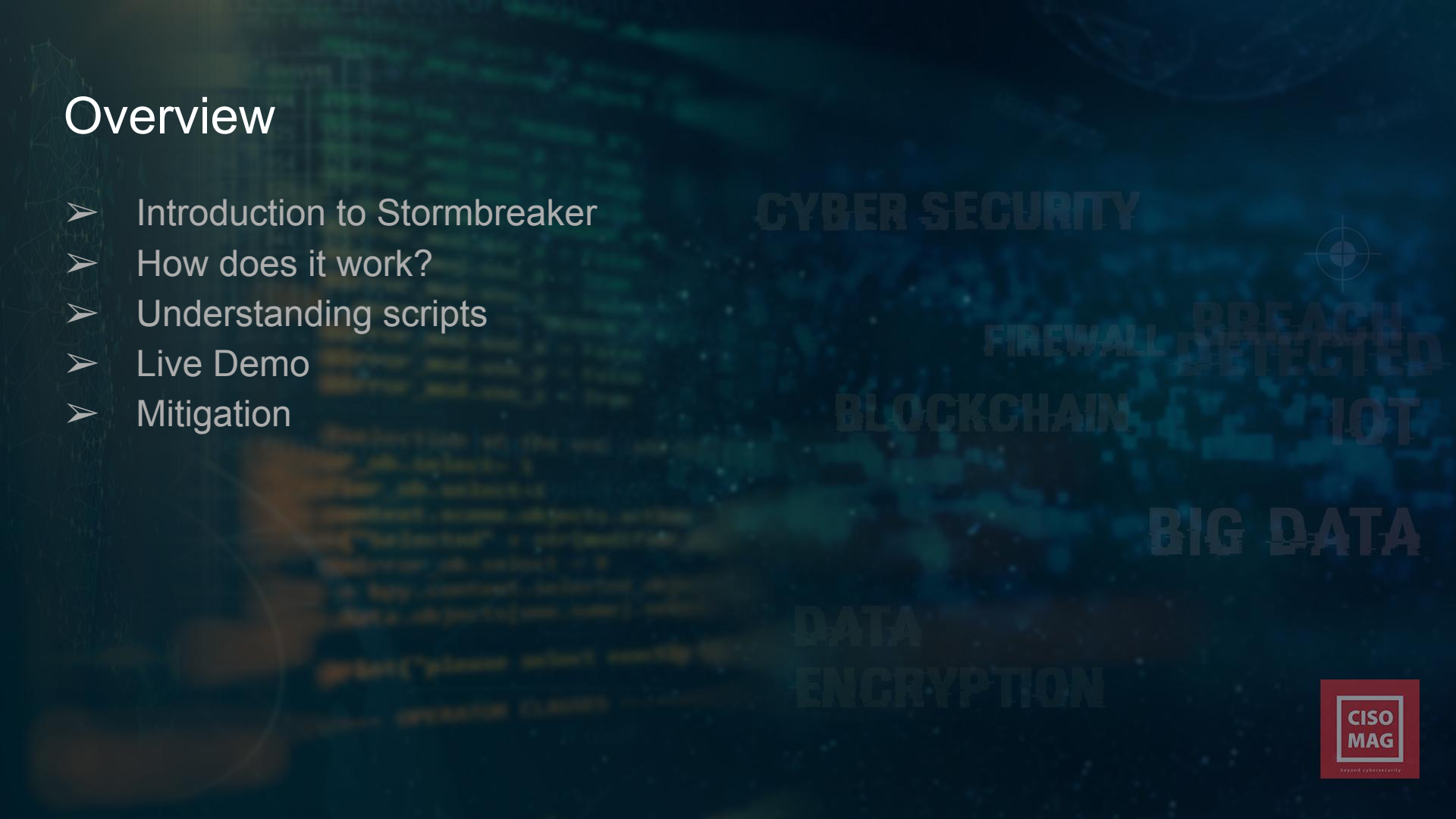
StormBreaker Social Engineering Exploit

By:
Alessandro Sant
Exequiel Millado
Naresh Arora
Gunveer Singh
Ernest Wong
Aneesh Sharma

Overview

- Introduction to Stormbreaker
- How does it work?
- Understanding scripts
- Live Demo
- Mitigation

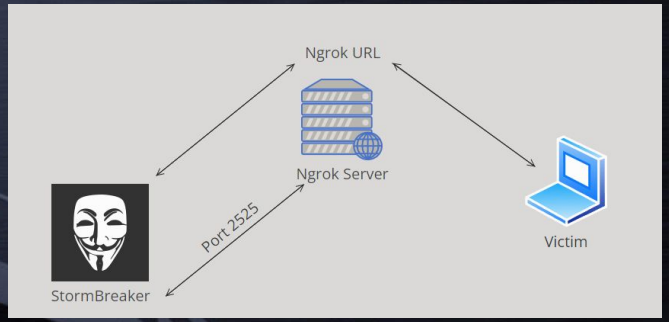


What is Stormbreaker?

StormBreaker is a social engineering tool that allows attackers to capture users

- Location
- Webcam
- Device information
- Microphone

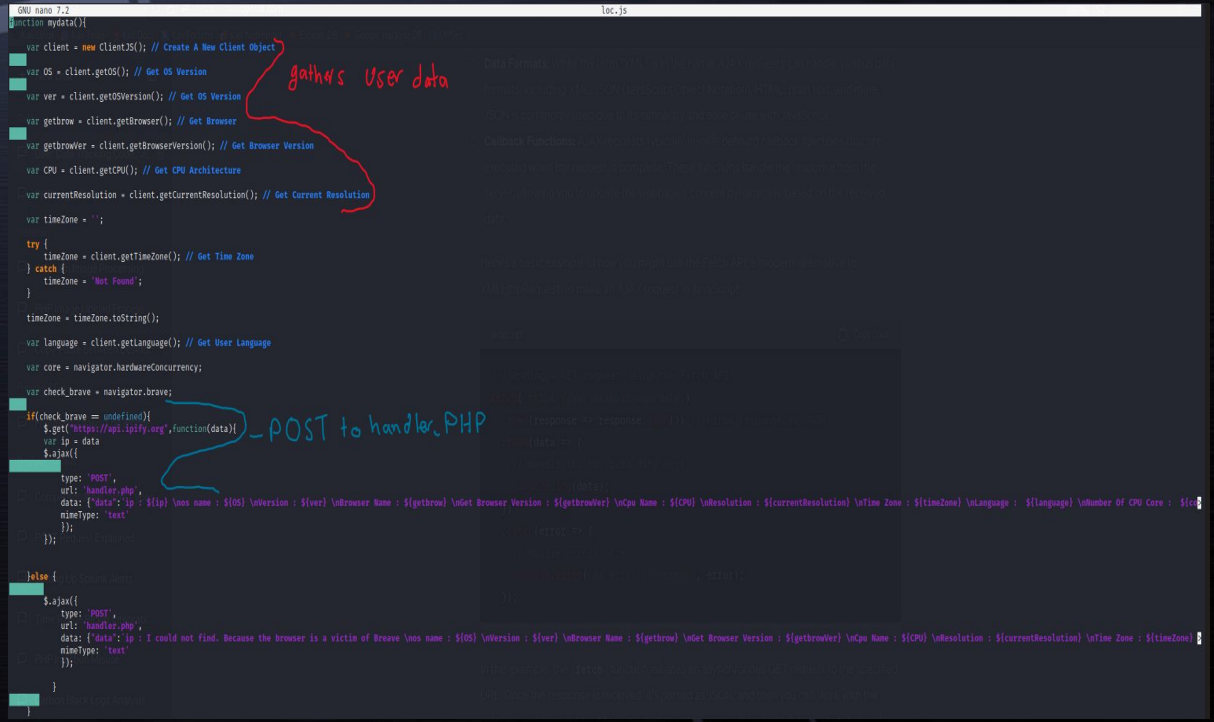
How does this work?



- Ngrok is a service that allows for internet access to a local machine
  - Ngrok allows us to host our local web application to the internet, which makes our application accessible anywhere around the world.
- The attacker runs Stormbreaker on the local machine using a PHP built in server
  - We then connect StormBreaker to Ngrok by running Ngrok on port 2525 which is what StormBreaker is running on locally.
  - Doing this creates a link that allows StormBreaker to be accessible anywhere in the world.
- Once the attacker sends the link to the victim, they are able to capture their information.
- Spreads the link and waits for victims to click on it

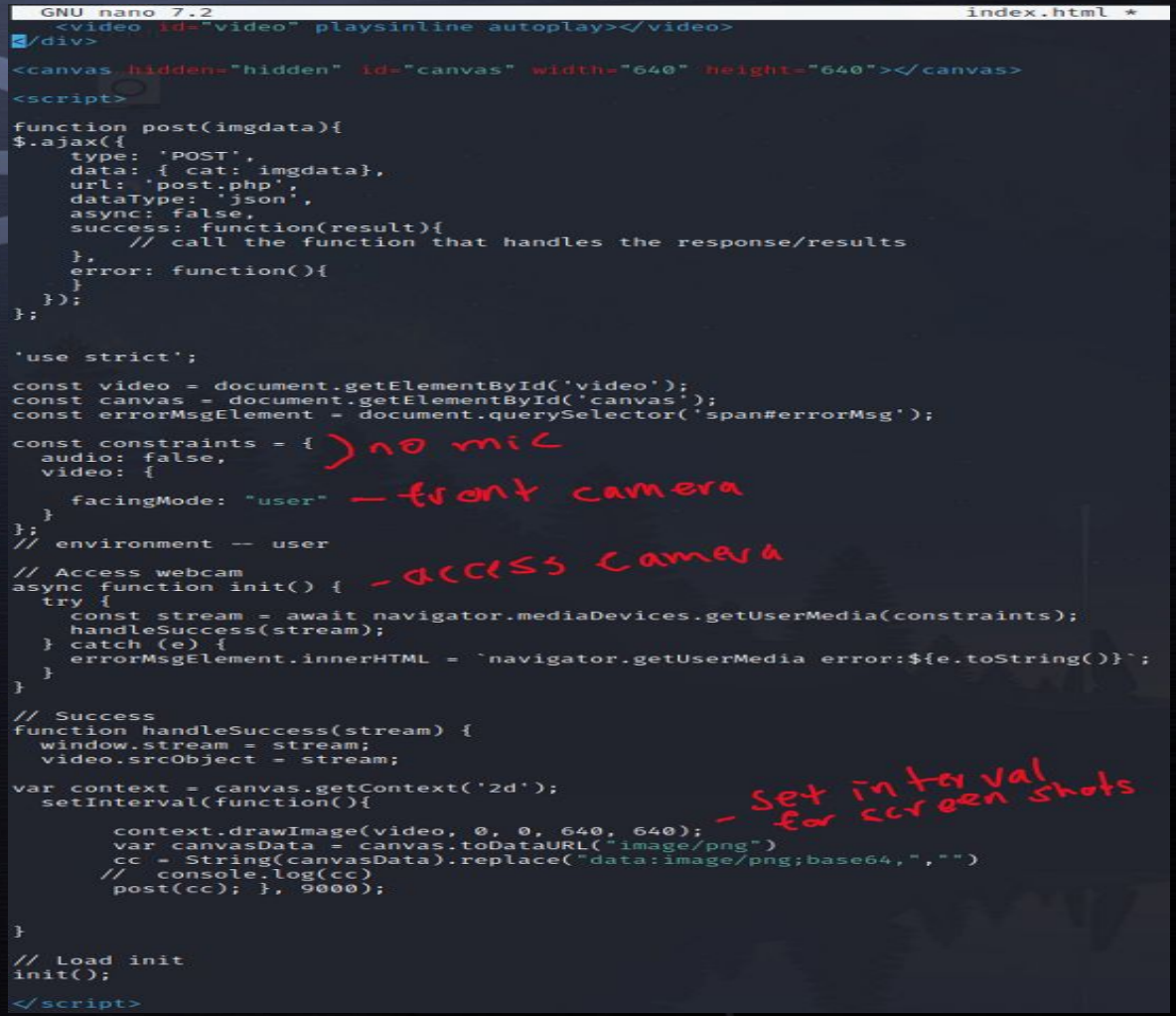
StormBreaker info Capture

- The loc.js file within StormBreaker contains JavaScript code that collects information such as OS, version, CPU on the victim machine.
- Once information has been gathered,it then sends it to a server using an AJAX request.
  - AJAX stands for Asynchronous, JavaScript and XML.
- Code uses $.get to retrieve the user IP from https://api.ipify.org. Then sends an AJAX POST request to the server side “handler.php”.



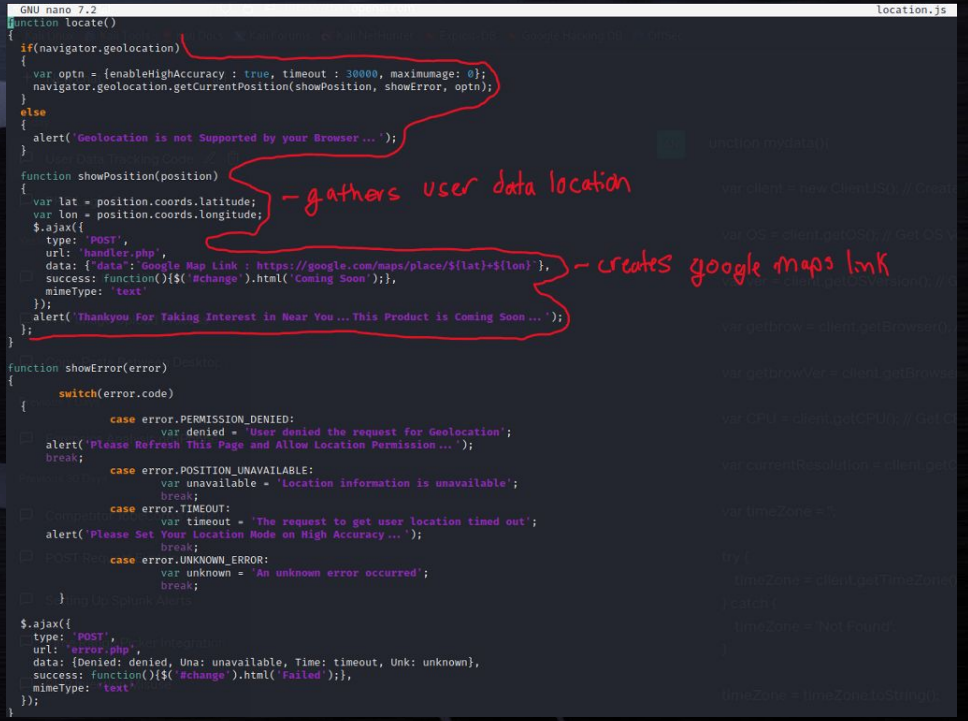
Camera Capture Script

- In the camera module exploit there is an index.html file which contains HTML, JavaScript and CSS code.
- The JavaScript code allows for us to access the user's camera and disable the mic.
- The init function attempts to access the user's camera and if successful, the handleSuccess function set up the video stream.
- The setInterval repeatedly captures frames from the video stream.



Location Capture Script

- StormBreaker uses JavaScript code to gather user location data using the navigator.geolocation API.
- The location function is defined using If else statements.
  - Checks if the browser supports Geolocation API.
- If supported,the high accuracy option will use all available resources to gather the most accurate information.
- The showPosition function contains the latitude and longitude.
- An AJAX post request is made to the server side handler.php that has the longitude and latitude that makes up our Google Maps link.



Live Demo

Tools used:

- ngrok cloud server, PHP server
- HTTP service on port 2525
- Linux on Virtualbox manager, Mozilla Firefox internet browser
- Slack, terminal, nano text editor, Zoom video recorder, Google Maps

Let’s start the Live Demo to understand what it does and how it works.

Cybersecurity Mitigation Alert!

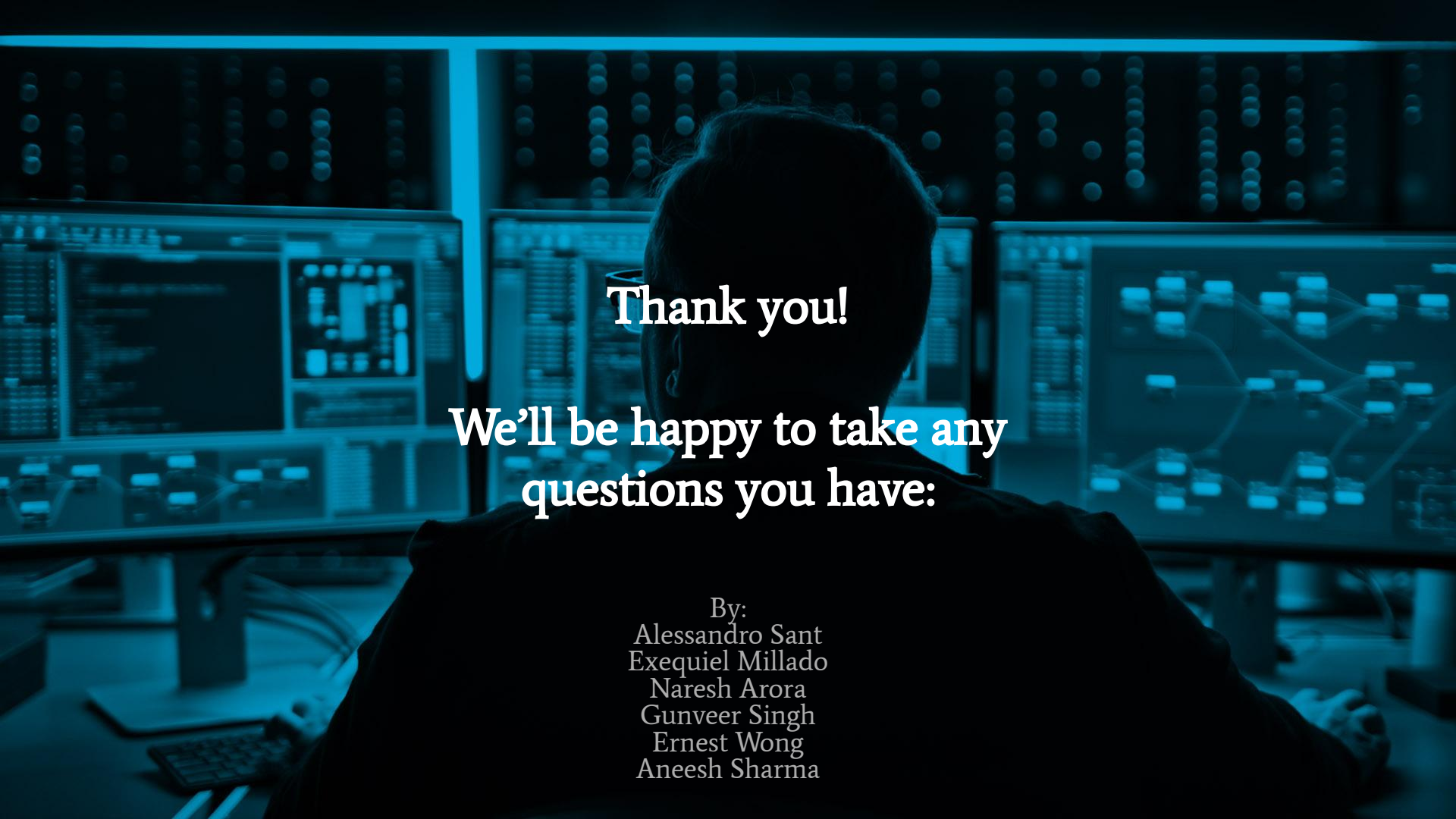
- Have you heard the saying, "A picture is worth a thousand words"? It seems cyber criminals are using it to their advantage.
- Cyber criminals are luring victims to click on images rather than downloading malicious files.
- One of the best policies, if you don’t recognize the image or link, investigate, verify first and if it looks suspicious DON’T click it.
- Install Anti-virus program with pop up blockers and legitimate anti-phishing add-ons on your browsers.
- Recommendation on putting a covering on your camera in case hackers were able to access it.
- Change passwords regularly and ensure complexity by using special characters, numbers, lower and uppercase letters.
- Don’t ignore security updates on your desktop computers, laptop, phones and tablets.
- Use multifactor authentication.

Mitigations

- Education is key for a company or corporation by giving employees the knowledge and techniques to help stop cyber attacks from breaching an organization's cyber defence. Also, HR needs to do a pen testing on a regular basis to test employees for not clicking suspicious images or links and attain or exceed the threshold that were set.
- Regular Security Audits and Penetration Testing: Conduct regular security audits and penetration tests to identify vulnerabilities in your systems and applications. Address these vulnerabilities promptly.
- Network Segmentation: Divide your network into segments to contain potential threats and prevent lateral movement by attackers. This limits the impact of a breach.
- Firewalls and Intrusion Detection/Prevention Systems: Employ firewalls to monitor and control incoming and outgoing network traffic. Intrusion detection and prevention systems can help identify and stop potential threats.

Continuing - Mitigations

- Backup and Disaster Recovery Plans: Regularly back up your critical data and systems. Create and test disaster recovery plans to ensure you can recover quickly from a cyber incident.
- Application Security: Implement secure coding practices, conduct code reviews, and use web application firewalls to protect against common vulnerabilities like SQL injection and cross-site scripting.
- Encryption: Use encryption to protect sensitive data both in transit and at rest. This includes encrypting communication channels (e.g., HTTPS) and using encryption tools for data storage.
- Incident Response Plan: Develop a comprehensive incident response plan to guide your actions in case of a cybersecurity incident. This ensures a coordinated and effective response to minimize damage.



Thank you!

We'll be happy to take any questions you have:

By:
Alessandro Sant
Exequiel Millado
Naresh Arora
Gunveer Singh
Ernest Wong
Aneesh Sharma