Payatu

Payatu Case Study

The Great Breach – A Full-Scope Red Team Assessment of a Financial Institution

Payatu Security Consulting Pvt. Ltd

Company Profile

For any major financial services company that handles the investments of millions of retail customers, a weak cybersecurity posture can have catastrophic consequences, such as regulatory penalties, loss of customer trust, market manipulation risk, and operational disruption that can take years to recover from.

This is why a leading financial services institution, one of India's largest broking and capital markets organisations, managing retail, institutional, and corporate clients across equities, derivatives, mutual funds, and investment banking, hired Payatu for an end-to-end red team assessment.

The client was clear about what it wanted: a rigorous, real-world test of its digital and physical defences, conducted from a fully external, black-box perspective. Every piece of information held by the organisation, digitally and physically, was considered sensitive and confidential. The best way to protect that information was to find out, first, how an attacker could get to it.

The engagement also had an internal purpose. The organisation wanted concrete findings, the kind that would be backed by real evidence. They didn't just want a report. They wanted proof that their defences could or couldn't hold.

And so Payatu's team set to work, rigorously challenging the client's systems, infrastructure, and physical premises from a fully adversarial perspective.

What followed was a complete compromise, domain administrator access achieved, two office locations physically breached, critical assets physically removed from the building, and sensitive customer data exfiltrated without triggering a timely SOC response. While some detections were logged, response actions came too late to prevent the attack chain from progressing.

The Rules of Engagement

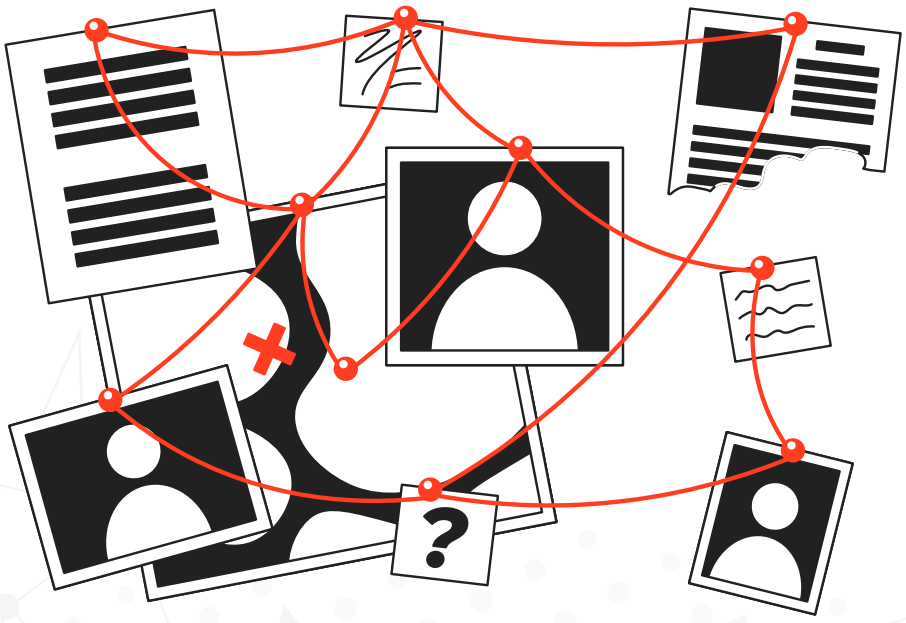
The team was given two targets: the corporate broking entity and the consumer-facing direct trading organization.

No Denial of Service. No zero-days.

Everything else? Fair game.

The engagement was conducted as a fully black-box exercise where the Bandits were given no prior knowledge of the client's internal systems, architecture, or credentials.

Basically, start from the outside and go as deep as possible.



In Scope

- Corporate broking entity (external and internal assets)
- Consumer-facing direct trading entity
- External asset mapping and reconnaissance
- Social engineering, phishing, and vishing campaigns
- Malware development and endpoint evasion
- Lateral movement and privilege escalation
- On-premises Active Directory domain compromise
- Cross-forest Active Directory lateral movement
- Physical intrusion testing across two locations
- Data exfiltration simulation with TTD/TTR measurement

The Attack:
A Week-by-Week Account

1. WATCHING FROM THE OUTSIDE

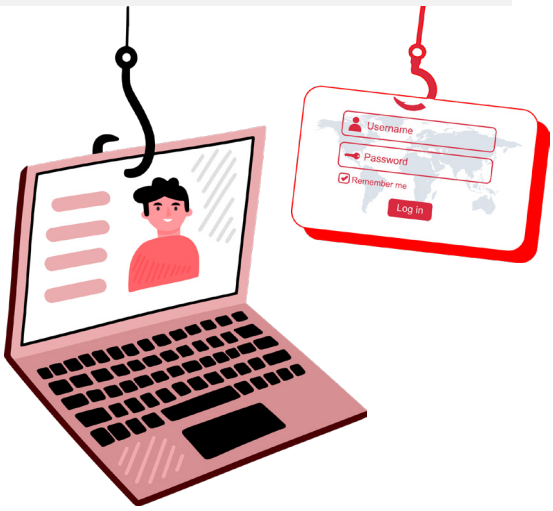
> *"Before you attack, you listen, you map. You learn everything there is to know about your target without them ever knowing you exist."*

The team started exactly the way a real adversary would, quietly. Open-source intelligence, DNS records, subdomain enumeration, certificate transparency logs, LinkedIn profiles, job postings - every public-facing service, API, and cloud asset catalogued and probed.

An external asset map took shape. Internet-facing databases, misconfigured services, employee email formats, org chart clues buried in public posts. The target didn't know they were already being studied.

2. THE FIRST KNOCK ON THE DOOR

> *"Getting phishing emails into the inbox of a major financial institution is not easy. It took multiple attempts, careful infrastructure setup, and a lot of patience."*



The First Challenge:

The organisation's email security gateway was doing its job. Phishing emails were being blocked. The team had to tune their sending infrastructure by rotating domains, adjusting configurations, warming up mail servers, before delivery into target inboxes became reliable.

Once the door cracked open, the team ran three distinct campaign types against employees in sensitive departments:

Credential Harvesting: Employees were directed to convincing spoofed login pages to capture their usernames, passwords and session cookies enabling access to compromised employee account without MFA.

Token Harvesting: Targeted phishing and vishing attacks against sensitive departments obtained Microsoft Azure tokens, enabling stealthy access and persistence without requiring a password or MFA.

Malware Delivery: Phishing emails carried payloads designed to establish a foothold on employee endpoints, feeding directly into the next phase of the attack chain.

Access to internal email, Microsoft Teams conversations, and high-value communications followed. One of the main objectives, insider threat simulation, was already done.

3. THE WALL THAT KEPT GETTING REBUILT

> *"Their EDR was genuinely good. It blocked us. Twice. Then a third time. So we stopped playing their game and started playing ours."*

The organisation had deployed one of the most capable Endpoint Detection & Response solutions on the market, reinforced by an Endpoint Privilege Management (EPM) layer that allowed only whitelisted software to execute. The first malware campaign was blocked immediately. The second was also caught.

A third variant failed. Most teams would have stopped here.

Instead, the Bandits went back to their first principles. They knew that signed applications- applications the operating system and EDR implicitly trust, represent a blind spot in most detection coverage. Microsoft Teams runs as a trusted Electron application on every Windows machine in the organisation. What if Teams itself delivered the payload?

Campaign 4: a backdoored Microsoft Teams build. The EDR saw a signed, trusted process. It raised no alert. The team now had a reliable foothold inside the network, with access to two employee workstations.

The organisation's best security tool was defeated not by guessing or using generic techniques, but by crafting targeted attack chains and by creativity.

4. THE DATA WAS ALWAYS THERE

> *"A database reachable from the internet. Server admin credentials hardcoded in a configuration file. Customer PII, one config read away. It took minutes to find."*

While the digital engagement progressed internally, the team identified something alarming on the external attack surface: a publicly reachable database. While the database required credentials to access, server administrator credentials had been hardcoded in a configuration file, making them trivial to discover. Once retrieved, the team had direct, authenticated access to customer personally identifiable information.

Inside the network, internal portals were accessed using compromised credentials and an OTP bypass technique. Sensitive Outlook and Teams communications of high-profile targets were read. And when the time came to exfiltrate data, the team used something already on the corporate laptop - and data was transferred out.

The SOC didn't fire a single timely alert.
The next objective of undetected exfiltration was confirmed.

5. THE PHYSICAL WORLD HAS NO PATCH

> *"We walked into their office, smiled at the security guard, connected a device to their internal network, and walked out with a critical device under our arm. Nobody asked a single question."*

Physical assessments were conducted at two India office locations. The team dressed in formal attire similar to the client's employees and arrived carrying fabricated employee ID cards, indistinguishable at a glance from the real thing.

At Location A, the security guard was doing his job. The RFID tap was required, and the right questions were asked. The team explained they were employees from another branch attending a meeting. When the guard noted the ID card wouldn't tap correctly, they said they'd need a new one made. He directed them to the cafeteria floor which was accessible without RFID. One unsecured cafeteria entry point was all it took.

At Location B, there were no meaningful controls. The team gained entry by tailgating employees through the entrance. An employee RFID card was procured through social engineering. Using it, the team moved freely through internal areas. An unauthorised external device was plugged into the internal network which bridged directly to the Active Directory environment. A critical device was picked up and walked out of the building.

The employee whose device was taken never reported it missing. The employee whose RFID card was taken only realised it was gone when they needed it to leave the office at the end of the day, and it was never formally reported as a security incident. In a real attack, that's weeks of undetected access from a physical device, inside the network perimeter, with domain credentials already in hand.

The most sophisticated endpoint security in the world cannot protect you from someone who is already sitting inside your office.

6. INSIDE THE NETWORK

> *"We didn't need to hack the Wi-Fi. We already had the password."*

Using credentials obtained through phishing, the team connected directly to the organisation's internal corporate Wi-Fi. No brute force. No sophisticated network attack. Just a username, a password, and an open connection to the internal network.

To get to that point, the team had already made their first physical visit to the premises, scoping entry points, observing employee movement patterns, and identifying how staff accessed the building. That groundwork made the subsequent physical breach significantly easier.

From inside the network, the team could see internal portals, communications infrastructure, and the beginnings of the Active Directory environment. The perimeter, in the traditional sense, no longer existed.

7. THE KEYS TO THE KINGDOM

> *"Once you're inside Active Directory, you're not just inside one system. You're inside all of them."*

From the compromised endpoints, the team pivoted into the on-premises Active Directory environment. A Kerberoasting attack pulled service account ticket hashes from the domain. Offline cracking recovered plaintext credentials.

Then came the decisive blow: **a misconfigured Certificate Authority template**. The team was able to escalate from a standard employee account to Domain Administrator.

Not content with domain admin, the team went further, adding a newly created account to the Enterprise Admins group, achieving full forest-level control. A cross-forest trust relationship was then exploited to pivot into a secondary Active Directory forest, where a privileged group access was obtained with a clear pathway to full Domain Admin on that forest too.

Two more objectives, **Domain Administrator access** and the **secondary forest escalation** were achieved.

Objectives:
How Did They Score?

Seven primary objectives were defined before the engagement began. All were either fully or partially achieved.

SR. NO	OBJECTIVE	STATUS
1	Gain Domain Administrator access within the Active Directory environment.	**Achieved**
2	Break physical perimeter security and establish internal network access by posing as a legitimate employee.	**Achieved**
3	Compromise a standard employee account through social engineering and reach internal systems simulating an insider-threat scenario.	**Achieved**
4	Execute lateral movement and privilege escalation from a low-privilege user to administrative access on at least one internal system.	**Partial**
5	Deploy and execute a custom malware payload on an internal endpoint to bypass antivirus/EDR controls.	**Achieved**
6	Exfiltrate a controlled set of sensitive data without triggering timely SOC alerts measuring Time to Detection and Time to Response.	**Achieved**
7	Identify and exploit exposed external assets, services, APIs, or cloud misconfigurations to gain initial unauthorised access.	**Achieved**

What Was Found:
23 Findings Across the Attack

6	7	3	2
CRITICAL	HIGH	MEDIUM	LOW

FINDING	CATEGORY	ATTACK VECTORS	SEVERITY
C2 Malware Delivery	Digital	Targeted delivery of C2 malware on systems to gain initial access to the internal networks.	CRITICAL
Microsoft Azure Tokens - Phishing	Digital	Targeted phishing and vishing attacks against sensitive departments to obtain Azure tokens, enabling stealthy access and persistence.	CRITICAL
Credential Phishing	Digital	Advanced phishing techniques deployed to bypass existing network filters with the goal of obtaining employee credentials.	CRITICAL
Domain Privilege Escalation	Digital	Privilege Escalation from low-privilege domain users to Domain Administrator via exploitation of misconfigured CA Certificate Template.	CRITICAL
Customer Data Leakage Via Database Compromise	Digital	Unauthorized access to a publicly reachable database containing customer PII data.	CRITICAL

FINDING	CATEGORY	ATTACK VECTORS	SEVERITY
Physical Infrastructure Perimeter Security	Physical	Physical access to restricted premises enabling direct tampering with systems and network devices, leading to the extraction of sensitive information.	**CRITICAL**
Unauthenticated Employee Data Leakage from External Portal	Digital	Unauthenticated endpoint leading to employee PII data disclosure.	**HIGH**
Privilege Escalation - Domain Administrator to Enterprise Administrator	Digital	Privilege escalation by adding a newly created Domain Admin account to the Enterprise Admins group, enabling full forest-level control.	**HIGH**
Kerberoasting Attack Leading to Account Compromise	Digital	Abuse of Kerberos service account authentication by requesting service tickets (TGS) and offline cracking them to recover service account credentials.	**HIGH**
Absence Of MFA on Sensitive External Portal	Digital	Unauthorized access to sensitive portal obtained via compromised credentials.	**HIGH**
Cross-Forest Lateral Movement Via Trust Account Abuse	Digital	Exploitation of Cross-Forest Trust to Pivot towards the internal forest.	**HIGH**
Social Engineering	Physical	Convinced employees via a fabricated pretext, enabling the team to exfiltrate a device and an employee RFID card.	**HIGH**

FINDING	CATEGORY	ATTACK VECTORS	SEVERITY
Internal Network Access Obtained Via External Device	Physical	Post physical breach, obtain access to internal network and On-Premises Active Directory by connecting external device to Wi-Fi.	**HIGH**
Internal Portal Access Via OTP Bypass	Digital	Access internal portal using compromised credentials and OTP bypass.	**MEDIUM**
Unauthorized Data Exfiltration via Corporate Asset	Digital	Leveraging native Python utilities on a corporate system to host a temporary HTTP server, enabling direct exfiltration of sensitive data from the internal environment to an external system.	**MEDIUM**
Weak Domain Passwords in Use	Digital	Conduct Offline Password Cracking on Recovered NTLM Hashes to Recover Plaintext Passwords.	**MEDIUM**
Sensitive Business Data Found in Compromised User Mails	Digital	Unauthorized access to high profile target Outlook and Teams communications enabled sensitive business data compromise.	**LOW**
Employee ID Enumeration	Digital	Enumeration of Employee ID conducted Via Teams and the web portal	**LOW**

What This Means for the Business

These findings are not theoretical. Every attack path demonstrated by the red team represents a scenario that a real adversary, whether a nation-state actor, a financially motivated criminal group, or a malicious insider could execute. The business consequences are material.

Regulatory Penalties & Mandatory Disclosure

Unauthorised access to customer PII, including from a publicly exposed database, triggers mandatory breach notification obligations under applicable data protection and financial services regulations. Fines, audits, and enforcement action follow.

Financial Fraud & Market Integrity Risk

Access to transaction data, research documents, and internal financial communications creates direct pathways for financial fraud, market manipulation, and insider trading facilitation with potential for irreversible monetary loss and regulatory sanction.

Customer & Brand Trust Erosion

A data breach or service disruption at a retail brokerage touches millions of individual investors. The reputational damage from a confirmed breach, especially one involving customer PII or trading data, can take years to recover from.

Extended Attacker Dwell Time

The SOC did not detect any phase of the attack in a timely manner. In a real-world scenario, an adversary with weeks of undetected access can cause damage that is orders of magnitude more severe than a quickly detected intrusion.

Operational Disruption

Domain-level compromise, physical device implantation, and the demonstrated potential for malware deployment mean that a motivated attacker could cause service outages affecting retail trading operations with direct financial and legal consequences.

Competitive Intelligence Leakage

Access to internal research, M&A advisory materials, and strategic planning data represents intellectual property that, in the wrong hands, could compromise client confidentiality, contravene market regulations, and erode competitive advantage.

Before VS After

AREA	BEFORE	AFTER
Customer Data Exposure	Customer PII accessible from a public-facing database; login was required, but server admin credentials were hardcoded in a configuration file	Database taken offline; external asset inventory initiated
Office Security	Both offices were physically breached, critical device was stolen, a rogue device was planted, and, an RFID was cloned	Physical access gaps closed; RFID and visitor controls overhauled
Wi-Fi Access	Internal network reachable using phished Wi-Fi credentials; also accessible via an unauthorised external device connected during the physical breach	Credentials rotated; network access controls tightened
Identity & Domain Control	One misconfigured certificate template allowed full takeover of all user accounts and systems	CA template patched; Domain Admin and Enterprise Admin access hardened

AREA	BEFORE	AFTER
SOC Visibility	Multiple attack stages, including data exfiltration completed with no timely alert raised	Detection playbooks, alerting rules, and TTD/TTR baselines under review
Employee Awareness	Phishing, vishing, and physical pretexts all succeeded; staff did not report stolen assets	Security awareness training and mandatory incident reporting protocols recommended

The End - And What Comes Next

> *"Every objective was met. The client was happy. Their security team finally had the evidence they needed."*

At the close of the engagement, the red team presented their findings.

The client received formal appreciation from their own security leadership. Not because the team had found weaknesses, but because, for the first time, those weaknesses were visible, evidenced, and actionable.

At a Glance

OBJECTIVES MET

7/7

All Primary Goals Achieved

CRITICAL FINDINGS

6

Require Immediate Action

HIGH FINDINGS

7

Significant Risk Exposure

TOTAL FINDINGS

23

Across Digital & Physical

SOC DETECTION

9%

Total Attacks Detected: 9/100

Full Domain Compromise

Both Offices Breached

Data Exfiltrated Undetected

Client Objective Achieved

About Payatu

Payatu is a Research-powered cybersecurity services and training company specialized in IoT, Embedded Web, Mobile, Cloud, & Infrastructure security assessments with a proven track record of securing software, hardware and infrastructure for customers across 20+ countries.

Red Team Assessment

Red Team Assessment is a goal-directed, multidimensional & malicious threat emulation. Payatu uses offensive tactics, techniques, and procedures to access an organization's crown jewels and test its readiness to detect and withstand a targeted attack.

Mobile Security Testing

Detect complex vulnerabilities & security loopholes. Guard your mobile application and user's data against cyberattacks, by having Payatu test the security of your mobile application.

Web Security Testing

Internet attackers are everywhere. Sometimes they are evident. Many times, they are undetectable. Their motive is to attack web applications every day, stealing personal information and user data. With Payatu, you can spot complex vulnerabilities that are easy to miss and guard your website and user's data against cyberattacks.

Product Security

Save time while still delivering a secure end-product with Payatu. Make sure that each component maintains a uniform level of security so that all the components "fit" together in your mega-product.

IoT Security Testing

IoT product security assessment is a complete security audit of embedded systems, network services, applications and firmware. Payatu uses its expertise in this domain to detect complex vulnerabilities & security loopholes to guard your IoT products against cyberattacks.

Payatu

AI / ML Security Audit

Incorrectly implemented AI/ML systems can lead to security and privacy issues. The severity of which depends on how critical the use case is. The repercussions of the same include misclassification of unauthorized entities, theft of intellectual property such as application train models, etc. With a dedicated team capable of effectively assessing and strengthening AI/ML systems, we can provide specific methods to prevent potentially damaging threats before they potentially derail your project.

Cloud Security Assessment

As long as cloud servers live on, the need to protect them will not diminish. Both cloud providers and users have a shared. As long as cloud servers live on, the need to protect them will not diminish.
Both cloud providers and users have a shared responsibility to secure the information stored in their cloud Payatu's expertise in cloud protection helps you with the same. Its layered security review enables you to mitigate this by building scalable and secure applications & identifying potential vulnerabilities in your cloud environment.

Code Review

Payatu's Secure Code Review includes inspecting, scanning and evaluating source code for defects and weaknesses. It includes the best secure coding practices that apply security consideration and defend the software from attacks.

Security Operations Center

Cyber threats are everywhere, often operating in the shadows. Their goal: to breach networks, compromise systems, and steal critical data. With Payatu's SOC service, you can uncover these hidden threats, bolster your defenses, and protect your data from relentless cyber attacks.

DevSecOps Consulting

DevSecOps is DevOps done the right way. With security compromises and data breaches happening left, right & center, making security an integral part of the development workflow is more important than ever. With Payatu, you get an insight to security measures that can be taken in integration with the CI/CD pipeline to increase the visibility of security threats.

Critical Infrastructure Assessment

There are various security threats focusing on Critical Infrastructures like Oil and Gas, Chemical Plants, Pharmaceuticals, Electrical Grids, Manufacturing Plants, Transportation systems etc. and can significantly impact your production operations. With Payatu's OT security expertise you can get a thorough ICS Maturity, Risk and Compliance Assessment done to protect your critical infrastructure.

CTI

The area of expertise in the wide arena of cybersecurity that is focused on collecting and analyzing the existing and potential threats is known as Cyber Threat Intelligence or CTI. Clients can benefit from Payatu's CTI by getting – social media monitoring, repository monitoring, darkweb monitoring, mobile app monitoring, domain monitoring, and document sharing platform monitoring done for their brand.

More Services Offered

- Trainings

More Products Offered

- EXPLIoT

Payatu

Payatu Security Consulting Pvt. Ltd.

www.payatu.com

info@payatu.io

+91-20-47248026