Payatu

Payatu Casestudy

Dark Web Data Leak Investigation for a German Manufacturing Company

Payatu Security Consulting Pvt. Ltd

Project Overview

The global nature of the Internet has allowed criminals to commit almost any illegal activity from anywhere in the world, causing monetary and non-monetary damage to individuals and organizations.

This story serves as a perfect example of the consequences of such criminal activity. This is about a well-recognized German manufacturing company specializing in pipelines and manual motor designs. The company received intel that some of its private data had been leaked on the dark web. So, it approached Payatu to help identify and investigate the leak on the dark web.

Having expertise and specialization in dark web threats, Payatu Bandits started their investigation. The first step of the process was to understand the client's threat landscape. So, the team developed a plan and began implementing it.

Scope

The scope of the project included:

Round-the-clock monitoring of dark web portals

Various parameters were tested on dark web, and several locations were examined for potential leaks; few of them were:

1. Dark web search engines
2. Darknet marketplaces
3 Ransomware sites
4. Web portals
5. Marketplaces
6. Forums
7. Chat servers

Gathering last three months' data for any possible mentions

Collecting and structuring the search results

How was the Project Executed:

The team carried out certain critical tasks such as:

Conducting searches and exploring multiple dark web portals.

Investigating different DLS(Data Leak Sites) to identify the leak.

Closely monitoring all dark web servers.

The Findings:

Amongst the historical artifacts obtained during the investigation, the team identified a data leak that was posted a couple of months earlier on one of the dark web marketplaces. They also observed that the same leak, that was posted on the dark web marketplace, was available on a Telegram channel called **Industrial Spy**.

Process

The team at Payatu carried out a detailed assessment and it was performed as follows:

1. The first step was to categorize keywords that could be used to publish data of the company on the dark web. The team made a list of all keywords followed by searching and analyzing them on 11 different marketplaces. Some of the market-places where the keywords were searched are mentioned as follows:

- Ramble (Reddit substitute to dark web)
- Breached Forum (substitute to RaidForums)
- XSS (Russian Darknet Market)
- Shadow Leaks
- Industrial Spy

2. As the next step, the Payatu team searched for any data containing the searched keywords on the dark web through different search engines.

Below are few sources where the team searched for related source type:

Source	Source type
Ahmia	Dark web search engine
Breached	Dark web forum

Source	Source type
NulledBB	Dark web forum
Antimigalki	Cards and credential marketplace
Ramble	Reddit alike forum on dark web
Raddle	Dark web forum
Shadow	Leaks leak market
XSS	Russian dark web market
Dark Leak Market	Leak market
Industrial Spy	Marketplace

The team went an extra mile and monitored a few more ransomware sites; some of them were:

- Alphv
- Cuba
- Everest
- Hive
- Lockbit 3.0
- AvosLocker

Challenges

The project was very time sensitive

Every monitoring step required accessing the dark web and due to the complex nature of the dark web, browsing and searching would take a lot of time

Mitigation Measures to Avoid Future Leaks:

To safeguard against potential leaks, the team recommended following certain best practices such as:

1 Apply a password update policy to avoid any potential data breach.

2 Apply two-factor authentication (2FA) for all employees.

3 Critical Infrastructure storing sensitive data like customer data should not have direct access to the Internet. Instead, segmentation of the network with access control is advisable.

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.

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.

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.

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.

Payatu

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.

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.

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.

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.

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.

More Services Offered

- AI/ML Security Audit
- Trainings

More Products Offered

- EXPLIoT
- CloudFuzz

Payatu

Payatu Security Consulting Pvt. Ltd.

www.payatu.io

info@payatu.io

+91 20 41207726