Payatu

Red Team Assessment for a Global Leader in the Semiconductor Industry

Payatu Casestudy

Here's another success story of the Payatu Bandits performing Red Team Assessment for a Global Semiconductor Manufacturer.

★★★★★

Payatu is glad to have performed the assessment successfully and get five on five for its professionalism, performance, and on-time delivery.

Table of Content

Project Overview

The client is a global semiconductor manufacturer known for creating solutions that enable secure connections for a smarter world. It employs 30,000+ people across 35 countries. Being a world leader in the semiconductor industry, the client has been the face of innovation for over a decade.

To have such a reputed and vibrant organization onboard for red teaming, their infrastructure was not only a great opportunity, but also a responsibility of backing an innovator in its vision of creating a more secure connection for everyone.

The scope of the assessment included the entire IT landscape of the client and its acquisitions.

The objective of the assessment was to leverage Payatu's extensive expertise in Red Teaming domain to evaluate the robustness of clients' IT infrastructure against intrusions and attackers, especially when a majority if client's employees were working remotely.

It has forever been Payatu's modus operandi to enjoy the tasks at hand and think from an eagle's point of view. This approach, ensured focused & seamless delivery along with the flexibility to modify plans if hit by a roadblock. The Bandits always take pride in supporting and strengthening the client's IT infrastructure.

The results of the assessment were outstanding! This is being said confidently because it isn't a standard practice for CISOs of such huge organizations to indulge in sharing positive feedback and patting the backs of a service provider. Payatu is extremely pleased to receive such a great response, and also can't help but feel proud of the bandits, who dedicated themselves in all entirety to this project.

The Scope

Replicating the type of attacks that could be initiated from the Internet on the client's infrastructure and applications including but not limited to

1 Web Servers and/or Applications

2 Mobile Application

3 Network

4 Servers

To identify vulnerabilities which can be exploited to

01 - Bypass the security controls implemented

Enumerate accounts - 02

03 - Gain privileged access to the infrastructure/ network/applications in scope

Gain access to internal network - 04

05 - Copy/Access data

All types of social engineering attacks like phishing, impersonation etc. to extract credentials or other sensitive information from employees.

Challenges

Since the purpose of this project surrounded infiltrating the network of the company, the Bandits decided to social engineer their way into the internal infrastructure of the organization. For this, Payatu had to design and share certain links with the employees via email. Some of the challenges pertaining to this process were -

01 The size of the organization coupled with its distribution centers and manufacturing centers spread across the globe made it relatively complex to identify the crown jewels.

02 Identification of the endpoint which was being used to connect to the internal network

03 2-Factor authentication of VPN, Mail Server, etc.

04 Ensuring phishing emails landing in primary inbox of end users

05 Bypassing antivirus/firewall

06 Time constraint for the red team activity

Process

Since this company is a highly recognized and of the most well-versed institutions in its respective domain, the scope of the project as well as its execution had to be planned meticulously and with utmost discretion.

Discretion, why?

As mentioned, the task at hand was to conduct a red team assessment. Red team assessment is a threat emulation where the Bandits had to gain access to the client's critical assets, in order to assess the posture and readiness of the client to detect and withstand any targeted attack.

Since this enterprise is one of the largest in the said industry, it owns multiple websites, apps, and domains.

The team started with listing down all the company owned websites inclusive of all the acquisition companies' domains and sub-domains. Roughly the number of websites lay in the range of 100-200.

All of these domains were assessed for vulnerabilities and due to the robust security posture of the company, there were no critical vulnerabilities found.

This led to the initiation of the second phase of the project, assessing the IPs and other networks owned by our client. Targeting the web applications first and then moving on to the network, the Payatu team conducted the assessment to identify vulnerabilities.

Certain vulnerabilities were identified but they were not critical enough to help us in exploiting the network to a greater extent.

And the last step to this phase was to assess the mobile applications, which were completed successfully.

Since getting inside the network was still a challenge, the team decided to leverage the weakest link in the cybersecurity domain and the easiest target of any attacker – the employees.

Bringing us to the third phase of the project, this is when the Bandits planned and agreed to conduct a phishing attack.

Starting with creating a mail template that would mimic the one's coming from the internal IT department of the company; it was the responsibility of the Payatu team to ensure that they infiltrate the system for identifying any gaps in the security posture of the client.

Payatu decided to social engineer certain employees of its client to lure them into opening their mails and clicking on infected links.

So, the plan was to roll out a specifically curated email to the employees of the client, disguising as their IT team, and asking them to click on the inserted links. One of the links when clicked would take the employee to a dummy website that the team created and ask the employee to insert his/her VPN credentials and change his/her password because suspicious activity was detected on his/her account.

After a couple of attempts and landing in the spam folder, the team was able to create a strategy that helped them land in the inbox of the client's employees and resulted in 60% of them clicking on the infected links and even changing their passwords.

Now, the team had the valid credentials of the official employees of its client, and these credentials were then used to login to the VPN of the organization. The VPN endpoints were derived out of the act of social engineering the sales team of the enterprise.

Note that once you can log in to the VPN of the company, you are inside the infrastructure of the enterprise. This means that now the bandits could stretch their scope to a different level, which was initially a little difficult with the internet due to them being internal networks.

The bandits then moved to pentesting with this newly developed strategy and scope, with an extensive research and information gathering of the number of machines, type of devices, number of users, servers, etc.

After entering the network, it was understood that there were over 25,000 computers and over 30,000 emails being used inside the network of the organization. The team was able to successfully compromise some of these networks with a laser-focused execution of social engineering.

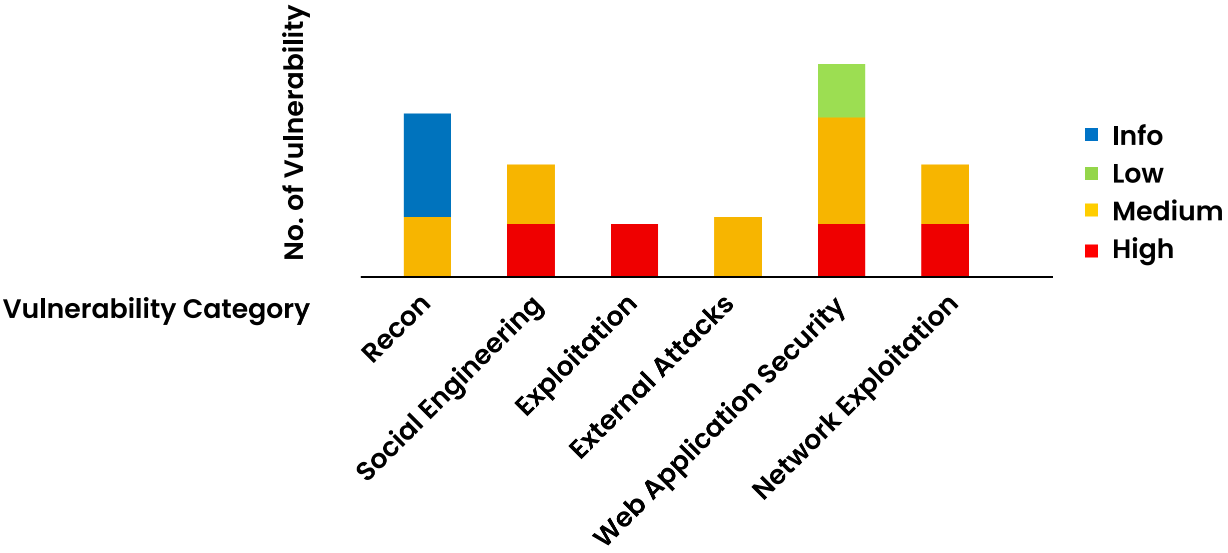
Findings

HIGH SEVERITY VULNERABILITY

1. Social Engineering – Phishing
2. Bypass in internal network
3. Privilege Escalation
4. Network Exploitation

MEDIUM SEVERITY VULNERABILITY

1. Recon
2. Social Engineering – Sales Support Chat
3. NoSQL Injection
4. Access Token Hijacking


No. of Vulnerability
Vulnerability Category
Recon
Social Engineering
Exploitation
External Attacks
Web Application Security
Network Exploitation
Info
Low
Medium
High

Recommendations

Utilizing its vast experience and expertise in the cybersecurity domain, Payatu delivered certain actionable recommendations to its client that would play a crucial role in safeguarding the assets and critical information of the company.

01 Implement U2F authentication.

02 Whenever a user adds a device for MFA approval, there should be an approval from the admin

03 2FA should be implemented in every portal where users can access O365.

04 Install all the security updates released from the vendor

05 Stop the use of OS which are no longer supported by Microsoft.

06 Remove default credentials from the router.

- Implement Azure Conditional Access that blocks user controlled MITM servers which can be used to perform sophisticated phishing attacks.
- Spread awareness among employees to not enter their credentials on any suspicious phishing emails.
- Monitoring teams should be more alert when any such mass phishing emails are received and should immediately block the phishing domain and inform the employees.
- RDP should be protected either with SmartCard sign-in or with certificate authentication and 2FA so that people with valid certificate can only access those servers.
- The best way to prevent NoSQL injection attacks is to avoid using unsanitized user inputs in application code, especially when building database queries
- Maintain a server-side list of all URLs that are permitted for redirection. Instead of passing the target URL as a parameter to the redirector, pass an index into this list.

Our Bandits, Our Pride.

At Payatu, we believe in following one's passion. With that thought, we have created a world-class team of researchers and executors who are willing to go above and beyond to provide best-in-class security services. We are a passionate bunch of folks working on the latest cutting-edge security technology - **Known as Bandits**

- Tech-led Security Services
- Vibrant Skillset
- Proven security analysis techniques
- Community Outreach
- Research-based Intelligence
- Lean Organization
- Flexible Team

Payatu

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.

Our deep technical security training and **state-of-the-art** research methodologies and tools ensure the security of our client's assets.

At Payatu, we believe in following one's passion, and with that thought, we have created a world-class team of researchers and executors who are willing to go above and beyond to provide best-in-class security services. We are a passionate bunch of folks working on the latest and cutting-edge security technology.

Payatu

Payatu Security Consulting Pvt. Ltd.

🌐 www.payatu.com
✉ info@payatu.com
☎ +91 20 41207726