DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

DSCI
THREAT INTELLIGENCE AND RESEARCH INITIATIVE

Note on Recent Data Breach

Recent Activities

Recent data breach exposed a portion of the 10 Cr user metadata on the dark web. The respective payment process company that processes payments for large enterprises and others reported that they have first detected an unauthorized attempt on servers on 18th August 2020 which was terminated when in progress. No card numbers, financial credentials, or transaction data were compromised at that time.

As per recent reports, the data that was leaked on the dark web included non-anonymised names, phone numbers, and email addresses.

Cause and Impact

- In the month of august 2020, due to unauthorized access (through expired old access key) a portion of users meta data (non-anonymised) got leaked. As per official reports, intrusion was traced immediately, and asset used in the hack was terminated.
- This signifies the importance of access control and management of digital assets (creation, updation and timely deletion on the completion)
- About 3.5 Cr records with masked card data and card fingerprint (which are non-sensitive information) were breached.
- A portion of the 10 Cr user metadata (Plain -text email ids, and phone numbers got compromised)

Common Pattern

Financial institutes are always on prime target, but in the last 2-3 incidents it is observed that threat actors are shifting their focus to technology start-ups, Fintech, and third-party payment service providers. All these cyber-attacks are financially motivated and Leaked data is being sold on the dark web for an undisclosed amount. Attackers contacting buyers on Telegram and asking for payments in Bitcoins.

What steps Start-ups/ organizations must take to avoid data breaches

In the context of recent data breach, many exploits are happening so far due to not getting security basics right-unprotected databases, failure to patch systems, poor authentication, and access controls (Not implementing MFA, Privilege based access etc.), unpatched servers and very importantly mistakes in software supply chain security.

1. ***Getting security basics right***

Financial services companies/ start-ups should be looking at how they can get basic security right and improve their security posture across all lines of defence – prevention, detection, response, policies and compliance, and testing and auditing. Organizations must take proactive steps not limited to the following :

a. *Periodic Security Assessment and Breach attack Simulations – Active incident monitoring and immediate triggers to respond those incidents.*

b. *Plan for active monitoring, handling and follow-up of cyber security incidents and breaches*.

c. *Risk quantification and implementation of robust information security policy*

d. *Secure Configuration management- On the public /private cloud ensuring secure configuration of servers, databases, instances becomes very crucial. While building, installing virtual instances and network devices, security misconfiguration is one of the most common gaps that threat actors tend to exploit.*

e. *Access Management – Manage accesses to high level assets such (databases, production servers etc.) with privilege-based access control and enforce MFA to every crucial access.*

f. *Manage Security keys and certificates carefully (Creation, secure storage, updation and deletion)*

g. *Along with personal sensitive data, also consider anonymising and protect personal data*

h. *Full time Security officer, team (function) and Security capability to operationalize security plans and strategies*

2. ***Strengthening payment ecosystem***

In the complex payment supply chain, several times organizations don't disclose in time that their own software or network has been compromised, putting their entire ecosystem of customers and partners at risk.

As an important constituent of payment supply chain, organization must know its environment end to end and must develop capabilities to monitor and rapidly detect incidents, identify operational security issues, build security testcases, and effective access management.

Refer discussion paper on guidelines for payment gateways and aggregators >> (Section 8 Security, Fraud Prevention and Risk Management Framework)

3. ***It becomes mandatory to timely report the breach and provide guidance to impacted userbase***

Post Breach Recommendations for end User

1. Get confirmation of the breach and check whether your information was exposed.
2. Change and strengthen your online logins, passwords, and security Q&As.
3. Stay alert and monitor your accounts

4. If your sensitive financial data such as card no, CVV and other details are exposed, take additional support from Bank/ Financial Service Provider to further replace/ change your passwords, cards and other credentials.

The Need of the Hour

Along with common security strategies, there is an advantage in setting up your own dark web monitoring capabilities. Organizations must start monitoring the threats and have to consider that organizations shall have to filter through scams and lots of useless information. But this will be additional step taken to pay for the benefit of increased security and reputation protection.

----------End of Note----------