**----------------------------------------------------START OF TICKET----------------------------------------------------**

**Reporting Analyst(s):**

**Executive Summary:**

**-------------------------------------------------------------------------------------------------------------------------------**

**Threat Name:**

**Time of Latest Activity:**

**-------------------------------------------------------------------------------------------------------------------------------**

**Proofpoint Alert Link:**

**Attributes:**

**Threat objective:**

**Involvement Information:**

**# of Emails sent:**

**# of Emails blocked:**

**# of Emails delivered:**

**# delivered with re-written URL:**

**# delivered with non-rewritten URL:**

**Clicks were blocked:**

**Clicks were permitted:**

**-------------------------------------------------------------------------------------------------------------------------------**

**Sender Information:**

**Header from:**

**Subject(s):**

**Header Reply-to:**

**Header To:**

**Envelope Sender(s):**

**Sender’s IP address(es):**

**Message-ID(s):**

**-------------------------------------------------------------------------------------------------------------------------------**

**Intended Recipient(s):**

**-------------------------------------------------OSINT INFORMATION-------------------------------------------------**

**Malicious URLs (Defanged)**

**Malicious Link # 1:**

**VirusTotal Link:**

**Risk Score:**

**Other OSINT Resources:**

**Malicious Link # 2:**

**VirusTotal Link:**

**Risk Score:**

**Other OSINT Resources:**

**Malicious File Attachments**

**Malicious File # 1**

**File Name:**

**File Hash(es):**

**VirusTotal Link:**

**Risk Score:**

**Other OSINT Resources:**

**Malicious File # 2**

**File Name:**

**File Hash(es):**

**VirusTotal Link:**

**Risk Score:**

**Other OSINT Resources:**

**Sending IP Address(es)**

**IP Address # 1 reputation:**

**VirusTotal Link:**

**Risk Score:**

**AbuseIPDB Link:**

**Number of Times Reported:**

**Confidence of Abuse:**

**URLScan.io Link:**

**Verdict:**

**Other OSINT Resources:**

**IP Address # 2 reputation:**

**VirusTotal Link:**

**Risk Score:**

**AbuseIPDB Link:**

**Number of Times Reported:**

**Confidence of Abuse:**

**URLScan.io Link:**

**Verdict:**

**Other OSINT Resources:**

**Malicious IP Address(es) [Found in Evidence > Forensics Section]**

**IP Address # 1 reputation:**

**VirusTotal Link:**

**Risk Score:**

**AbuseIPDB Link:**

**Number of Times Reported:**

**Confidence of Abuse:**

**URLScan.io Link:**

**Verdict:**

**Other OSINT Resources:**

**IP Address # 2 reputation:**

**VirusTotal Link:**

**Risk Score:**

**AbuseIPDB Link:**

**Number of Times Reported:**

**Confidence of Abuse:**

**URLScan.io Link:**

**Verdict:**

**Other OSINT Resources:**

**-------------------------------------------------------------------------------------------------------------------------------**

**Additional Information:**

**-------------------------------------------------------------------------------------------------------------------------------**

**Declaration:**

**-------------------------------------------------------------------------------------------------------------------------------**

**Recommendations:**

**Block IP Address(es):**

**Block Sender:**

**Block URL(s):**

**Purge emails from recipient Inbox:**

**Reset email recipient credentials:**

**Other:**

**------------------------------------------------------END OF TICKET-----------------------------------------------------**