**JLA Phishing Attack**

**ISSC455 Digital Forensics:**

**Investigation Procedures and Response**

**Jon Nelson**

**Professor Tawalbeh**

**19 Feb 2022**

**Case Number: ISSC455-20-000X**

A sign in front of a building

Description automatically generated

**Documents Properties**

|  |  |
| --- | --- |
| Title | ISSC455-20-000X Forensic Report |
| Version | 1.0 |
| Authors | Jon Nelson |
| Reviewed By | Loai Tawalbeh |
| Approved By | Loai Tawalbeh |
| Classification | Confidential: For Educational Purposes Only |

**Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Authors | Description |
| 1.0 | 19 Feb 2022 | Jon Nelson | Final Draft |

**Disclaimer**

The information contained in this report, APUS ISSC455 Report JLA Phishing Attack, is intended for training and learning purposes only and is not for the purpose of providing digital forensic investigation recommendations. The scenario leading to this report is provided by Shanken Security Solutions and has been approved for use as Education Purposes Only. If this report is found, please delete, shred (if hardcopy) or report to [classroomsupport@apus.edu](mailto:classroomsupport@apus.edu) for further instructions if delete or shred are not available.

APUS AND PROFESSOR JOHNNY JUSTICE DISCLAIM ALL LIABILITY AND RESPONSIBILITY FOR ANY ERRORS OR OMISSIONS IN THE CONTENT CONTAINED IN THIS REPORT.

Contents

[Table of Figures 4](#_Toc96365233)

[1.0 Scope 6](#_Toc96365234)

[**1.1 Purpose** 6](#_Toc96365235)

[**1.2 Team Overview** 6](#_Toc96365236)

[**1.3 Executive Summary** 6](#_Toc96365237)

[2.0 Narrative 7](#_Toc96365238)

[3.0 Findings 8](#_Toc96365239)

[**3.1 Quick View** 8](#_Toc96365240)

[**3.2 Email 1: Sabre Project - October 15, 2019 - 1938 hours** 9](#_Toc96365241)

[**3.4 JLAENTREPRISE.com Domain Created - October 15, 2019 - 2054 hours** 12](#_Toc96365242)

[**3.6 Email 4: Sabre Project - October 16, 2019 - 0653 hours** 14](#_Toc96365243)

[**3.7 Email 5: Sabre Project - October 17, 2019 - 1123 hours** 16](#_Toc96365244)

[**3.8 Email 6: JLA Enterprise and Sabre Project - October 17, 2019 - 1209 hours** 18](#_Toc96365245)

[**3.10 Email 8: Sabre Project - October 17, 2019 - 1337 hours** 20](#_Toc96365246)

[**3.11 Email 9: JLA Enterprise and Sabre Project - October 17, 2019 - 1431 hours** 22](#_Toc96365247)

[**3.12 Email 10: Sabre Project Wiring Instruction - October 17, 2019 – 1443 hours** 23](#_Toc96365248)

[**3.13 Email 11: Sabre Project Wire Transfer - October 17, 2019 - 1445 hours** 24](#_Toc96365249)

[**3.14 Email 12: Sabre Project Wire Transfer - October 17, 2019 - 1459 hours** 25](#_Toc96365250)

[**3.15 Email 13: Sabre Project Wiring Instruction - October 17, 2019 - 1506 hours** 28](#_Toc96365251)

[**3.16 Email 14: Sabre Project Wire Transfer - October 17, 2019 - 1542 hours** 29](#_Toc96365252)

[4.0 Conclusion 31](#_Toc96365253)

[**4.1 Email 1: - June 01, 2019 - 0710 hours** 31](#_Toc96365254)

[**4.2 Email 2: - August 02, 2019 - 1808 hours** 32](#_Toc96365255)

[5.0 Recommendations 33](#_Toc96365256)

[Appendix A: Wiring Instructions (Fraudulent EAST HUN CHIU Account) 34](#_Toc96365257)

# **Table of Figures**

[Figure 1 - Email 1 - Michael SCOTT to Jim Halpert (Start of Phishing Attempt) 10](#_Toc43544352)

[Figure 2 - jimhalpert@jlaenterprise.com auto-forwards to officeman1987a@gmail.com and SCOTT’s IPv6 address 10](#_Toc43544353)

[Figure 3 - IPv6 Geographical Location - 2601:98a:100:57b:206f:26a1:323a:fb5c 11](#_Toc43544354)

[Figure 4 - jimhalpert@jlaenterprise.com auto-forwards to officeman1987a@gmail.com and SCOTT’s IPv4 address 12](#_Toc43544355)

[Figure 5 - IP Address Lookup Details - 83.110.250.231 12](#_Toc43544356)

[Figure 6 - IPv4 Geographical Location - 83.110.250.231 13](#_Toc43544357)

[Figure 7 - Email 2 - Michael SCOTT to Jim Halpert (Covering Mistake) 13](#_Toc43544358)

[Figure 8 - MX Query - JLAENTREPRISE.COM 14](#_Toc43544359)

[Figure 9 - Whois Information (jlaentreprise.com) 14](#_Toc43544360)

[Figure 10 - IP Geographical Location - 50.63.202.52 (jlaentreprise.com) 15](#_Toc43544361)

[Figure 14 - IP Address Lookup Details - 23.239.21.243 19](#_Toc43544365)

[Figure 15 - IPv4 Geographical Location - 23.239.21.243 19](#_Toc43544366)

[Figure 16 - Email 4 - Jim Halpert (Counterfeit Account) to Dwight Schrute (Phishing Attempt) 20](#_Toc43544367)

[Figure 17 - jhalpert@jlaentreprise.com used an IPv4 address from a location previously used by SCOTT’s email account 21](#_Toc43544368)

[Figure 18 - IPv4 Geographical Location - 83.110.250.20 21](#_Toc43544369)

[Figure 19 - Email 5 - Jim Halpert (Counterfeit Account) to Michael SCOTT and Dwight Schrute (Confirm Payment) 22](#_Toc43544370)

[Figure 20 - abernard@jlaenterprise.com auto-forwards to andybernard@abcglobal.com 23](#_Toc43544371)

[Figure 21 - IPv4 Geographical Location - 192.155.90.47 23](#_Toc43544372)

[Figure 22 - Email 6 - Dwight Schrute (Counterfeit Account) to Andy Bernard and Jim Halpert (Legitimacy) 24](#_Toc43544373)

[Figure 23 - jhalpert@jlaentreprise.com to dwightschrute68@gmail.com 25](#_Toc43544374)

[Figure 24 - Email 7 - Jim Halpert (Counterfeit Account) to Dwight Schrute (Correspondence over Email) 25](#_Toc43544375)

[Figure 25 - Email 7 - Jim Halpert (Counterfeit Account) to Dwight Schrute (Correspondence over Email) (continued) 26](#_Toc43544376)

[Figure 26 - abernard@jlaentreprise.com to dwightschrute68@gmail.com and nee.beesly@gmail.com 27](#_Toc43544377)

[Figure 27 - Email 8 - Andy Bernard (Counterfeit Account) to Dwight Schrute and Pam Beesly 28](#_Toc43544378)

[Figure 28 - Email 9 - Dwight Schrute (Counterfeit Account) to Andy Bernard (Establishing Legitimacy) 29](#_Toc43544379)

[Figure 29 - abernard@jlaenterprise.com auto-forwards to andybernard@abcglobal.com 30](#_Toc43544380)

[Figure 30 - IPv4 Geographical Location - 173.230.128.135 30](#_Toc43544381)

[Figure 31 - Email 10 - Dwight Schrute (Counterfeit Account) to Andy Bernard (Wiring Instructions) 30](#_Toc43544382)

[Figure 32 - X-Originating-IP: 192.81.133.156 (Mail Server in California) 31](#_Toc43544383)

[Figure 33 - IPv4 Geographical Location - 192.81.133.156 31](#_Toc43544384)

[Figure 34 - Email 11 - Dwight Schrute (Counterfeit Account) to Andy Bernard (Wire Transfer) 31](#_Toc43544385)

[Figure 35 - X-Originating-IP: 45.33.17.101 (Mail Server) 32](#_Toc43544386)

[Figure 36 - IPv4 Geographical Location - 45.33.17.101 32](#_Toc43544387)

[Figure 37 - Email 12 - Dwight Schrute (Counterfeit Account) to Andy Bernard (Wire Transfer Second Email) 33](#_Toc43544388)

[Figure 38 - Email 12 - Dwight Schrute (Counterfeit Account) to Andy Bernard (Wire Transfer Second Email) (continued) 34](#_Toc43544389)

[Figure 39 - X-Originating-IP: 83.110.250.20 35](#_Toc43544390)

[Figure 40 - Email 13 - Jim Halpert (Counterfeit Account) to Pam Beesly (Real Account) (Signed by Dwight Schrute) 35](#_Toc43544391)

[Figure 41 - X-Originating-IP: 23.239.21.244 36](#_Toc43544392)

[Figure 42 - IP Address Lookup Details - 23.239.21.244 36](#_Toc43544393)

[Figure 43 - Email 14 - Dwight Schrute (Counterfeit Account) to Andy Bernard (abcglobal.com email) 37](#_Toc43544394)

[Figure 44 - X-Originating-IP: 83.110.250.232 38](#_Toc43544395)

[Figure 45 - IPv4 Geographical Location - 83.110.250.232 38](#_Toc43544396)

[Figure 46 - IP Address Lookup Details - 83.110.250.232 39](#_Toc43544397)

[Figure 47 - Email 15 - Jim Halpert (Counterfeit Account) to Dwight Schrute (Real Account) 39](#_Toc43544398)

[Figure 48 - Email 15 - Jim Halpert (Counterfeit Account) to Dwight Schrute (Real Account) (continued) 40](#_Toc43544399)

[Figure 49 - Jim Halpert (Real Account) to Kevin Malone about Phishing Scam 41](#_Toc43544400)

[Figure 50 – IPv6 Geographical Location - 2601:98a:100:57b:206f:26a1:323a:fb5c 42](#_Toc43544401)

[Figure 51 - IP Geographical Location – 23.239.21.243 43](#_Toc43544402)

[Figure 52 - IPv6 Geographical Location - 2601:98a:100:57b:206f:26a1:323a:fb5c 43](#_Toc43544403)

# **1.0 Scope**

## **1.1 Purpose**

The purpose of this investigation is to determine who and how they were able to phish wiring instructions for 2.3 million dollars from JLA Enterprise and how it can be mitigated in the future.

## **1.2 Team Overview**

The following APUS team members were assigned to conduct the secondary analysis on the report findings provided by Dr. Kevin Malone:

|  |  |
| --- | --- |
| Team Role | Name |
| Chief Consultant | Loai Tawalbeh |
| Chief Cyber Security Researcher | Jon Nelson |
| Senior Cyber Security Researcher | Johnny Justice |
| Senior Cyber Security Researcher | Liam Nesson |

Table 1 - Team Overview

## **1.3 Executive Summary**

APUS was asked to investigate a phishing attempt on JLA Enterprise for 2,300,000 dollars to an East Hun Chiu trading account from current and former contractors for JLA Enterprise. Evidence revered includes emails from legitimate and fake accounts set up by the attacker. There were over 15 emails that were exchanged between the parties

# **2.0 Narrative**

On October 15, 2019 , at 1938 hours, Michael SCOTT (Managing Partner, DSS Venture Partners LTD and former consultant to JLA Enterprise) accidentally sent an email to Jim Halpert (General Manager, JLA Enterprise) at jhalpert@jlaenterprise.com to confirm JLA Enterprise requested 2.3M from an East Hun Chiu based company, who was investing in JLA Enterprise research through Dwight Schrute (former subcontractor to DSS Venture Partners LTD and current Business Partner and Investor in JLA Enterprise). The money was to be transferred to JLA Enterprise’s East Hun Chiu trading account upon closing. SCOTT requested the wire instructions and said HE would forward them to HIS business partner Dwight Schrute.

At 1947 hours, SCOTT identified HIS mistake and replied to HIS original email at 1938 hours to explain HE wrote Jim Halpert in error. Within the email, HE mentioned that Dwight Schrute wrote to SCOTT and the account is being set up to wire to JLA Enterprise. At 2054 hours, the counterfeit domain jlaentreprise.com was registered with GoDaddy.com, LLC. At hours 1445, SCOTT sent an email chain to Dwight Schrute containing an email discussion related to the wire transfer of 2.3M to an East Hun Chiu Bank and two individuals who will manage the account ( Pam Beesly and Dwight Schrute).

On October 16 2019, at 0653 hours, SCOTT sent an email from HIS counterfeit Jim Halpert (officeman1987a@gmail.com) account to Dwight Schrute and Pam Beesly. The counterfeit email was designed to appear as if Jim Halpert was telling Dwight Schrute that HE (as Jim Halpert) discussed with Michael (SCOTT), that JLA Enterprise will need to transfer 2.3M to an East Hun Chiu trading account. SCOTT also attached wiring instructions

On October 17, 2019, at 0237 hours, JLA Enterprise personnel identified the counterfeit domain triggering an internal investigation and seeking external professional assistance. At 1123 hours, SCOTT sent an email response from HIS counterfeit Jim Halpert account to SCOTT’s and Dwight Schrute’s legitimate email accounts, while sending a carbon copy to the counterfeit Jim Halpert email address (officeman198a7@gmail.com). SCOTT’s original email sent at 0534 hours, questioned if the East Hun Chiu bank routing number was in place and if the transfer would be completed by Friday or Monday when the bank was open. SCOTT’s fraudulent response thanked HIMSELF and asked if the transfer of $2.3M USD would come in a one-time transfer since they had waited a long time for the money.

On October 17, 2019, at 1209 hours, SCOTT sent another counterfeit email, however this time posing as Dwight Schrute (dwightschrute68@gmail.com) with the goal of establishing further legitimacy for the wire transfer. The email addressed to Andy Bernard (CEO and Founder of JLA Enterprise) and Jim Halpert stated Dwight Schrute’s company now runs the East Hun Chiu investor, since the DSS contract with JLA Enterprise had already expired. At 1325 hours, SCOTT sent an email to Dwight Schrute from HIS counterfeit Jim Halpert email account. The email contained information regarding the money transfer and expressed to maintain contact with him directly.

On October 17, 2019, at 1337 hours, SCOTT sent another counterfeit email, however this time posing as Andy Bernard (abernard@jlaentreprise.com) addressed to Dwight Schrute’s and Pam Beesly’s legitimate email accounts while sending a carbon copy to HIS counterfeit Jim Halpert email address (jhalpert@jlaentreprise.com). SCOTT (as Andy Bernard) stated he would read all the emails again and provide an answer later that day. However, he (as Andy Bernard) asked Dwight Schrute to acknowledge the new wiring instructions as confirmed by Jim Halpert. He asked Dwight Schrute to work directly with him (Jim Halpert) on the project. At 1431 hours, SCOTT sent a second email to Andy Bernard from HIS counterfeit Dwight Schrute email account with hopes of Andy Bernard approving the wire transfer to Dwight Schrute. SCOTT’s fraudulent email stated that SCOTT was becoming a nuisance by emailing and texting via WhatsApp 2 to 3 times a day asking for the progress of the money transfer. SCOTT was attempting to convince Andy Bernard that he (Dwight Schrute) would still pay SCOTT even though on past contracts, HE did not perform appropriately by Dwight Schrute.

# **3.0 Findings**

## **3.1 Quick View**

The table below is designed to provide a quick view of all the identified findings Each link will take you to the section with a detailed report of the findings.

|  |  |
| --- | --- |
| # | Findings Title |
| 3.2 | [Email 1: Sabre Project - October 15, 2019 - 1938 hours](#_3.2_Macau_-) |
| 3.3 | [Email 2: Sabre Project - October 15, 2019 - 1947 hours](#_3.3_Re:_Macau) |
| 3.4 | [JLAEntreprise.com Domain Created - October 15, 2019 - 2054 hours](#_3.4_JLAENTREPRISE.com_Domain) |
| 3.5 | [Email 3: Sabre Project - October 15, 2019 - 2258 hours](#_3.5_Fw:_Macau) |
| 3.6 | [Email 4: Sabre Project - October 16, 2019 - 0653 hours](#_3.6_Re:_Macau) |
| 3.7 | [Email 5: Sabre Project - October 17, 2019 - 1123 hours](#_3.7_Re:_Macau) |
| 3.8 | [Email 6: JLA Enterprise and Sabre Project - October 17, 2019 - 1209 hours](#_3.8_Flow_Pharma) |
| 3.9 | [Email 7: Sabre Project - October 17, 2019 - 1325 hours](#_3.9_Re:_Macau) |
| 3.10 | [Email 8: Sabre Project - October 17, 2019 - 1337 hours](#_3.10_Re:_Macau) |
| 3.11 | [Email 9: JLA Enterprise and Sabre Project - October 17, 2019 - 1431 hours](#_3.11_Flow_Pharma) |
| 3.12 | [Email 10: Sabre Project Wiring Instruction - October 17, 2019 – 1443 hours](#_3.12_Re:_Wiring) |
| 3.13 | [Email 11: Sabre Project Wire Transfer - October 17, 2019 - 1445 hours](#_3.13_Wire_Transfer) |
| 3.14 | [Email 12: Sabre Project Wire Transfer - October 17, 2019 - 1459 hours](#_3.14_Re:_Wire) |
| 3.15 | [Email 13: Sabre Project Wiring Instruction - October 17, 2019 - 1506 hours](#_3.15_Re:_Wiring) |
| 3.16 | [Email 14: Sabre Project Wire Transfer - October 17, 2019 - 1542 hours](#_3.16_Re:_Wire) |
| 3.17 | [Email 15: Sabre Project Wiring Instruction - October 19, 2019 - 1202 hours](#_3.17_Re:_Wiring) |
| 3.18 | [Phishing Scam Sent to JLA Enterprise Consultant - October 19, 2019 - 2233 hours](#_3.18_Phishing_Scam) |

## **3.2 Email 1: Sabre Project - October 15, 2019 - 1938 hours**

A close up of a tree

Description automatically generated

Figure 1 - Email 1 - Michael SCOTT to Jim Halpert (Start of Phishing Attempt)

A picture containing knife, table

Description automatically generated

Figure 2 - jimhalpert@jlaenterprise.com auto-forwards to officeman1987a@gmail.com and SCOTT’s IPv6 address

A screenshot of a cell phone

Description automatically generated

Figure 3 - IPv6 Geographical Location - 2601:98a:100:57b:206f:26a1:323a:fb5c

**3.3 Email 2: Sabre Project - October 15, 2019 - 1947 hours**

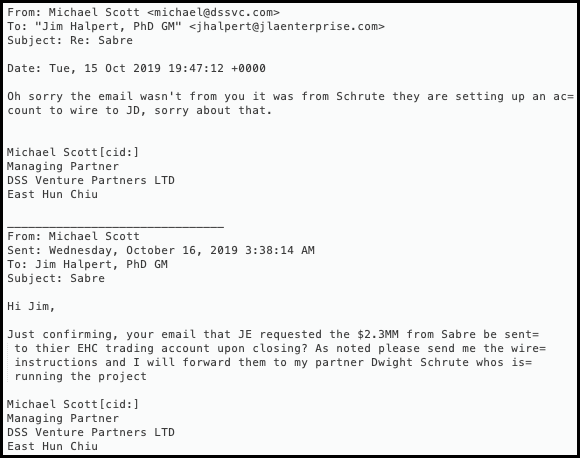


Figure 4 - jimhalpert@jlaenterprise.com auto-forwards to officeman1987a@gmail.com and SCOTT’s IPv4 address

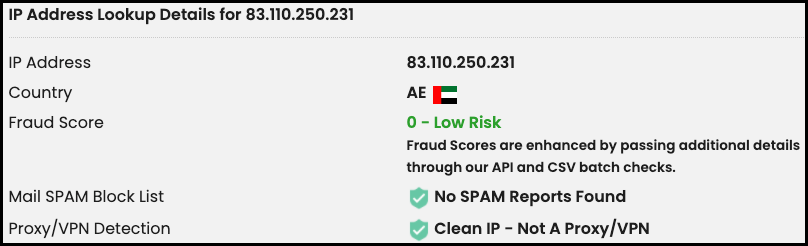


Figure 5 - IP Address Lookup Details - 83.110.250.231



Figure 6 - IPv4 Geographical Location - 83.110.250.231

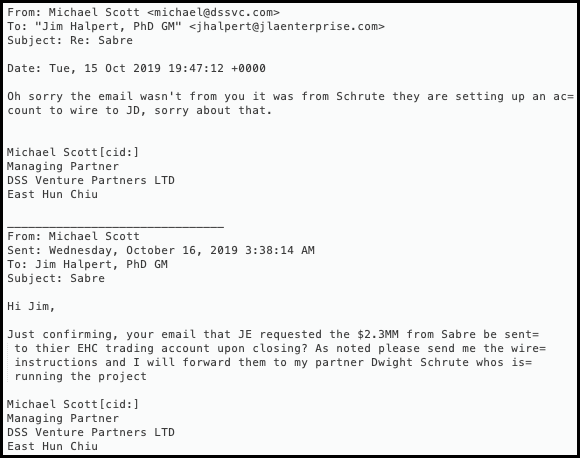


Figure 7 - Email 2 - Michael SCOTT to Jim Halpert (Covering Mistake)

## **3.4 JLAENTREPRISE.com Domain Created - October 15, 2019 - 2054 hours**



Figure 8 - MX Query - JLAENTREPRISE.COM



Figure 9 - Whois Information (jlaentreprise.com)

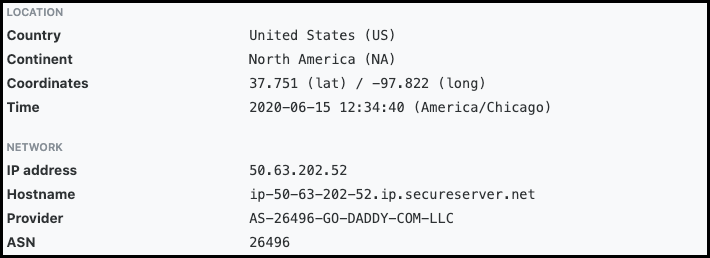


Figure 10 - IP Geographical Location - 50.63.202.52 (jlaentreprise.com)

## **3.6 Email 4: Sabre Project - October 16, 2019 - 0653 hours**

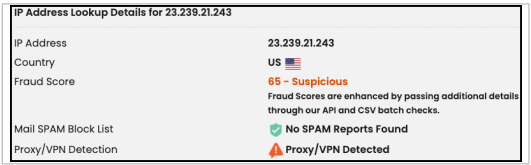


Figure 14 - IP Address Lookup Details - 23.239.21.243

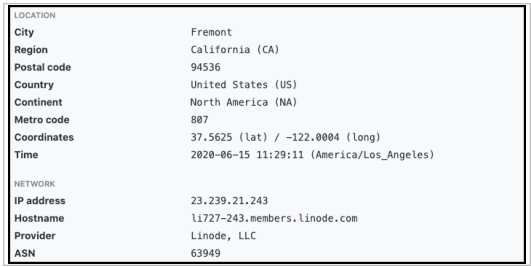


Figure 15 - IPv4 Geographical Location - 23.239.21.243

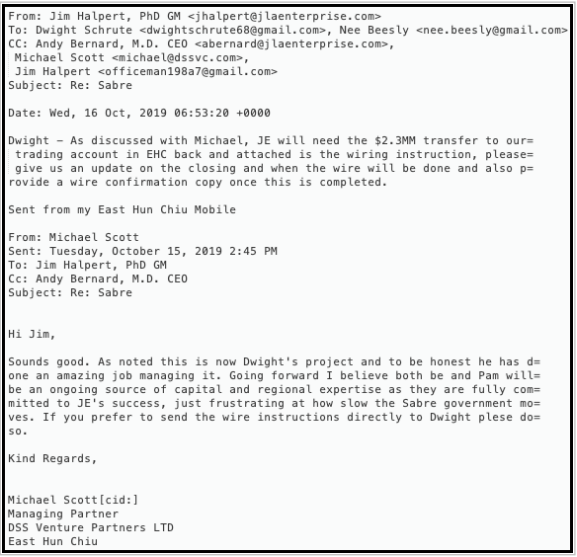


Figure 16 - Email 4 - Jim Halpert (Counterfeit Account) to Dwight Schrute (Phishing Attempt)

## **3.7 Email 5: Sabre Project - October 17, 2019 - 1123 hours**



Figure 17 - jhalpert@jlaentreprise.com used an IPv4 address from a location previously used by SCOTT’s email account

Figure 18 - IPv4 Geographical Location - 83.110.250.20

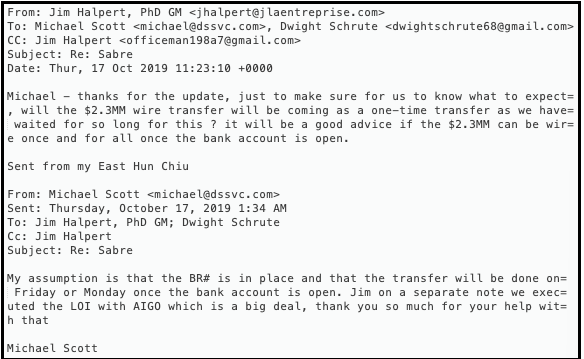


Figure 19 - Email 5 - Jim Halpert (Counterfeit Account) to Michael SCOTT and Dwight Schrute (Confirm Payment)

## **3.8 Email 6: JLA Enterprise and Sabre Project - October 17, 2019 - 1209 hours**



Figure 20 - abernard@jlaenterprise.com auto-forwards to andybernard@abcglobal.com

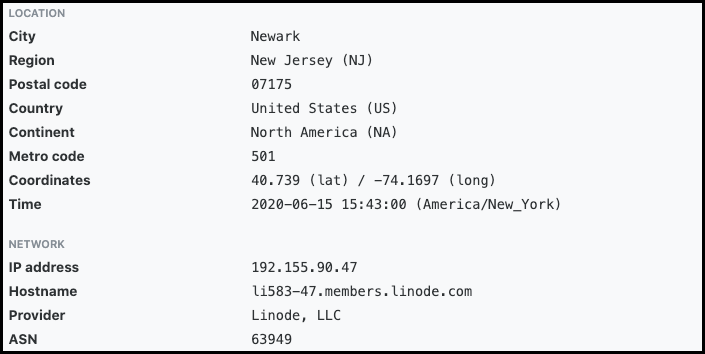


Figure 21 - IPv4 Geographical Location - 192.155.90.47

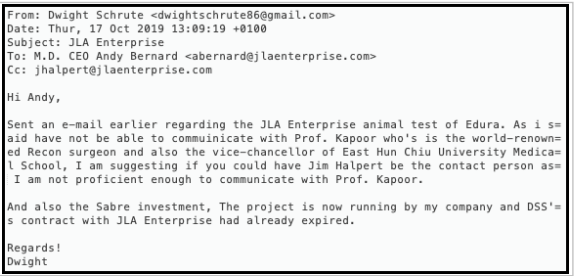


Figure 22 - Email 6 - Dwight Schrute (Counterfeit Account) to Andy Bernard and Jim Halpert (Legitimacy)

## **3.10 Email 8: Sabre Project - October 17, 2019 - 1337 hours**

A screenshot of a cell phone

Description automatically generated

Figure 26 - abernard@jlaentreprise.com to dwightschrute68@gmail.com and nee.beesly@gmail.com

A screenshot of a social media post

Description automatically generated

Figure 27 - Email 8 - Andy Bernard (Counterfeit Account) to Dwight Schrute and Pam Beesly

## **3.11 Email 9: JLA Enterprise and Sabre Project - October 17, 2019 - 1431 hours**

A screenshot of a social media post

Description automatically generated

Figure 28 - Email 9 - Dwight Schrute (Counterfeit Account) to Andy Bernard (Establishing Legitimacy)

## **3.12 Email 10: Sabre Project Wiring Instruction - October 17, 2019 – 1443 hours**

A picture containing table

Description automatically generated

Figure 29 - abernard@jlaenterprise.com auto-forwards to andybernard@abcglobal.com

Figure 30 - IPv4 Geographical Location - 173.230.128.135



Figure 31 - Email 10 - Dwight Schrute (Counterfeit Account) to Andy Bernard (Wiring Instructions)

## **3.13 Email 11: Sabre Project Wire Transfer - October 17, 2019 - 1445 hours**

A picture containing table

Description automatically generated

Figure 32 - X-Originating-IP: 192.81.133.156 (Mail Server in California)

A screenshot of a cell phone

Description automatically generated

Figure 33 - IPv4 Geographical Location - 192.81.133.156

A close up of a flower

Description automatically generated

Figure 34 - Email 11 - Dwight Schrute (Counterfeit Account) to Andy Bernard (Wire Transfer)

## **3.14 Email 12: Sabre Project Wire Transfer - October 17, 2019 - 1459 hours**

Figure 35 - X-Originating-IP: 45.33.17.101 (Mail Server)

Figure 36 - IPv4 Geographical Location - 45.33.17.101

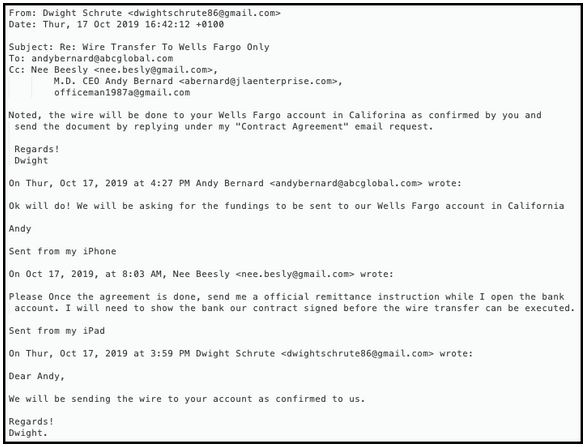


Figure 37 - Email 12 - Dwight Schrute (Counterfeit Account) to Andy Bernard (Wire Transfer Second Email)

Figure 38 - Email 12 - Dwight Schrute (Counterfeit Account) to Andy Bernard (Wire Transfer Second Email) (continued)

## **3.15 Email 13: Sabre Project Wiring Instruction - October 17, 2019 - 1506 hours**



Figure 39 - X-Originating-IP: 83.110.250.20

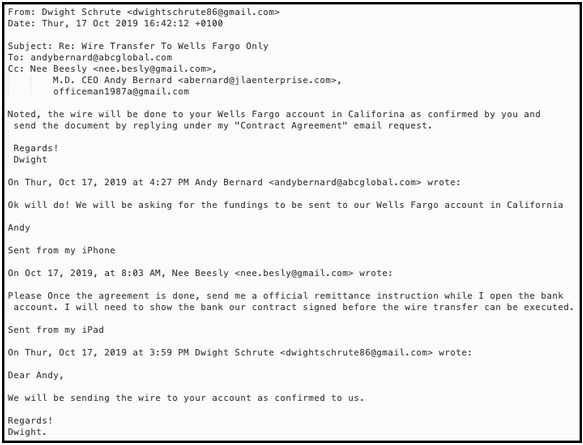


Figure 40 - Email 13 - Jim Halpert (Counterfeit Account) to Pam Beesly (Real Account) (Signed by Dwight Schrute)

## **3.16 Email 14: Sabre Project Wire Transfer - October 17, 2019 - 1542 hours**



Figure 41 - X-Originating-IP: 23.239.21.244

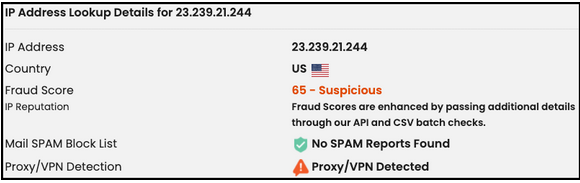


Figure 42 - IP Address Lookup Details - 23.239.21.244

A screenshot of a social media post

Description automatically generated

Figure 43 - Email 14 - Dwight Schrute (Counterfeit Account) to Andy Bernard (abcglobal.com email)

# **4.0 Conclusion**

## **4.1 Email 1: - June 01, 2019 - 0710 hours**

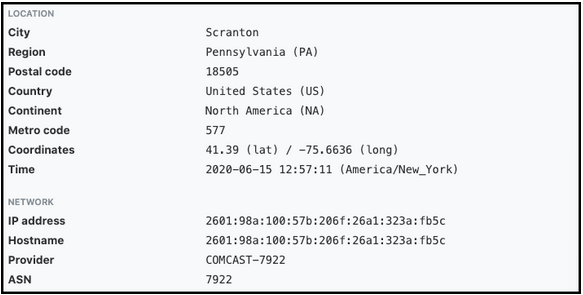


Figure 50 – IPv6 Geographical Location - 2601:98a:100:57b:206f:26a1:323a:fb5c

## **4.2 Email 2: - August 02, 2019 - 1808 hours**

A picture containing table, knife

Description automatically generated

Figure 51 - IP Geographical Location – 23.239.21.244

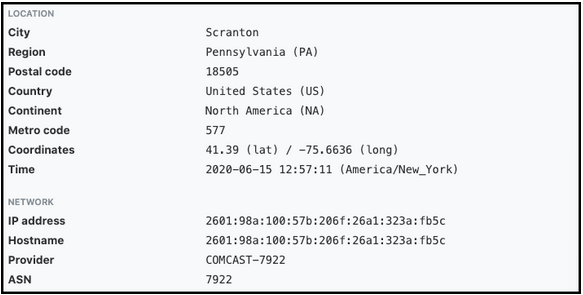


Figure 52 - IPv6 Geographical Location - 2601:98a:100:57b:206f:26a1:323a:fb5c

# **5.0 Recommendations**

# **Appendix A: Wiring Instructions (Fraudulent EAST HUN CHIU Account)**

A screenshot of a cell phone

Description automatically generated