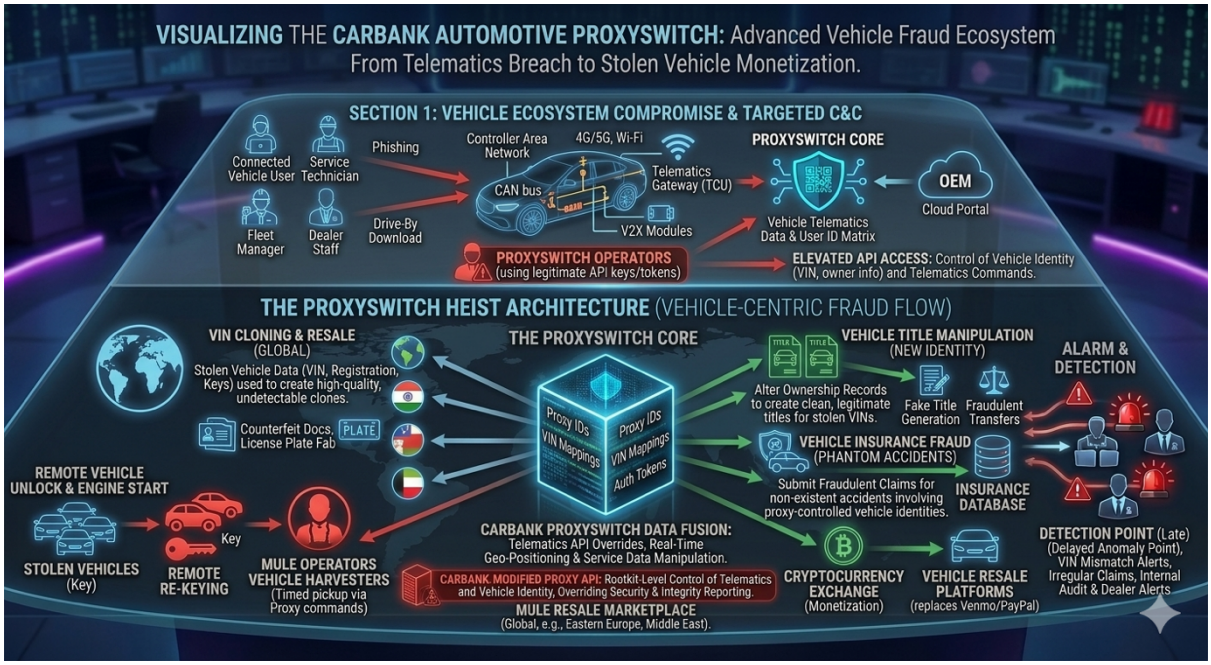

Fig 2. Carbanak Automotive Proxyswitch

4,1.4 Mitigating Detection and Balancing Loops

- **Database Co-manipulation:** To ensure the wire transfers did not trigger immediate account balance alarms internally, Carbanak operators often altered the bank's core Oracle accounting databases.

- **Balance Inflation Cover:** They would artificially inflate an existing account balance (e.g., changing a $1,000 balance to $10,000) right before the SWIFT transfer took place. They would then wire out the excess $9,000 via SWIFT. To the bank's daily automated balancing ledger, the original customer's transaction and actual balance still appeared mathematically intact.

- **The Infiltration:** The attackers used highly targeted spear-phishing emails with malicious attachments to compromise the computers of internal bank employees.

- **The Surveillance:** Once inside, they didn't instantly steal money. They stayed hidden for 2 to 4 months per bank, recording videos, taking screenshots, and keylogging the daily routines of cash transfer clerks.

- **The Cash-Out:** Once they learned the exact software, architecture, and behavioral patterns of the clerks, they mimicked them to siphon cash. They stole money through

three main avenues:

- **ATM Jackpotting:** Commanded specific ATMs to physically dispense cash at scheduled times, where physical "money mules" were waiting to collect it.
- **SWIFT & Wire Fraud:** Transferred millions to overseas dummy accounts via international banking networks.
- **Database Alterations:** Modified oracle databases to inflate account balances (e.g., altering a balance from $1,000 to $10,000) and transferring out the difference so the original customer never noticed.

4.1 Defence Evasion Mechanisms

To bypass corporate firewalls and security software, the Carbanak backdoor used highly advanced anti-analysis and defence evasion techniques:[13]

- **Process Injection & Masking:** The malware injected malicious code into legitimate, trusted active system processes to trick Endpoint Detection and Response (EDR) agents.
- **Software Packing & Obfuscation:** The binaries were heavily packed and encrypted using custom, dynamically generated keys for every unique build. This effectively neutralized traditional signature-based antivirus scanners.
- **Traffic Blending:** Command and Control (C2) communications utilized standard encrypted protocols (like HTTPS) and passed through common networking ports, making malicious traffic indistinguishable from ordinary web browsing.
- **Legitimate Tool Abuse:** Rather than deploying loud, custom hacking utilities, the group leveraged built-in operating system administrative tools (known as "Living off the Land") and commercial administrative software like the Ammyy Remote Administration Tool to manage internal networks without triggering alerts.

[13] Matt Burgess, Inside the Takedown of the Alleged €1bn Cyber Bank Robber. Wired Magazine, April 4, 2018. https://www.wired.com/story/carbanak-gang-malware-arrest-cybercrime-bank-robbery-statistics/

4.2 Intruder Mode & Internal Operation

Carbanak's operations stood out because of how they structured their internal software modules to act as a stealthy "intruder" inside the victim's infrastructure.

- **Automated Reconnaissance Mode:** When first executing, the backdoor functioned in a quiet reconnaissance mode. It scanned the infected registry and local drives exclusively searching for specialized banking applications or retail Point-of-Sale (PoS) database configurations. If none were found, the malware would lay dormant or uninstall to prevent exposing the campaign.

- **Passive Espionage Mode (Intruder Surveillance):** Once a core banking asset was found, the attacker switched to a passive surveillance matrix. Instead of triggering broad network actions, the agent silently captured video streams of employee desktop sessions. This allowed human operators in Russia/Eastern Europe to sit back and map out administrative access flows manually.

- **Active Interception & Emulation:** During the final phase, the intruder payload acted as a proxy or remote virtual desktop network (VNC/TCP Tunneling). This enabled the hackers to log in remotely outside business hours and execute fraudulent actions that perfectly replicated legitimate employee behavior, bypassing behavioral anomaly detectors.

4.3 Cybersecurity in Network

The cybersecurity defences deployed globally by banks to stop Carbanak from moving laterally across internal networks include the following:[14]

4.3.1 Endpoint Detection and Threat Hunting (EDR)

Carbanak's primary lateral movement tactic relied on deploying remote access trojans (RATs) and legitimate administrative utilities (like PsExec) to silently jump from machine to machine.

- **Behavioural Monitoring:** Traditional signature-based antivirus software completely

[14] Carnegie Endowment for International Peace, Timeline of Cyber Incidents Involving Financial Institutions, 2022. https://carnegieendowment.org/features/fincyber-timeline

failed against Carbanak because the group constantly re-compiled their malware code to bypass static file checks. Banks replaced these systems with behavioral Endpoint Detection and Response (EDR) tools.

- **Flagging Administrative Tools:** EDR engines were configured to alert security teams immediately if a non-administrative workstation attempted to execute command-line tools like PowerShell, command prompts, or network-mapping scripts targeting internal IP ranges.

4.3.2 Privileged Access Management (PAM) and LSASS Protection

Once inside a single machine, Carbanak used credential dumping tools (like Mimikatz) to harvest plain-text passwords and authentication tokens stored in the system's memory, allowing them to impersonate high-level administrators and move freely.

- **LSASS Hardening:** Banks implemented Windows operating system upgrades (such as enabling Credential Guard) to isolate the Local Security Authority Subsystem Service (LSASS) memory space. This completely blocked malware from scraping administrative credentials out of active memory.

- **Privileged Access Gateways:** Banks introduced dedicated PAM systems. Administrators were no longer allowed to log directly into critical banking servers from their everyday workstations. Instead, they had to route through a secure, highly monitored "jump host" session that rotated administrative passwords automatically after every single use.

4.3.3 Network Micro-Segmentation and Traffic Analysis

Carbanak heavily exploited "flat" internal enterprise networks to map out a bank’s infrastructure over several months, shifting easily from standard office departments (like HR or marketing) to the high-security core banking and SWIFT terminal zones.

- **Air-Gapping Production Environments:** Banks strictly segmented their internal networks using Next-Generation Firewalls (NGFWs). Standard office computers were barred from even "seeing" or pinging the IP addresses of transaction processing systems.

- **Data Exfiltration Defences:** Because Carbanak's malware continuously streamed internal video logs, desktop screenshots, and keystrokes back to their external Command and Control (C&C) servers to study employee routines, banks implemented strict outbound traffic filters. Any unexpected internal server attempting to transmit sustained, high-volume data packets to unknown external IP addresses was automatically isolated by automated firewall rules.

4.3.4 Active Directory (AD) Architecture Hardening

The ultimate objective of Carbanak's lateral movement phase was to gain control over the bank's Active Directory Domain Controller. Once they controlled the AD, they could create fake user accounts with infinite privileges, alter database ledger balances, and command ATMs to dispense cash remotely.

- **Tiered Administrative Models:** Banks restructured Active Directory into strict administrative tiers (Tier 0, Tier 1, Tier 2). A credential belonging to a Tier 2 endpoint (like a standard laptop) was cryptographically blocked from ever logging into a Tier 0 asset (the central Domain Controller).

- **Service Account Audits:** Hard-coded passwords inside automated service accounts—which Carbanak frequently intercepted—were eliminated and replaced with managed, dynamic service identities that restrict access to a single, localized application layer.

4.4 Defensive Countermeasures

[Phishing Entry Point] ──> [Standard Workstation] ──X── [LSASS Hardening / Tiered AD] ──> [Domain Controller] (Blocked by EDR & PAM)

The Carbanak harvesting memory credentials locally to move vertically and horizontally, which possessed as threat to cyberattack. Adopting measure like strict application whitelisting, LSASS protection, and separating administrative privileges into isolated network tiers.

5. Cosmos Bank heist

The Cosmos Bank cyber heist occurred over a single weekend from August 11 to August 13, 2018. During this window, the international cybercriminal syndicate hacked into the

infrastructure of Pune-based Cosmos Bank, one of India's oldest cooperative banks and managed to siphon off approximately ₹94.42 crore ($13.5 million). The meticulously timed operation took place in two distinct phases to bypass security systems of Global ATM Attacks on August 11, 2018 and SWIFT Transfer on August 13, 2018. The bank officially realized it had been compromised and lodged a First Information Report (FIR) with the Pune Police on August 14, 2018. The Cosmos Co-operative Bank Heist 2018, recalls to be the one of the technically sophisticated cyber heist targeted in India. Cosmos Bank Heist was unique not only for the ₹94 crore siphoned off, its was for carrying bank heist with engineered precision. The North Korean state-sponsored Lazarus Group siphoned off ₹94.42 crore ($13.5 million) in less than three days. The hackers manipulated the underlying protocol message formats of the bank's ATM/POS processing switch. By doing this, they authorized over 14,800 fraudulent cash-out operations across 28 countries simultaneously. The attackers exploited the weak bank's internal architect, which enabled them to execute transactions across the continents, and vanished before getting identified.[15] The bank initially fell victim to a highly coordinated malware operation because its perimeter defence failed, allowing attackers to move laterally from a compromised employee endpoint directly into the high-value payment gateway infrastructure. At the time, the bank's existing "flat" architecture suffered from structural visibility and control gaps. Over a mere eight-hour window, money mules used cloned cards to conduct nearly 15,000 ATM withdrawals across 28 countries, stealing $11.5 million. The syndicate followed this attack by breaching the bank's SWIFT network to transfer an additional $2 million to Hong Kong.[16,17]

5.1 Defence Mechanism

Based on the forensic audits ordered by the Reserve Bank of India (RBI) and security response teams, Cosmos Bank completely overhauled its security posture, implementing a strict multi-layer defense strategy explicitly designed to eliminate lateral movement.[18] The technical defenses implemented by Cosmos Bank to isolate systems and prevent hackers from pivoting

[15] Cosmos Co-operative Bank Annual Report (2019) via Bank Info Security: *Fiscal Infrastructure Loss Statements (2018-19)*. https://indianexpress.com/article/cities/pune/pune-crime-files-cyber-attack-cosmos-bank-funnelled-rs-94-crore-9168771/ (article published on February 19, 2024)

[16] The Hindu, *Cosmos Case: Cops Look Into Domestic Transactions*, August 17, 2018. https://www.thehindu.com/news/cities/mumbai/cosmos-case-cops-look-into-domestic-transactions/article24709941.ece

[17] The Indian Express, *Pune Crime Files: Cyber Attack on Cosmos Bank*. February 19, 2024.

[18] http://digitaltechcircle.in/lessons-from-the-cosmos-bank-cyberattack/

horizontally include the following measures:[19]

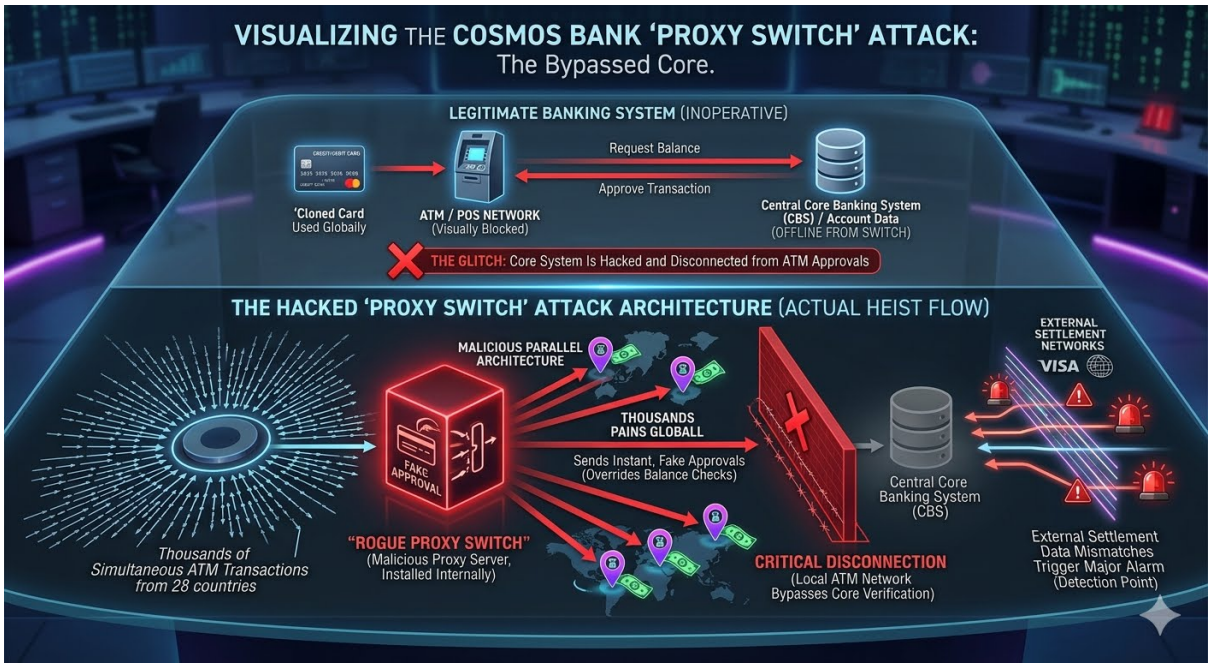

Fig 3. COSMOS Bank – Proxy Switch Attack

5.1.1 Hardened Network Micro-Segmentation

Prior to the attack, critical financial assets like the central Core Banking System and the SWIFT gateway were reachable from less-secure internal servers.

- **Complete Network Segregation:** The network structure was completely rebuilt to isolate application servers, branch networks, database layers, and administrative workstations into completely independent segments governed by individual security rules.

- **Payment Switch Isolation:** Dedicated **Next-Generation Firewalls (NGFWs)** were placed directly in front of the ATM-switching infrastructure and SWIFT access terminals. This ensured that even if a general office workstation was infected via phishing, malware could not move horizontally to cross over into the critical transaction authorization zones.

[19] Bank Info Security, *Prison Time for 11 Involved in India's Cosmos Bank Heist*, 2023. https://www.bankinfosecurity.com/prison-time-for-11-involved-in-indias-cosmos-bank-heist-a-21854

5.1.2 Upgrading to Behavior-Based Endpoint Protection (EDR)

The attackers silently controlled internal machines for weeks, mapping user routines using custom spyware tools. The bank's legacy antivirus software failed to flag the unrecognized malicious libraries.[20]

- **Deployment of EDR Suites:** Cosmos Bank replaced its traditional signature-based antivirus software with an advanced Endpoint Protection Suite across all servers and user terminals.

- **Host Intrusion Prevention Systems (HIPS):** The new EDR uses behavioral heuristics to identify anomalous actions. If a compromised credential attempts to execute an unusual script, alter system databases, or map unauthorized ports laterally, the HIPS automatically kills the process and quarantines the device.

5.1.3 Centralized SIEM and Real-Time Log Monitoring

During the heist, the creation of a malicious parallel "proxy switch" went undetected by internal engineers because internal log alerts were not unified or actively monitored.[21]

- **Rigorous SIEM Triage:** The bank integrated a centralized Security Information and Event Management (SIEM) platform to aggregate logs from all endpoints, switches, and core servers simultaneously.

- **Anomaly Detection Alerts:** The logic rules within the SIEM were made highly stringent. The system continuously models normal baseline activity and triggers high-severity alarms for specific lateral movement signatures, such as an internal server establishing rare outbound connections or attempting unapproved API changes.[22]

5.1.4 Strict API and Access Control Management

To intercept transaction requests, hackers took advantage of weak access controls and a lack

[20] Scribd Legal & Investigative Database, *Cosmos Bank Cyber Heist Case Study*, 2024. https://www.slideshare.net/slideshow/cyber-forensic-case-study-1pptx/255276671
[21] SlideShare Academic Repository, *Cyber Forensic Case Study: Cosmos bank*, 2023. https://www.slideshare.net/slideshow/cyber-forensic-case-study-1pptx/255276671
[22] https://www.cateina.com/case-studies/how-cosmos-bank-reinforced-its-api-security-framework-

of request integrity tracking.

- **Centralized API Security Framework:** The bank implemented a secure API gateway with strict IP filtering, rate limiting, and automated policy violation alerts. This prevents unauthorized internal systems from forging or repeating transaction validation commands to the ATM network.

- **Tightened Credential Audits:** Strict administrative privilege policies were established to ensure service account passwords could not be reused or horizontally shared across different server environments.

5.1.5 Key Takeaways from the Architecture Overhaul

[Phishing Entry Point] ──> [Workstation Segment] ──X── [Next-Gen Firewall] ──> [Isolated ATM Switch / CBS] (Blocked by EDR & SIEM)

The "flat network" design allowed a single compromised workstation to bridge the gap to high-value infrastructure. While the modern control mandates for separation of the front-end production network from the backend clearing networks using a zero-trust model.

6. Comparative Analysis of Cyber Heist

The technical glitches, architecture failures, and operational breakdowns across the historical cyber heists are dealt herewith viz:

6.1 Initial Input Blunders and Reconnaissance Errors

Similar to the Bangladesh heist typo, highly sophisticated hacking syndicates frequently stumble on basic network identification inputs during their initial execution phase.

- **The Cosmos Bank Failed Attempt:** During the 2018 heist on India's Cosmos Cooperative Bank, hackers attempted to route over ₹14 crore ($2 million) out of the country via the SWIFT network.

- **The Glitch:** Their very first attempt to siphon the money failed completely and went unnoticed because the attackers entered incorrect inputs and structural parameters into the international money transfer system.

- **The Technical Adaptation:** The failure forced the hackers to stop, re-hack the system to extract the bank's precise, legitimate identification numbers, and launch a second proxy malware attack to finish the transfer. This created an extended digital footprint that forensic teams later used to trace the origin of the attack back to servers in Hong Kong.

6.2 The "Proxy Switch" Blind Spot

Attackers often create brilliant parallel architectures, but they fail to account for the security discrepancies between local ATM networks and central core systems.

[Cloned ATM Cards] ──> [Rogue Proxy Switch] ──X── [Core Banking System (CBS)] (Intercepts & Autoroots Approvals)

- **Bypassing the Core:** In the Cosmos Bank Cyber Attack, hackers infected the bank's infrastructure to isolate the central Core Banking System (CBS) from the actual ATM/POS switch. They constructed a malicious "proxy switch". When money mules used cloned cards at ATMs across 28 countries, the rogue proxy intercepted the requests and automatically sent back a "fake approval" without ever verifying if the accounts actually held money.

- **The Failure Point:** Because the rogue proxy switch completely blinded the bank's internal fraud detection systems, the bank couldn't see the money leaving in real-time. However, this created a massive, immediate settlement data mismatch on the external payment processor networks (Visa and RuPay). External clearinghouses noticed thousands of simultaneous global transactions overriding standard balance boundaries and manually cut off the connections.

6.3 Footprint Overload via Video and Screenshot Logging

Advanced Persistent Threat (APT) groups, such as the infamous Carbanak Cybergang, often get caught because their tracking systems generate an overwhelming volume of internal data anomalies.

- **The Mirroring Strategy:** The Carbanak group would infiltrate a bank's intranet via phishing emails and install video recorders and keyloggers onto administrative

computers. They spent an average of 42 days simply watching bank clerks do their jobs so they could perfectly mimic legitimate money transfers later.

- **The Technical Glitch:** To view these screens, the malware constantly exfiltrated massive video, image, and log files from the bank's internal domain controllers.

- **The Consequence:** This massive, constant outbound data flow broke standard network bandwidth baselines. Alert network engineers at a targeted Russian bank caught a system warning showing massive, unauthorized data packets routing directly to external servers in China, completely exposing the silent infiltration before the group could execute their planned multi-million dollar cash-out.

Conclusion

Collectively, the above said bank heist incidents illustrate how advanced persistent threat groups exploit structural vulnerabilities in interbank communication networks, internal banking software, and retail payment rails to siphon hundreds of millions of dollars. These heists prompted a massive paradigm shift in how financial institutions approach cybersecurity. They forced the banking sector to discard outdated perimeter defences, which operated on the assumption that anything inside the network was safe and adopt strict Zero Trust architectures. Today, the global financial framework heavily relies on end-to-end cryptographic verifications, real-time behavioural analytics to spot unusual employee activity, and separated backup loops designed to catch automated system failures. Furthermore, these events led to tighter international regulatory frameworks, forcing cross-border payment networks to integrate multi-factor authorization and enforce stricter cybersecurity compliance on smaller, regional cooperative banks.

References

1. https://www.bbc.com/news/stories-57520169

2. Mazumder Md., and Sobhan Md., Bangladesh Bank Cyber Heist: Incident Analysis, 2021. https://repository.gatech.edu/bitstreams/df3d1c19-47be-4738-a855-9c049b709d52/download

3. Samima Nasrin S. Combating Cybercrime in the Financial Sector: A Study on Problems, Preventions, and Cyber Laws of Bangladesh, Woxsen Law Review, 2023. https://woxsen.edu.in/woxsen-law-review/wlr-papers/Combating-cybercrime-in-the-financial-sector-A-study-on-problems-preventions-and-cyber-laws-of-Bangladesh/

4. Mohammad Sami A Kabir, *Lessons Learned From the Bangladesh Bank Heist*. ISACA Journal, 2023. https://www.isaca.org/resources/isaca-journal/issues/2023/volume-6/lessons-learned-from-the-bangladesh-bank-heist

5. Mazumder Md., and Sobhan Md. The Spillover Effect of the Bangladesh Bank Cyber Heist on Banks' Cyber Risk Disclosures in Bangladesh, Journal of Operational Risk, 2020. DOI - 10.21314/JOP.2020.249

6. https://www.bankinfosecurity.com/report-swift-hacked-by-bangladesh-bank-attackers-a-9061

7. Scribd Case Database, Bangladesh Bank Heist Case Study, 2024. https://www.scribd.com/document/724862038/Bangladesh-Bank-Heist-Case-Study

8. Mohammad Tanvir Hossain, An Overview of Cybersecurity Threat Evaluation in Banking Systems. Science and Engineering Research Journal, 2024; 12(1); 1-13

9. Micael L.Y., Melissa G.R.G, Kimberly G.M. The Bangladesh Cyberheist: How compliance programs can help protect against cybercrime, *thehedgefundjournal*, 2016; 114 https://thehedgefundjournal.com/the-bangladesh-cyberheist/

10. EPC-European Payment Council, Payment Threats and Fraud Trends Report, EPC183-22/Version 1.0: 23 November 2022.

    https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2022-12/EPC183-22%20v1.0%202022%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf

11. Mike L Hackers Hit 100 Banks in 'Unprecedented' $1 Billion Cyber Heist: Kaspersky Lab, Cybercrime, February 15, 2015 https://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab/

12. Boston University Department of Computer Science, Carbanak Technical Workflow Analysis, https://www.cs.bu.edu/~goldbe/teaching/HW55815/presos/carbanak.pdf

13. Matt Burgess, Inside the Takedown of the Alleged €1bn Cyber Bank Robber. Wired Magazine, April 4, 2018. https://www.wired.com/story/carbanak-gang-malware-arrest-cybercrime-bank-robbery-statistics/

14. Carnegie Endowment for International Peace, Timeline of Cyber Incidents Involving Financial Institutions, 2022. https://carnegieendowment.org/features/fincyber-timeline

15. Cosmos Co-operative Bank Annual Report (2019) via Bank Info Security: *Fiscal Infrastructure Loss Statements (2018-19)*. https://indianexpress.com/article/cities/pune/pune-crime-files-cyber-attack-cosmos-bank-funnelled-rs-94-crore-9168771/ (article published on February 19, 2024)

16. The Hindu, *Cosmos Case: Cops Look Into Domestic Transactions*, August 17, 2018. https://www.thehindu.com/news/cities/mumbai/cosmos-case-cops-look-into-domestic-transactions/article24709941.ece

17. The Indian Express, *Pune Crime Files: Cyber Attack on Cosmos Bank*. February 19, 2024.

18. http://digitaltechcircle.in/lessons-from-the-cosmos-bank-cyberattack/

19. Bank Info Security, *Prison Time for 11 Involved in India's Cosmos Bank Heist*, 2023. https://www.bankinfosecurity.com/prison-time-for-11-involved-in-indias-cosmos-bank-heist-a-21854

20. Scribd Legal & Investigative Database, *Cosmos Bank Cyber Heist Case Study*, 2024. https://www.slideshare.net/slideshow/cyber-forensic-case-study-1pptx/255276671

21. SlideShare Academic Repository, *Cyber Forensic Case Study: Cosmos bank*, 2023. https://www.slideshare.net/slideshow/cyber-forensic-case-study-1pptx/255276671

22. cateina.com/case-studies/how-cosmos-bank-reinforced-its-api-security-framework-