Payatu

Payatu Case Study

The Money Heist: A Red Team Assessment of a Financial Services Organization

Payatu Security Consulting Pvt. Ltd.

Project Overview

For any major company that handles people's money, the impact of a weak cybersecurity posture can be drastic!

This is why a **$100 million** revenue-generating financial services company specializing in digital loans, home loans, microloans, mutual funds, and health insurance, hired Payatu for a red team assessment.

This client was extremely clear in its understanding that each piece of information that existed with it, digitally and physically, was of utmost importance and highly confidential. So, the best way to protect this information is to identify ways in which an attacker can gain access to the organization's assets.

The best approach for this client to test its security posture was to have Payatu Bandits rigorously challenge the client's systems and infrastructure, from an antagonistic perspective.

And thus began our Bandits' meticulous execution of a red team assessment for this financial services provider.

Scope

1. **To replicate the type of attacks that could be initiated on the internet on the client's:**
   - → Web Servers and/or Applications (Web/Mobile)
   - → Network
   - → Cloud Assets
2. **To identify vulnerabilities that can be exploited to:**
   - → Gain access to sensitive data such as passwords
   - → Gain access to the internal network
   - → Bypass the security controls implemented
   - → Escalate privileges
   - → Laterally move inside the organization to compromise/gain access to crown jewels
3. **All types of social engineering attacks like phishing and vishing**
4. **To perform physical pentesting on the client's premises in scope to:**
   - → Gain physical access to the client's office
5. **Compromise wireless network(s)**

Process

Reconnaissance - The process started with reconnaissance, to gather information prior to launching an attack. Two types of reconnaissance activities were conducted, namely, active reconnaissance and passive reconnaissance.

- **Active Reconnaissance -** In active reconnaissance, the Bandits interacted directly with the client's infra to collect information that is not easily available by other means.
- **Passive Reconnaissance -** Passive reconnaissance is an attempt to gain information about the organization without actively engaging with the infra.

Initial Compromise - Once the Bandits were done collecting all the information in their reconnaissance phase, they moved on to the next stage i.e., initial compromise. The following social engineering activities were performed in conjunction with each other to steal employees' credentials:

- Phishing email campaigns
- Vishing call campaigns

Establish Persistence - The team then used the stolen credentials to login into different enterprise applications and tried to maintain its access to the same.

Post-Exploitation, Lateral Movement - The team then tried to work towards escalating its access by using the captured credentials followed by exploitation of crown jewels.

Data Exfiltration - Finally, towards the end the Bandits analyzed sensitive data belonging to the client's customers and attempted to exfiltrate it using different channels.

Physical Pentesting

1. The Bandits combed through the client's websites, resources, social media accounts, profiles of employees on social media platforms, and many other pages to catch hold of something that could be of use to them in physical pentesting. This is when they came across an ID card of an employee who had put up a post mentioning the client.

2. This ID was then used to morph pictures of Payatu Bandits and make it look like the IDs belonged to them and that they were a part of the company.

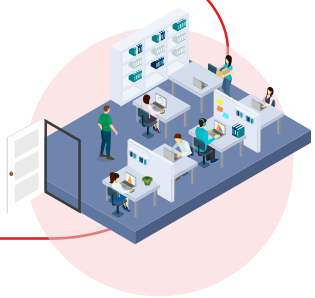
3. These Bandits spent around 2 days just to recon the client's premises and observe how the employees were allowed entry to the premises.

4. Upon arriving at the client's office building, getting in did not prove to be very difficult as the Bandits could easily use the morphed ID cards and pretend to be employees of the client, when stopped by the guard.

5. They were asked if they had an ID and all they had to do was say "yes" and flash it to the guard, post which they were granted the entry.

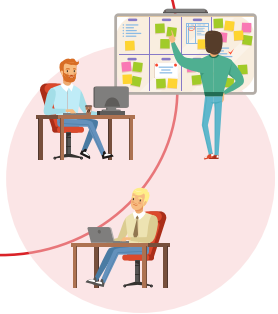
Payatu

6. The Bandits did not even have to tailgate anybody to get inside the office, as the doors were left slightly open.



7. After getting into the office, they took some video POCs and made conversations with a couple of client's employees to avoid raising any suspicion.

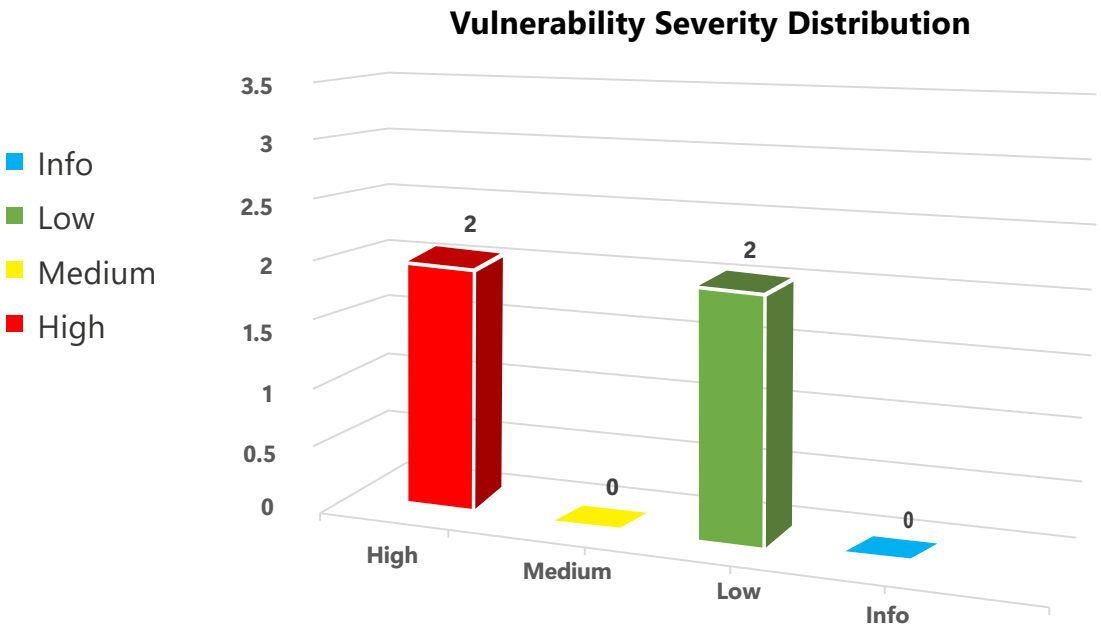
8. Inside the premises, many IPs, passwords, and other information related to network were uncovered, as most of it was readily available on the employees' pinboards, written on sticky notes.



9. To leave the premises, the Bandits (impersonators) tried using the fire exit, where they were stopped by a guard.

10. When inquired about who they were, the Bandits revealed their real names to the guard and mentioned they were visitors from the client's headquarters. This led to the guard calling the headquarters office and confirming if they were actual employees of the organization.

Findings



1. **High Severity Vulnerability -** Phished and vished the client's employees together to steal their credentials and logged in to their Google Workspace accounts.

2. **High Severity Vulnerability -** Impersonated as the client's employees to enter and leave the premises.

3. **Low Severity Vulnerability –** Hardcoded Wireless-Network credentials (for different location), internal portal's credentials, etc.

4. **Low Severity Vulnerability-** Captured WPA-handshake for WPA2-PSK network.

Potential Impacts

TECHNICAL IMPACT	BUSINESS IMPACT
An adversary can perform phishing on employees using a website disguising as a legitimate client's website to steal credentials, ask victims to install ransomware, or perform other malicious activities which can lead to huge financial loss, reputation loss etc.	Organizations risk emerging situations where they face huge financial losses as well as customer trust. In fact, a reputable European bank once lost around **$75.8 million**, as a result of the email account of a high-level executive (CEO) of the bank being compromised.
An adversary can call an employee impersonating as an Information Technology Administrator and ask him/her the 2FA, leading to account takeover. An adversary can call an employee disguising as a job recruiter and ask for details on certain infrastructure-related details in the pretext of getting details from him/her.	Companies can fall prey to several attacks and be at the center of the risk of critical information leaks. According to a report by Statista, vishing attacks have grown from **54% to 71%** in a span of mere two years. The numbers are alarming and so can be, its impact on the business.
An adversary can cause monetary damages by destroying/incapacitating equipment. An adversary can cause severe disruption of services by deployment of malware. An adversary can plant remote devices to maintain persistent network access.	Office premises have tremendous amounts of sensitive information stored while operations take place. Physical threats and disruption to operations can be highly fatal for any organization. During a Presidential Election in the USA, certain supporters stormed into the U.S. Capitol building, giving attackers access to individual chambers and offices, every device, computer, server, network outlet, Wi-Fi hotspot, router, and internet connection in the Capitol. When critical premises such as the Capitol even are not safe from physical break-ins, organizations need to take a serious look at their own physical security measures.
An adversary can capture the wireless handshake and try to brute-force to retrieve the password.	A report from Cisco states that cyberattacks are costing **71%** of surveyed businesses over **$100,000** a year, with 41% claiming their total damages exceed half a million dollars for the same period.

Challenges

01 Port and vulnerability scanning on Network IPs did not reveal any running vulnerable service that can be exploited to gain privileged access

02 Since the domain name used by the client was previously registered by another organization, it became difficult to identify the actual assets that belonged to the client

03 Some wireless access points at the client's physical location had MFP enabled, making things a little more complicated than expected

04 Due to time constraints, fully simulating an attacker's persistence and patience proved to be challenging

05 No success on initial phishing campaigns due to presence of email security device

Recommendations

Employees should be given awareness training on:

01 Social engineering attacks

02 Not sharing sensitive information such as passwords, 2FA over a voice call

03 Not agreeing to any instructions provided over voice calls, when the credibility of source cannot be confirmed

04 Not sharing any information/details such as ID card, employee ID, etc., on social platforms.

Use FIDO keys instead of traditional TOTP or SMS-based 2FA.

Implement access control policies throughout the organization.

The use of biometrics, access cards or both should be implemented for sensitive zones/areas.

Only authorized people should be allowed inside the premises after identifying and validating them.

Security personnel should ensure that there should be no tailgating or piggybacking.

Avoid leaving unattended documents/whiteboard that can disclose sensitive information such as network architecture, passwords, etc.

Implement practice of using one time password sharing throughout the organization instead of hardcoding credentials or sharing them in plain text over chat, emails etc.

Management Frame Protection (MFP) on the router should be enabled.

Regular penetration testing of external facing assets should be conducted.

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.

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.

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.

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 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.

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. pipeline to increase the visibility of security threats.

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.

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.

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.

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 by Payatu

- AI/ML Security Audit
- Trainings

More Products Offered by Payatu

- EXPLIoT
- CloudFuzz

Payatu

Payatu Security Consulting Pvt. Ltd.

www.payatu.com

info@payatu.io

+91 20 41207726