Go-Phishing

- **Group 2:**
  - Darren, Lim Yu Kun
  - Lau, Siew Ping
  - Kwong, Kai Man
  - Tsai, Hsuan Hsieh

Outline

- Go-Phishing Overview
- Target Identification
- Open Source Intelligence: LinkedIn
- Maltego: Mapping GT Systems via TA Credientials
- Phishing Email Structure
- Phishing Attack Execution & C2 Setup
- End-to-End Phishing Call Flow
- Target Profile & Reconnaissance
- Ethical & Academic Considerations
- Defense Mechanisms & Prevention
- Conclusion

Go-Phishing Overview

Objective:

1. Campaign Type

Spear-phishing targeting a Georgia Tech TA

2. Desired Data

Steal login credentials by tricking the target into entering Georgia Tech SSO info on a fake webpage

3. Purpose:

Simulate how an attacker could access student records or grading systems, altering grades or misusing data

4. Value

- ✓ **Potential Damage**: Disrupt academic integrity, harm performance records, and tarnish the institution's reputation.
- ✓ **Monetary Value**: Stolen credentials can be sold or used to manipulate records for financial gain.
- ✓ **Market:** Academic credentials are valuable in cybercrime for fraud and impersonation.

Target Identification

Target Identification:

Ali Segovia is a TA with a cybersecurity background, requiring a highly convincing phishing attempt.

Reconnaissance Plan:

- **LinkedIn Profile:**

  Gather information on Ali's professional background, interests in IoT and cybersecurity, and identify key projects or events (e.g., conferences) to craft a tailored phishing email.

- **TA Credentials:**

  Use Maltego to map services tied to her GT credentials (e.g., Canvas, GT VPN) and create a phishing email based on her regular tools.

Target Environment:

Identify tools she regularly uses (e.g., Georgia Tech systems). Analyze vulnerabilities like her involvement in conferences or collaborations that could increase her likelihood of clicking a link.

Open Source Intelligence: LinkedIn

About

"The truly exciting thing about your life is that there is no core curriculum; the entire place is an elective." - Jon Stewart

Motivated individual, dedicated team member, and Navy veteran who strives to make lasting contributions to each and every project and workplace. Whether it is creating employee information security training, writing technical documentation for business continuity, or even creating marketing materials, I am dedicated and focused on both long and short term goals.

As a technical cybersecurity consultant, I help enterprise level clients optimize their existing toolset and make the right decisions when it comes to investing in their cybersecurity posture and creating solutions to fit their needs. I serve as a technical resource that can be counted on to keep up with the latest cybersecurity trends and best practices.

Learned //

I am currently a Master of Science student of Cybersecurity at Georgia Institute of Technology, where my focus is cybersecurity policy. My anticipated graduation is May 2023.

I hold a Bachelor of Science degree in Internet of Things (IoT) Engineering and a BS in Electrical Engineering, focusing in cyber security and embedded systems from Florida International University. I had the honor of graduating from FIU as Cum Laude and with a World's Ahead recognition from the College of Engineering and Computing.

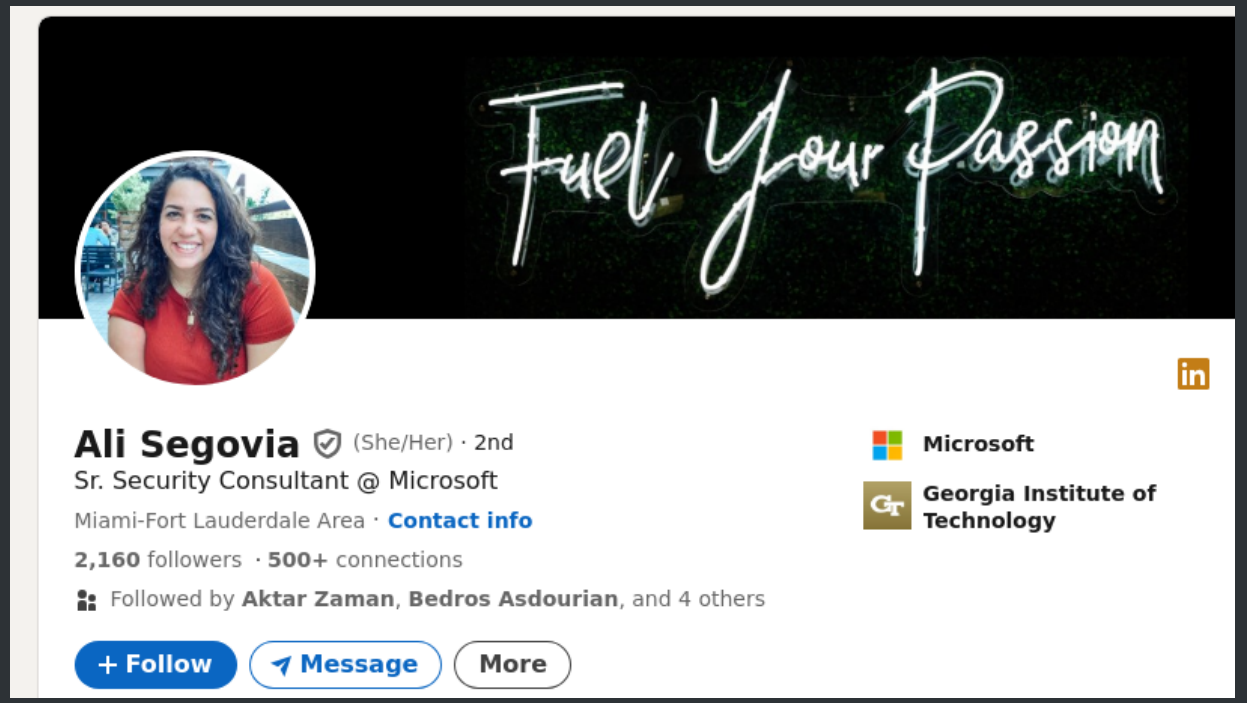
Loved //

On my free time, I am an avid outdoorswoman. I enjoy managing and writing for my own blog, mountain biking, off-roading my Jeep in challenging terrains, hiking, camping, and glamping. I love road trips and escaping life on the weekends to explore a new park. I also love kayaking and paddleboarding, and heading out to the sandbar with my friends for some sun and fun.

I have a personal passion for the automotive industry, especially in Jeeps and trucks. You can often find me at car shows on the weekends and watching automotive documentaries.

Occasionally, you can find me on the couch binge-watching the latest Netflix shows or indulging in my guilty pleasure, The Bachelor or The Bachelorette.

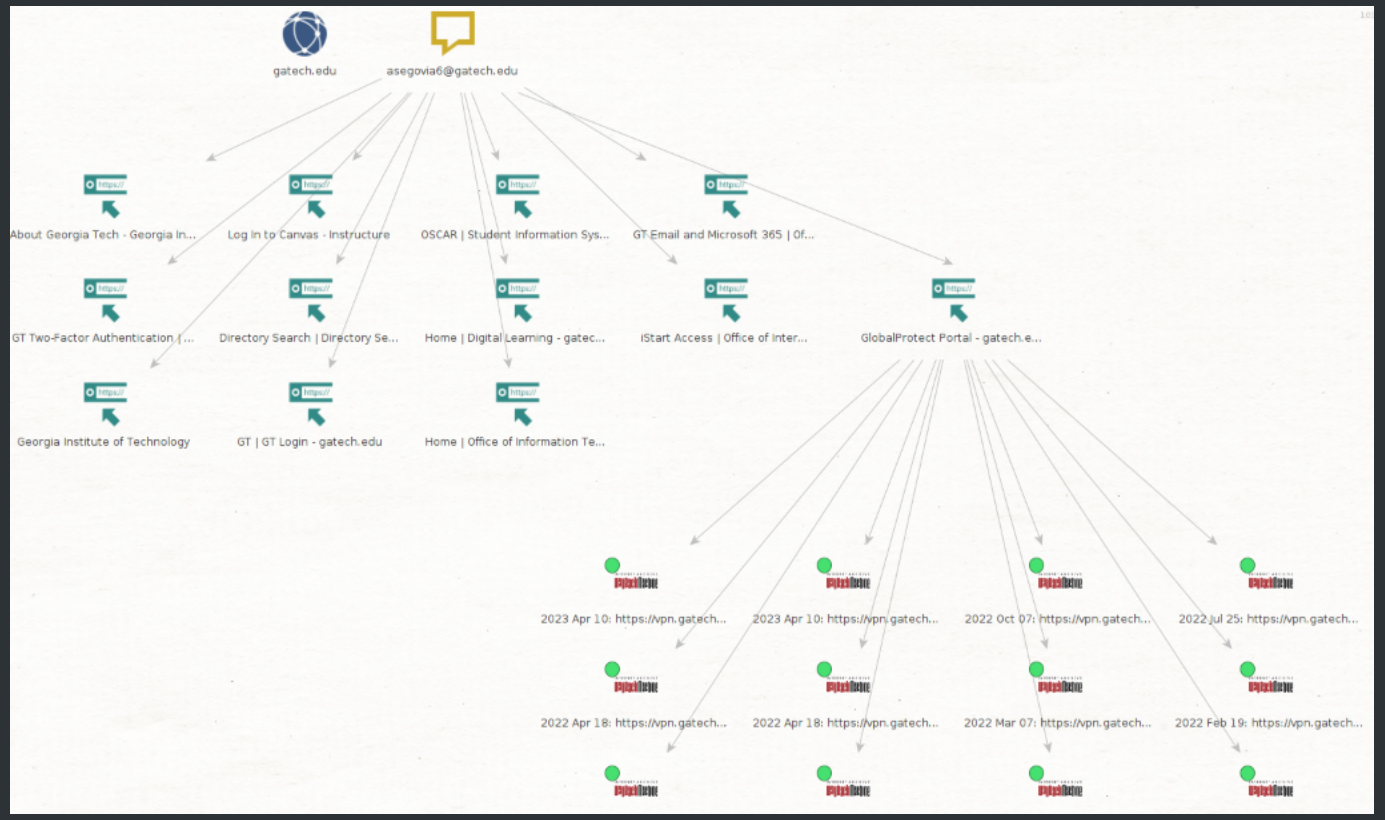
Located // Miami, FL



Maltego: Mapping GT Systems via TA Credientials

Maltego maps services tied to the TA's GT credentials (e.g., Canvas, OSCAR, GT VPN, Microsoft 365).

Understanding these systems helps craft phishing emails based on her frequent interactions (e.g., fake Canvas login or VPN security update)



Phishing Email Structure

1. Message Construction:

Phishing email mimics legitimacy, using trust-building and urgency tactics

2. Plausible Source:

Email: chrislau73@gatech-sso.com, designed to look official with the Georgia Tech domain

3. Subject:

"Invitation to Judge: Student IoT Innovation Capacity Building Challenge," relevant to the target's interests

4. Body Text:

Personalizes by name, mentions "Christopher Lau" from Georgia Tech-affiliated CDAIT, links IoT event to target's expertise, and urges "RSVP by September 24, 2024" via a malicious link

5. URL Obfuscation:

Displayed URL mimics Georgia Tech but redirects to a phishing page

6. Social Engineering:

Email builds trust by referencing the target's background, avoiding phishing red flags

Phishing Attack Execution & C2 Setup

1. Phishing Attack Execution:

Technical setup to steal credentials

2. Execution Flow:

- Phishing email prompts the TA to RSVP and log in
- Malicious link redirects to a fake VPN page
- C2 server captures credentials

3. Command and Control (C2) Node:

- Hosted on AWS EC2 with Docker
- Logs credentials for unauthorized access
- Ensures scalability

4. Delivery Platform:

GoDaddy M365 mimics Georgia Tech's internal emails, bypassing filters

5. Payload and Exploit:

Fake login page captures credentials for access to academic systems

6. Technical Diagram:

Phishing email → Redirect to fake page → Credentials sent to C2

End-to-End Phishing Call Flow

1. **Phishing Email**

   Sent to Georgia Tech TA from gatech-sso.com using SPF, DKIM, and GoDaddy M365 to appear legitimate.

2. **User Interaction:**

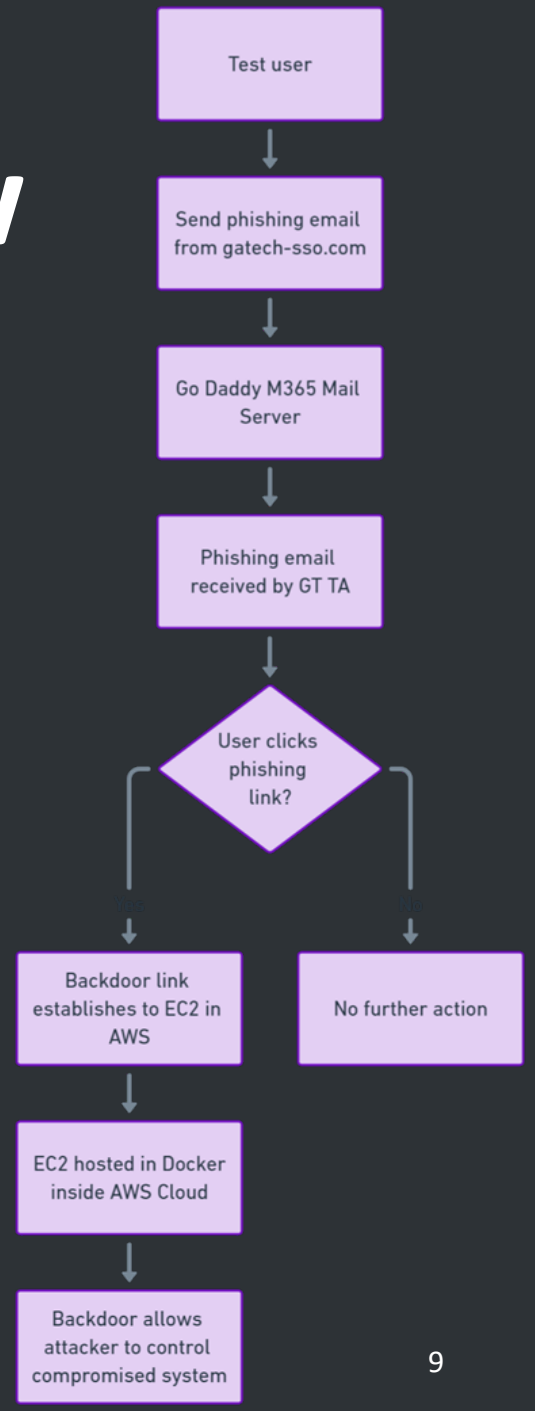
   Email appears authentic, prompting TA to click, leading to a CloudFlare-hosted fake login page where credentials are captured.

3. **Infrastructure:**

   Phishing setup hosted in Docker containers on AWS EC2 for scalability and isolation.

4. **Backdoor Control:**

   Credentials are sent to the C2 server for remote access or further exploitation.



Target Profile & Reconnaissance

1. Target Details:

- **Target:** Alexandria Segovia, Georgia Tech TA, focused on IoT and cybersecurity
- **Role:** Likely has access to sensitive academic information, including grades

2. Reconnaissance Plan:

- **Info Gathering:** Attacker researches her background via public staff directory and LinkedIn
- **Adaptability:** Phishing email could target other staff with similar access

3. Environment Vulnerabilities :

- **Email Dependence**: Official communications rely heavily on email, making phishing emails appear routine
- **Single Sign-On (SSO):** Centralized login system is vulnerable to exploitation

4. Failure Points:

- **Defenses:** Target may have security awareness training and anti-phishing filters
- **Single Sign-On (SSO):** Centralized login system is vulnerable to exploitation

5. Key Vulnerability:

Lack of MFA: Without MFA, phishing success is more likely

Ethical & Academic Considerations

This phishing simulation is a controlled academic exercise, conducted under Georgia Tech’s ethical hacking guidelines.

No Real Harm:

No data or credentials are stolen, and no malicious code is executed. The victim receives a "You are phished" message after the exercise.

Informed Consent:

The target is informed after the simulation that it was part of a learning exercise.

Adhering to Policies:

The simulation follows Georgia Tech’s ethical standards, avoiding spoofing real login pages as per assignment guidelines.

Students gain hands-on experience in constructing phishing campaigns, understanding the attack lifecycle, and simulating credential theft.

Defense Mechanisms & Prevention

Phishing Prevention Techniques:
Defense strategies to prevent phishing attacks

- **Email Filtering:**
  - Advanced spam filters detect spoofed domains or unfamiliar senders.
  - Machine learning algorithms identify deceptive URLs and social engineering.
- **User Awareness & Training:**
  - Regular training to identify phishing and avoid suspicious links.
  - Simulated phishing campaigns to improve awareness.
- **Two-Factor Authentication (2FA):**
  - MFA adds a layer of security, preventing unauthorized access even if credentials are stolen.
- **Email Verification:**
  - Verify sender legitimacy before clicking links.
  - Hover over URLs to ensure they match the displayed address.

Conclusion

1. Phishing Simulation Success:

Through targeted reconnaissance, OSINT tools like LinkedIn and Maltego, and a carefully crafted phishing email, we successfully simulated a realistic phishing campaign against Georgia Tech's TA, demonstrating the attack lifecycle.

2. Ethical Considerations:

The simulation adhered to ethical standards, ensuring no real harm was done. Informed consent was obtained post-exercise, emphasizing the importance of ethical hacking and responsible testing of vulnerabilities.

3. Defense & Prevention:

The exercise highlights the need for strong defense mechanisms, such as MFA, email filtering, and user awareness training, to prevent successful phishing attacks in academic environments.

Thank you