Cybersecurity through Crowdsourcing

Deloitte

Use Case Three
Decreasing Risk of Data Breaches through Crowdsourced Clients

April 30, 2018

Group Two:
Yiqing(Alice) Guo
Steve Cardozo
Li Chen
Pan Deng
Mengwen Zhou

Information Technology Master's Capstone
ITWS-6800

Prof. Richard M. Plotka

Use Case Two

Table of Content

Targeted Issue

Different kinds of attacks have been revealed recently, which involved new sophisticated ways of stealing data from companies. Companies also frequently fail to patch security flaws in a timely manner. In 2017, credit reporting agency Equifax hired cybersecurity firm Mandiant to conduct a forensic analysis, which revealed a massive data breach affecting 145.5 million U.S. consumers.[1] A popular ride hailing service, Uber, failed to disclose a massive data breach last year for more than 57 million Uber drivers and riders.[2] Although the biggest, headline-grabbing cyber attacks tend to only hit the biggest companies, all companies actually need to be aware of the risk of data breaches.

Solution Purpose

Many businesses have taken steps to protect their data, but the average size of the data breaches in 2017 still increased by 1.8 percent to more than 24,000 records.[3] Sometimes companies can hardly respond quickly enough to the issue to avoid any losses.

The proposed solution will connect as many companies as possible to enable them to respond together to the latest cyber attack issue before being hacked and share the solution with each other at the same time.

Crowdsourcing Approach

The solution team will have ten experts. The business will look for client companies who want better protection to avoid cyber attacks. The solution team will set a honeypot into each client's system. A honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. It consists of data that appears to be a part of the site, but is actually isolated and monitored. Therefore, once a certain company's honeypot is attacked, the team can get data on the attackers.

All of the client companies will be able to share the log of such attack at the same time. It may help the clients avoid an incoming attack. Meanwhile, the experts in the solution team receive the honeypot data from the attackers and can immediately begin to work on the

[1] Williams, Fred O. *Equifax Breach Exposes Data of 147.9 Million U.S. Consumers*. 2 Mar. 2018, www.creditcards.com/credit-card-news/equifax-data-breach-143-million-id-theft.php.
[2] *Uber Hid a Hack That Exposed Data of 57 Million Users and Drivers for More than a Year*. 21 Nov. 2017, www.cnbc.com/2017/11/21/uber-hack-exposes-data-of-57-million-users-and-drivers-report-says.html.
[3] *Cost of Data Breach Study*. www.ibm.com/security/data-breach.

defense solution for this attack. Once the solution has been coded, all of the clients will share it together. By having crowdsourced clients, the whole method can be perfected to help them respond to the latest attack in a timely manner.

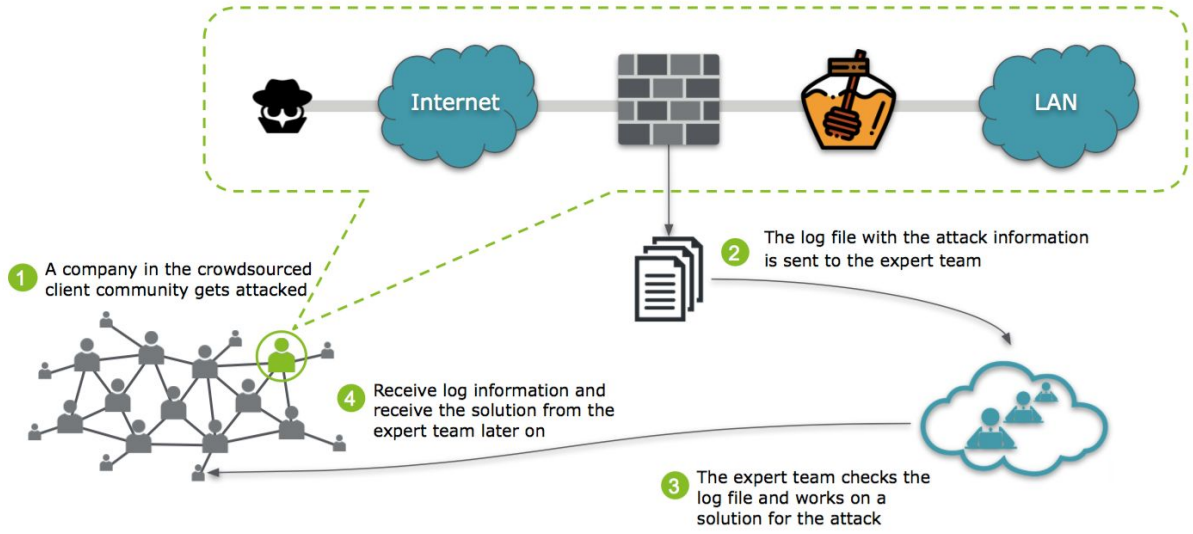

Figure 1 : High-level Work Flow Diagram.

Honeypot setup: T-Pot16.10 multi-honeypot platform.[4]
By using Docker, the following honeypot containers will be provided on the same network interface with low maintenance for the entire system:

- Cowrie is a medium interaction honeypot that can record the accounts and passwords of the attackers and record the hackers' operations by providing a fake file system. It can also save files downloaded through wget/curl and files uploaded through SFTP and SCP.[5]
- Dionaea's purpose is to trap malware which exploits vulnerabilities exposed by services offered to a network.[6] It's ultimate goal is to gain a copy of the malware. When there are external connections, it simulates normal service to give feedback and records the data flow out of the network. The network data is processed by the detection module according to its category. If there is shellcode, the program will automatically download all the malicious files in the shellcode.

Potential Clients

According to the structure of the crowdsourcing approach above, the potential clients are the companies who have data center and focus on avoiding data breaches. They must agree to share log information with other companies who have joined the network.

[4] *T-Pot 16.10*. dtag-dev-sec.github.io/mediator/feature/2016/10/31/t-pot-16.10.html.
[5] Oosterhof, Michel. *Cowrie Honeypot*. www.micheloosterhof.com/cowrie/.
[6] *Home of the Dionaea Honeypot*. github.com/DinoTools/dionaea.

List of Requirements for the Crowd

The employees who are responsible of the log in each company are also responsible for contacting the solution expert team.

Potential Issues

Client companies may be worried about their confidential data being leaked when they share their log information with other companies.

Possible Solutions

Although the log has to be shared immediately, it still needs to be checked before sharing. First, it will be sent to the solution team to check if there is any confidential information included in it. Then, the solution team will send the log to all the other client companies. Since the solution team should have signed the confidentiality agreement beforehand and they also have access to the log, they are the ideal people to be responsible for this task.