Team Binary Bros: Vision Statement
Project: TackleBox

Developers

Christopher Garsia (Team Lead), Sam Pettus (Scribe),
Brice Redmond, Eric Guerrero, Ori Mizrahi

Company

Novacoast

Problem and Importance

2020 has seen a sharp rise in the frequency of cybersecurity attacks and with an increase in their sophistication. These improvements make the attacks harder to spot, thus allowing them to compromise higher-value targets. Often these attacks will target people as the weakest link in the security chain and as a result phishing scams—a tactic which uses fraudulent emails to trick receivers into revealing sensitive information—are becoming ever more apparent. Once sensitive information—like a sysadmin password— has been stolen, the hacker may be able to steal integral data from the company, encrypt it, and then demand money for the encryption key. Since currently there is no way to decrypt the data without the key, the organization is forced to pay the ransom. As a result, prevention is the only method to combat these attacks. Preventing employees from accessing these fake domains can be difficult though even with proper safety training. The process of registering a fake domain, pushing malicious code and emailing victims can take less than an hour total. This speed paired with high volumes of attacks allows some fake domains to exist for weeks or months without being spotted and thus it is only a matter of time before someone makes a mistake and falls for the trap. Furthermore, these attacks are not only tricky to combat, but are also extremely costly—The FBI issued a PSA that estimates that over $12 billion were lost due to email phishing between 2013 and 2018.

Current Implementations

To combat phishing, spam filter engines are typically the first line of defense. However, this solution cannot match the rampant speed at which attacks are being launched. Spam filter engines usually pull suspect domains from older data sources and therefore do not provide a real time solution. On the other hand, educational programs can provide real time solutions by bolstering security through teaching a company's workforce to detect and avoid phishing scams. Although effective, companies are still vulnerable to phishing due to human error.

Outcome

The outcome of this project is an automated service that quickly identifies phishing DNS addresses and aids the company’s response to them. To locate phishing DNS addresses, our system will analyze the risk that these addresses are malicious using open source intelligence. Then our system will rank the similarity of the spoofing website with Novacoast’s record of the real website using natural language processing and regular expression comparisons. Once the risk and similarity have been analyzed, our service will do 4 things with the results:

1. Block navigation to these websites for Novacoast platform users.
2. Notify the company’s legal team if the phishing website uses stolen intellectual property so they can take action against the creator of the phishing website.
3. Send reports of the websites that have been made to steal data from a company.
4. Post the data we have collected to open source projects so that others can benefit from what we have discovered.

Technologies

Frontend: React, Responsive Design, UI Component library (potentially Bootstrap)

Backend: Flask (Python), Microservices using GraphQL

Database: PostgreSQL

Hosting: AWS

Technologies: RabbitMQ

Containerizations: Kubernetes, Docker

Milestones

1. Set up development environment for all team members
2. Research tools / technologies
3. Get frontend UI skeleton running
4. Design backend and its API schema
5. Connect frontend to backend
6. Complete first detection. Determine if a domain has been registered, and push it to the database
7. Automate the process of calculating similarity between domain names
8. Automate the process of calculating the risk of the website using open source intelligence
9. Design response for identification of malicious domains