CASE STUDY

Malware Scanning

ABSTRACT:

- This case study dissects the malware attack on many organization using a business website to interact the visitors in the way of e-commerce sites, banks sites, social media sites and etc. Similarly one of our banking firm cladding their banking customer are getting infected by continuous malicious activity on their website., and soon after, they faced a defacement attack where the intruder insert the hazardous content, images, malicious code into their website which is being use as attacking later on by continuity operation of stolen the sensitive information. Also they observe the instances like code injections which creates or delete the web directories of their website and which causes the risk of putting the customer's data in grave danger. Such defaced web pages is inflicting the severe damage to their bank's reputation and reliability.
- Furthermore, due to the malicious contents founds in their site, the Top safe search authorities (Google, MacAfee, Norton Safe web, Google Malware) blacklisted the website which increases the negative consequences of their brand image and the SEO rank. Their issue even increases when they found the bad links placed into their website that download the Virus into the computer of their customers and this Virus/Trojan(Spy Eye, Zeus) tracks the activity of the banking customer once they logged into their bank account. Also their online banking customers had no idea they were infected with Trojans due to which their online banking sessions were being compromised. Hence to get the proper protection, this firm adopted various vendors in the market but their IT professions thinks that their application are still on risk of being attacked as their bank's website can potentially to be infected by a new virus every minute. They feel, the lack in security measures being taken for the zero day attacks as "New attack vector are constantly emerging as new technology evolves".
- Hence this bank firm decided to have the application security which will constantly scanning their website through automated where it checks for malware, viruses, defacement, Zero day threats persistently throughout the day with the mitigation guidelines.

STRATEGY & RECOMMENDED SOLUTION:

- Indusface WAS provides a scanning solution with the services such as (Malware monitoring, Application Audit and Vulnerability Assessment). After monitoring the continuous malicious activity on their website and in order to facilitate this attacks, we proposed to run the Malware monitoring scan on their website at every 30 minutes to identify the fast growing malwares relentlessly and provide the full report to the customer with the remediation guidelines which will help to patch the exploited risk before it impact the bank's customer. We also suggest to maintain the scan reports for inspecting the code level changes identified by the continuous running Malware scan as defacement alerts and it also includes the blacklisting check of the website from among the top safe search engines which helps to secure the Bank's character by maintaining the SEO rank.

IMPLEMENTATIONS:

- The customer confirms our suggestion and agreed to run the malware monitoring scan for every 30 minutes on their website and gets the below benefits:

1. By persistently running scan on their website, it helps to identify the hacked links, foreign links and suspicious links being placed on their website at a real time.
2. The on-going scan will help by providing the active alerts on the website with the mitigation guidelines, on which the customer can proactively take the security measures before it impact the user.
3. The defacement checks helps to identifies, where exactly those incorrect references locate in your code.
4. It also helps the organization with the early identification of security infringements.
5. The continuous scan helps to monitor for security warnings by ensuring the checks from the top blacklisting search Authorities.
6. It will benefit of negate the impact on search engine page rank due to the defaced web page.
7. It also helps to identify the Trojan, Virus, botnets in the website and help to remove the alerts provided by the WAS solution.
8. WAS's malware engine combines with constantly updated database which contains the malware signature along with the behavioral analysis, this will allows to find the zero day attacks and newly discovered malwares.
9. WAS solution also provides the granular detail report to the customer on every hourly basis which describe the exploitable risk and its severity level along with the steps to patch the vulnerability even more quickly.