**Group 3 Project Report**

**IS 4893**

*Jacob Corder*

*Avery Scarsella*

*David-Jeremiah Barza Lim*

*Ngenge Nfor*

*Jeremiah Poblete*

*Caleb Villarreal*

**Background**

In this report, we will be discussing a complex spear phishing[[1]](#footnote-1) attack that occurred on December 22nd, 2024. The target of this attack was a prominent airline organization known as Unite Airlines. The attack targeted C-suite executives who work out of the corporate offices in Dallas, Texas in an effort to obtain information.

After successfully gaining access to an executive’s credentials, the unknown hacker group was able to escalate privileges, setup backdoor access, and utilized File Transfer Protocol (FTP) to exfiltrate flight data and customer information (credit card data, flight records, etc.) over a period of 24 hours.

Finally, after records were taken, the attackers took over the flight data for the holiday season, encrypted the data with a ransomware attack, shut down flight servers, and requested that the airline company pay an undisclosed amount to have their systems restored.

**Network Topology**

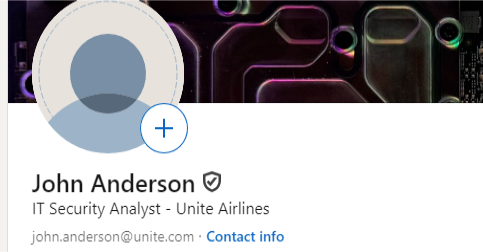
**A diagram of a computer network

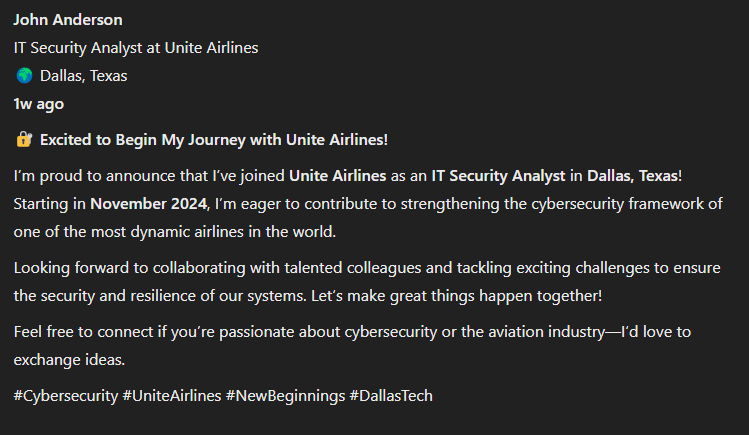
Description automatically generated**

Unite Airlines uses a system of three servers which house all proprietary information. These networks are known as the corporate network, customer data server and flight data server. The attackers spear phishing campaign was targeted at not only C-Suite executives but also happened to attack an executive on the 10.15.4.00 subnet. The above network topology was crafted to display the way in which the victims have compartmentalized their network. Despite this compartmentalization, the blaring vulnerability of human error was the one that the hackers targeted.

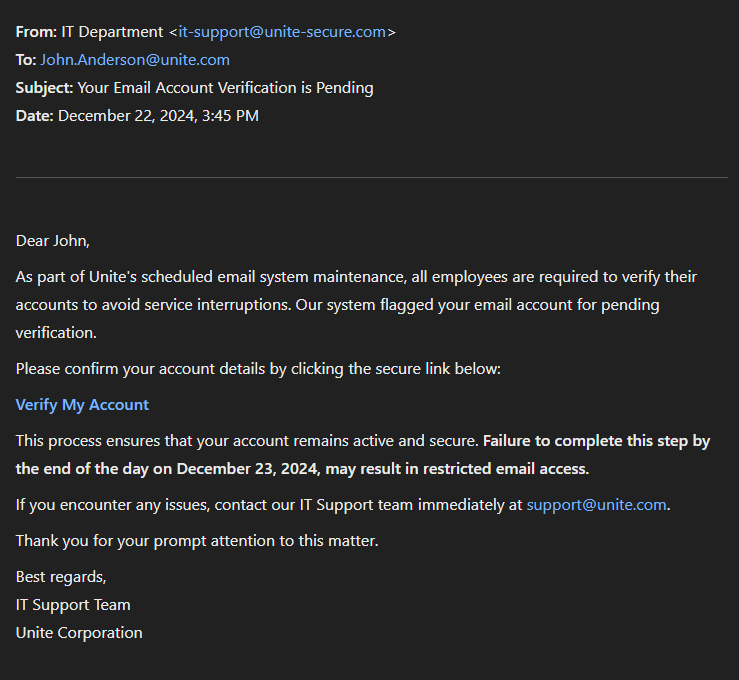
**Breach Analysis**

Access to Unite Airlines’ system was achieved through a targeted spear-phishing attack (T1566.002, MITRE ATT&CK). Using the Social Engineering Toolkit (SET) a crafted email was designed to impersonate the Unite Airlines Security Team, making it appear legitimate and trustworthy. By leveraging social engineering techniques, detailed information was obtained about John Anderson. Using LinkedIn, they identified his job title, email address, and a post announcing his start date with the company. This information allowed us to tailor the phishing email to increase its credibility and deceive the target.





John Anderson was an ideal candidate for a spear-phishing attack based on the information gathered in the reconnaissance phase. By leveraging the information gathered, we are able to increase the likelihood of the target clinking the embedded malicious link. The link contained in the email executes a payload designed to compromise the user system. The payload successfully revealed the users IP address is 10.15.4.255, and enabled port 3389. This port allows communication that will allow us to remotely control the compromised system providing an entry point for further exploitation.



Once his account was successfully accessed, the team escalated their user privileges by bypassing the user account controls (TA0004.002, MITRE ATT&CK) obtaining administrative access. As soon as they had access to the target systems, they proceeded to utilize their data exfiltration protocols (T1011.001, MITRE ATT&CK) to steal customer information, valuable flight data, and more. Lastly, they uploaded malware to their targeted servers to perform a denial-of-service malware attack, grounding their systems.

**Initial Access & Techniques**

Prior to the events of December 22nd, the attackers utilized several different methods to gain initial access. The timeline of events is as follows:

* Attackers utilized LinkedIn’s search feature, scanning for potential targets that may be susceptible to a phishing email. The main factors they used in determining their targets were age, organizational seniority, and position information.
* Once they had gained access to their victim’s domain, they utilized said access to scan for administrator accounts and spread to other compromised accounts (Anderson, 2024).
* Once credentials had been obtained, they utilized various connection methods, most notably RDP through a virtual machine, in order to access their target machine on the IP address 10.15.4.225 (Anderson, 2024).
* Once inside, they were able to disable Windows Defender using SystemAdminsFlows.exe, start network mapping, and used NETSCAN.EXE for internal reconnaissance to gain a better understanding of the network topology and prepare for data exfiltration (Anderson, 2024).

**Attacker Techniques**

In this section we will be discussing the various attack techniques that the attackers used in the process of the breach.

* Scan the domain of the airport for admin accounts (Anderson, 2024).
* Phishing email/credential harvester targeting the corporate network after the reconnaissance phase has taken place.
* Utilize RDP to move laterally through systems and test network connections for further movement (Anderson, 2024).
* Use SystemSettingsAdminFlows.exe to disable Windows Defender (Anderson, 2024).
* From there, move through the system to systematically infected systems based on priorities.
* Priority 1 will be PCs connected to the switches and routers for daily operations so the ransomware can be deployed.
* Use WMIC (Windows Management Instrumentation) to deploy the ransomware to the targeted machines (Anderson, 2024).
* Priority 2 will be any other servers connected to the network map, like customer data servers and flight data servers for data exfiltration if the ransom is not met. The data will be stolen and encrypted to aid in extortion.
* Move data to 7-Zip and WinRAR to archive the collected data for extortion before the data is exfiltrated (Anderson, 2024).
* Use cmd.exe to launch the payloads (Anderson, 2024).

Below are screenshot artifacts taken at the time of attack, displaying the different commands that were used to gain access:

A screenshot of a computer program

Description automatically generated A computer screen shot of a computer

Description automatically generated

**Impacted Systems**

The first system that was affected by the attack was mainly linked to the corporate network on 10.15.5.1. This network contained a large amount of information regarding corporate credentials and proprietary organizational data. It was believed that the attackers targeted this network so that they could gain access to the other networks and setup a backdoor access for later use.

Once the attackers gained access to the main corporate network, they used their upgraded privileges to laterally switch to 10.15.4.1. This switch allowed them to access the router at 10.15.3.1 and connect to adjacent devices on the network now masked as regular network traffic. Their reasoning for linking to the router and masking themselves as natural network traffic was not only to infect the other systems that connect to these access points, but to also infect and access their main targets: the customer data on server 10.15.7.1 and the flight data on server 10.15.6.1.

Once they gained access to the systems, they then were able to exfiltrate the data to a secure location and spread their ransomware across all 3 main servers. This is what led to the shutdown of flight plans for the organization which led to a grounding of all flights for the holiday weekend until the attack’s remediation.

A diagram of a computer network

Description automatically generated

**Impacted Data**

In this section we will be covering the data that was impacted because of the attack. For the most part, since the incident most of the information has been accounted for. Though, in this report, it is important to account for all impacted services regardless of its current state.

Most of the data that was impacted was customer data with over 20,000 pieces of Personally Identifiable Information being sent to the attackers. This information included credit card data, customer names, flight information, and more. Additionally, important internal information such as flight server and operation data were either locked behind ransomware or sent to the attackers. All organizational information from the corporate, flight, and customer networks became free reign for the attackers. Not to mention that all operations were locked behind ransomware until ransomware remediation and/or payment.

Below is a screenshot of the ransomware screen that was seen by those on the network:

A screenshot of a computer

Description automatically generated

Lastly, below is a screenshot of the information that was taken by the attackers, showcasing the information that was taken by the attackers:

A screenshot of a computer

Description automatically generated A screen shot of a computer

Description automatically generated

**Containment Measures**

Immediately after Unite Airlines realized that they had been attacked, they segmented the various networks from one another. This isolated each sever by disconnecting their network access, effectively disabling the attackers from accessing their systems via a network connection. Once segmentation of the networks was complete, they proceeded to quarantine key systems such as their Airline Data Gateways[[2]](#footnote-229) (ADG), Central Reservation System[[3]](#footnote-21479) (CRS) and other inventory management systems.

Additionally, while isolating their systems, they discovered that many accounts on the corporate network were compromised. There IS team manually disabled each of the compromised accounts to both contain and locate which account the initial access point could be attributed to.

Lastly, after continued investigation, they shut down all three networks and halted PC operations. Since the infiltration was so widely spread and deeply engrained within the organization, shutting down the box was necessary as it halted any additional malware from being brought into their systems. It also allowed their security team to begin patch management and investigation on the closed network.

**Remediation and Recovery**

After the discovery and containment of the unfortunate breach of the Unite Airlines network, their IS team began working towards creating a safer network for their users. They first cleared all the current usernames and passwords of their executives and required each one to create a new version of both items. They additionally equipped all C-Suite executives with company phones equipped with MDM[[4]](#footnote-12258) software and two factor authentication processes to both monitor and verify their identities.

In addition to this, Unite Airlines implemented a traffic filtration system which documented all packets that passed through the network. This, coupled with their training of new employees in deep packet inspection, the addition of an email filtration system (with assigned employee emails), and installation of both and IPS and IDS worked to create a safer environment for both customer and corporate data.

With the security of their data now ensured, they restored all customer data after patching all of the bugs that were discovered during the containment process and scrubbed their network clean. They lastly have placed a port management software with in-built intrusion detection software on the network to monitor port traffic (which was the main reason attackers were able to connect) and notify those in charge of any abnormalities.

Lastly, to recover from their brand image, they offered free flight credits to all impacted customers and full refunds on any flights booked within the time of the attack. They also now periodically hire a red team to pen-test their system monthly to ensure they are up to date and secure.

**Conclusion**

In conclusion, on December 22nd, 2024, Unite Airlines was infiltrated by a group of attackers by utilization of a spear-phishing attack. Once the organization was infiltrated, the attackers accessed their corporate network and scanned for compromised administrative accounts using RDP to connect and NetScan to execute their objective.

They escalated their privileges, exfiltrated vital organizational and customer data, and effectively shut down said with a ransomware attack. This attack grounded several flights for the holiday season, interrupted air travel across the country, and is widely known as one of the worst airline attacks in history

It is important to not only to recognize the success of the attackers, but also the faults of the organization. Many of their employees were not trained against recognizing phishing emails, which is what lead to one such individual being compromised. Additionally, they had a network that did not discriminate against its users access privileges and allowed for the hackers to roam freely once they gained access.

While they were able to recover and learn from this experience, they also learned a valuable lesson in the importance of mitigating human error. Had they had a proper email filtration system, port monitoring/management system, and other technologies to minimize access and recognize risk, they would have been able to avoid such a widespread loss of data and customer trust.

**References**

Anderson, M. (2024, June 1). INC Ransom. Attack.Mitre.org. Retrieved December 1, 2024, from https://attack.mitre.org/groups/G1032/

Basan, Maine. “Spear Phishing Prevention: 10 Ways to Protect Your Organization.” eSecurity Planet, 23 Aug. 2023, https://www.esecurityplanet.com/networks/how-to-prevent-spear-phishing-attacks/.

Aircraft Data Gateway. https://aerospace.honeywell.com/us/en/products-and-services/product/services/maintenance-and-service-plans/aircraft-data-gateway. Accessed 4 Dec. 2024.

“Flight Booking Process: Airline Reservation, Ticketing, And.” AltexSoft, https://www.altexsoft.com/blog/flight-booking-process-structure-steps-and-key-systems/. Accessed 4 Dec. 2024.

Hewitt, Nik. “Eight Ransomware Containment Best Practices • TrueFort.” TrueFort, 9 Aug. 2023, https://truefort.com/ransomware-containment/.

Cichonski, Paul, et al. Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. NIST SP 800-61r2, National Institute of Standards and Technology, Aug. 2012, p. NIST SP 800-61r2. DOI.org (Crossref), https://doi.org/10.6028/NIST.SP.800-61r2.  
  
“What Is Mobile Device Security?” ThreatDown by Malwarebytes, 12 Apr. 2024, https://www.threatdown.com/glossary/what-is-mobile-device-security/.

**Generative AI was used in the report to create the artifact screenshots**

1. Spear-phishing is a method of phishing in which a large amount of emails are sent to specific targets in order to gain access to secure systems [↑](#footnote-ref-1)
2. Airline Data Gateways are the systems that airlines use to load software and read the real time flight data on aircrafts [↑](#footnote-ref-229)
3. Central Reservation Systems are software that airline companies utilize to save customer data, flight records, and more. [↑](#footnote-ref-21479)
4. MDM stands for Mobile Device Mangement, which is a software that allows a company to monitor mobile devices that are linked to their network [↑](#footnote-ref-12258)