Anjali Gupta

CS 573 - Fundamentals of Cybersecurity

Professor Amoroso

May 5th 2025

Final Examination Paper

I. Brief Introduction

A. The New Jersey Department of Labor and Workforce (also known as NJDOL) was subject to a large-scale, multi-vector attack by an assailant looking to disrupt the department's unemployment insurance program by taking down the network that allows unemployed individuals to claim benefit checks through the NJDOL website. The attack included a combination of AI generated phishing, trojan horse malware and exploitation of a misconfigured firewall. A post was later found on the popular dark web forum called XSS where the assailant claimed responsibility. Although a lengthy post, the assailant exhibited right-wing ideologies and berated NJDOL and their unemployment insurance program, deeming it as "un-American". Since then, the assailant has been identified as a right-wing extremist and an active member of the Proud Boys organization.

II. Initial Phishing Campaign

A. The early signs of the attack were seen when the first phishing email was sent to an employee in the business sector of the department on May 31th, 2025 at 1130. The first employee targeted was part of the HR department; an effort to target less technologically savvy and knowledgeable employees of the organization. The email was found to be AI generated to target the employee specifically and

remove any sort of grammatical mistakes and generate any special characters to mask the actual domain of the email to make it seem more legitimate. DeepSeek, a Chinese AI company, was used to draft the email. The email domain used as part of the phishing campaign was meant to imitate a restaurant in the area the company frequently used as a catering service for employee events. The email was a $10 dollar coupon redemption for any NJDOL employees that clicked the link and "redeemed the offer." The targeted employee clicked on the link at precisely May 31st, 2025 at 1300. From the website link, the targeted employee was prompted to click a button to "redeem the offer." From there, a fake e-coupon was downloaded onto the employees laptop and malware was downloaded onto the employee's machine.

III. Malware Installation and Botnet Creation

A. The malware downloaded onto the employee's machine was a Remote Access Trojan (also known as RAT). This malware was able to give the hacker complete access to the employee's machine, monitoring any and all user behavior and activity. Through unrestricted access to the machine, the hacker was able to send more social engineered phishing emails to employees in the same department in the hopes of creating a bot network (botnet); all emails from this point on were sent internally using the first employee's infected machine. Being able to send validated emails internally using an infected machine strengthened the hold the hacker had on the organization because he no longer needed to bypass any authentication protocols. With access to the NJDOL Microsoft 365 Suite through keylogging login credentials, the hacker was able to send more secure, tailored

emails to other employees in the department, inviting them to sign up for a pilates class at a local gym where many employees have memberships. Through the second phishing campaign, the hacker was able to use the same RAT malware to gain viewing access to other employees in the business department. By the end of the phishing campaign, the hacker was able to gain access to 30 employee machines; being able to control roughly 50% of employee machines in the Newark NJDOL network through similar RAT software without employees knowing. Through keylogging and password reuse, the hacker was able to gain access to 90% of employee Outlook accounts and access to restricted servers. The reused login credentials across personal and professional accounts allowed the attacker to bypass multi-factor authentication (MFA) where it was improperly configured or even non-existent. By combining these techniques, the hacker could exploit and escalate privileges, move between departments, and ultimately gain access to the unemployment insurance server.

IV. Attack on Unemployment Insurance Sever

A. As aforementioned, the hacker was looking to target the unemployment insurance network; crashing the network for a certain period of time so people could not claim their checks. NJDOL unemployment insurance checks come on the first of every month at precisely 0800; claimants can log into the OpenAM portal through the NJDOL website and claim their checks. The hackers' goal was to bring the login server down for a certain amount of time to prevent users from claiming their checks. On June 1st at approximately 0030, from the controlled botnet, the hacker was able to deploy a SYN flood attack where the IP addresses of the

machines were spoofed to be mismatched (ie. machines IP addresses on the botnet were mismatched to come from different machines on the same network). Specifically, as part of the three-way TCP handshake process, a large and continuous amount of SYN packets were sent to the front-end web server that hosted the login page, targeting the HTTPS port number 443. The server was responding to the request by sending SYN-ACK packets but never received the final ACK packet to complete the connection request. Due to the server waiting for a final ACK packet as well as responding to the continuous SYN, the server remained open and was consuming resources. This led to the crashing of the web server due to half open TCP connections and an overconsumption of resources due to waiting and response time.

V. Firewall Misconfiguration Causing Server Collapse

A. Firewalls are an essential piece to every network as they are the entity that permits or denies requests that try to access a specific server or network. At its core, a firewall consists of a set of predetermined rules that filters which traffic is permitted and which traffic is blocked. The rules are determined by each organization. In the case of this attack, the hacker was able to exploit a small loophole within the existing firewall to conduct a SYN flood attack. The firewall used by NJDOL allowed any and all internal network traffic; essentially any source IP address that was within the organization's IP realm was permitted to participate in the TCP/IP connection. Additionally, the firewall only restricted the number of outside open TCP connections; if a certain number of out-of-network connections were left open/no ACK packets were sent back, the server would

"drop" those connections and respond to other requests. With little to no restrictions on requests sent from IP addresses within the NJDOL network, the hacker was able to bypass the misconfigured firewall and overwhelm the web server with SYN requests and eventually crash the login page.

VI. Analysis

A. One of the biggest problems that allowed the hacker to move laterally throughout the network was poor password management. After a comprehensive analysis of each employee's username and password combinations to enter both professional and personal accounts, it showed that employees commonly used the same passwords for both types of accounts. As aforementioned, the hacker was able to use a simple gym membership login to get into employee work accounts and access the organizations' Microsoft Suite. Password reuse is a common occurrence among the general public and one of the main human risks/behaviors that contribute to common security breaches. Having a secure password manager for employees to manage their credentials for all platforms that require login credentials as well as enforcing password resets every six months to a year is an important way for an organization to strengthen their credential validations. Additionally, the NJDOL systems were configured to use the industry standard but slightly weaker AES-128 symmetric encryption algorithm for securing internal communication. AES-128 or Advanced Encryption Standard using 128 bits was the underlying symmetric encryption used for protecting session data. The use of AES-128 over AES-256 could have exposed the organization to more brute-force attacks and allowed for the circumventing of existing cryptographic

protocol. This further allowed the hacker to move laterally throughout the network by being able to decrypt sensitive communication or extract important data, such as login credentials. The combination of password reuse and weak encryption allowed the hacker to gain easy access into the system.

VII. Phishing Prevention

A. As it is the case with most cyber attacks, the entryway into the NJDOL network and the deployment of malware was made possible through the massive phishing campaign and the high human risk exhibited by the amount of employees susceptible to believing phishing emails. The first plan of action to try and prevent something of this scale from happening again would be to create employee phishing training to educate employees on the signs of a phishing email and encourage speaking with colleagues regarding the validity of an email. Although not an immediate prevention, the NJDOL cybersecurity department can deploy fake phishing emails to actively test employees and their vigilance on identifying a phishing campaign. How it would work: whichever employees click on links sent via the phishing emails sent out by the cybersecurity department will have to go through mandatory training. This will help to create a sense of awareness and weariness among employees when clicking on suspicious links and emails.

VIII. Prevention for Networks

A. If the front-end login server is to remain on the network, something that can be implemented to protect the server in a more offensive way rather than defensive would be to make use of honey tokens or honey pots. Both concepts are essentially used to entice and trap hackers and notify IT administration of a

hackers' movement throughout their network. One idea would be to place a honey pot disguised as the front-end login server or any server that is of value to an organization; this would notify NJDOL IT admin that there is an attacker within their network. Additionally, placing honey tokens disguised as email addresses and database data can also mark and entrap hackers. Alternatively, a more immediate solution to prevent a hacker's access to an important server that may be eye catching to a hacker would be to remove it from the network. The safest place to put apps and servers would be to host them via the cloud; using some sort of cloud provider such as Amazon Web Services or Microsoft Azure. By removing the servers from the network and onto the cloud, no matter how laterally the hacker moves through the network or is able to take or crash down the network in some way, the server won't be connected to the network, making it inaccessible to the hacker. Similarly, using a honey pot server residing on the network in addition to cloud migration is a good way to combine defensive and offensive techniques for maximum security. In addition to training and cloud migration, NJDOL could benefit from switching existing encryption protocol from AES-128 to AES-256. Although AES itself was approved and became the standard back in 2001, AES-256 is proven to be superior to its counterpart as it uses a much larger key value (in this case 256 bits), generating more combinations to encrypt and decrypt blocks of data. By using larger key values, AES-256 makes encryption much harder to break, offering much better protection against brute-force attacks. Additionally, in the wake of quantum computing and the ultimate rise of quantum attacks, some studies have shown that making the

switch to AES-256 would prove to be effective in circumventing these new attacks.

IX. Firewall Protection

A. The loophole within the existing firewall additionally allowed for the SYN flood attack, bringing down the front-end login server. By switching over a more costly but more secure implementation called a WAF (Web Application Firewall), it can help to better filter incoming requests. WAF's are designed to monitor, filter and block any incoming HTTP or HTTPS traffic by looking "inside" web traffic, such as analyzing URLs and API calls. WAFs can work better than traditional firewalls as they can detect and filter any and all incoming traffic, regardless of whether it comes from inside or outside the network. Additionally, it will filter the number of HTTP traffic and detect abnormal traffic patterns, such as a high amount of SYN packet connection requests.

X. Network Diagram:

A. Below is a network diagram and how the hacker was able to deploy a botnet of internal machines to bring down the unemployment insurance server.

Network Diagram: