**Title:** Email Analysis

**Group/Name:** Aimé Fraser

**Indicators and Technical Details**

|  |  |  |  |
| --- | --- | --- | --- |
| **Datetime** | **Identifier  (IP, Domain, URL, Hostname)** | **MITRE Technique ID** | **Analyst Comment** |
| No date given | Email does not have the same design aesthetic as the real site. | N/A | Each Indicator is shown in the screenshot narrative below. |
|  | Attempts to create a sense of urgency |  |  |
|  | Unprofessional presentation – code visible on screen, and footer text that doesn’t match. |  |  |
|  | Unprofessional language “vibe” |  |  |
|  | Link text does not lead to Elastic site |  |  |
|  | Warning about download when email opens |  |  |
|  | The reset password button directs to the unprofessional-looking site with no directions |  |  |
|  | Click the login button, and the screen shows obfuscated XML |  |  |
|  | When the password is entered and asked to save, there is no acknowledgment that anything happened |  |  |
|  | Security Practices link leads to a web address showing an .hta file. Adobe asks to enable the add-in |  |  |
|  | Clicking that link leads to downloading the files helper.ps1 |  |  |
|  | Click password recovery link brings up a warning window |  |  |
|  | Clicking yes to run Recovery.ps1 runs Mimikatz |  |  |
|  | From and return path are not the same in the header. |  |  |
|  | The from address is a Gmail account. |  |  |
|  | From path obfuscated to avoid spam detection |  |  |

**Executive Summary**

A GoodCorp user flagged an email as potential phishing. Analysis proved it is a phishing email that contained links to download PowerShell scripts that use a fake website to harvest users’ Elastic Corp. logins and passwords. Each entry into that page (which has unprofessional graphic design) is unsuccessful. The goal is to have the user click the forgot password button, which will download the Mimikatz credential-stealing binary. This will harvest all credentials stored in the victim’s computer.

The only computers affected were those that clicked on any links in the email. For those machines/users, all passwords stored on the machine should be changed, as the attacker now has them.

**Technical Summary and Analysis.**

See below for a graphical walk-though of the email. This narrative is in screenshots, and due to layout limitations in Word, the pages are visually uneven. Please keep scrolling through the pages until reaching the final page, which is marked --End—

The overall feel of the email is clunky and unprofessional. Graphical user interface, application, website

Description automatically generated

The real Elastic site is exciting and engaging. Graphical user interface, text, application

Description automatically generated

The text attempts to create a sense of urgency by saying access to Elastic has been restricted.

Graphical user interface, application, website

Description automatically generated

Looking more closely, code artifacts litter the screen, a sign of uncaring design.

Graphical user interface, application

Description automatically generated

Unprofessional language in these circumstances –“vibe.”

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

Link text does not lead to Elastic site.

Graphical user interface, application, website

Description automatically generated

The reset password button directs to unprofessional-looking site with no directions.

A screenshot of a computer

Description automatically generated

All attempts to log in with various email addresses lead to variations of this. The <HostID> code was always different.

Graphical user interface, text, application, email

Description automatically generated

The <HostId> when decoded with Zip always yielded this. Unble to decode or find file.txt.

Graphical user interface, text, application, email

Description automatically generated

The Security Practices link leads to a web address that downloads an .hta file. Graphical user interface, text, application, email

Description automatically generated

The hta file shows a download link for PowerShell script helper.ps1.Text

Description automatically generated

Opening the link to helper.ps1 leads nowhere. Graphical user interface, text, website

Description automatically generated

The password recovery link reveals another PowerShell link.

Graphical user interface, text, application, email

Description automatically generated

Clicking on it brings up a warning.

Graphical user interface, application, Word

Description automatically generated

Clicking open will download Mimikatz.

Graphical user interface, application

Description automatically generated

The From: and Return: paths are not the same in the email header. They are from a gmail account. This is unprofessional. Text

Description automatically generated

Text

Description automatically generated

The email path is obfuscated to avoid spam detection.

Text

Description automatically generated

The SPF gives a pass saying Gmail is qualified to send emails for GoodCorp. This is unlikely, but it is possible to arrange if the phisher sets up a fake domain and adds its own SPF record. Text

Description automatically generated

This is what happened here.

Graphical user interface, text, application, email

Description automatically generated

Phishing emails from gmail.com pass DKIM (as shown here) because Gmail is a legitimate server. Passing DKIM only assures the legitimacy of the servers and integrity during transmission. It does not guarantee that email’s contents are safe or legitimate.

Text

Description automatically generated

**Remediation and Recommendations**

[M1049](https://attack.mitre.org/mitigations/M1049) Antivirus/Antimalware  
Anti-virus can automatically quarantine suspicious files.

[M1031](https://attack.mitre.org/mitigations/M1031) Network Intrusion Prevention   
Network intrusion prevention systems and systems designed to scan and remove malicious email attachments or links can be used to block activity.

[M1021](https://attack.mitre.org/mitigations/M1021) Restrict web-based content  
Determine if certain websites or attachment types (ex: .scr, .exe, .pif, .cpl, etc.) that can be used for phishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.

[M1054](https://attack.mitre.org/mitigations/M1054) Software Configuration  
Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross-domain) to perform similar message filtering and validation.

[M1017](https://attack.mitre.org/mitigations/M1017) User Training  
Users can be trained to identify social engineering techniques and phishing emails.

[DS0015](https://attack.mitre.org/datasources/DS0015) Application Log  
Monitor for third-party application logging, messaging, and/or other artifacts that may send phishing messages to gain access to victim systems. Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed.[[4]](https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-protection?view=o365-worldwide)[[5]](https://www.cyber.gov.au/sites/default/files/2019-03/spoof_email_sender_policy_framework.pdf) URL inspection within the email (including expanding shortened links) can help detect links leading to known malicious sites. Detonation chambers can be used to detect these links and either automatically go to these sites to determine if they're potentially malicious, or wait and capture the content if a user visits the link.

[DS0022](https://attack.mitre.org/datasources/DS0022) File  
Monitor for newly constructed files from phishing messages to gain access to victim systems.

[DS0029](https://attack.mitre.org/datasources/DS0029) Network Traffic  
Monitor and analyze SSL/TLS traffic patterns and packet inspection associated with the protocol(s) that do not follow the expected protocol standards and traffic flows (e.g. extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated with traffic patterns (e.g., monitor anomalies in the use of files that do not normally initiate connections for the respective protocol(s)). Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed.

Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

[DS0009](https://attack.mitre.org/datasources/DS0009) Process Creation  
Monitor for newly executed processes that may abuse PowerShell commands and scripts for execution.

[DS0012](https://attack.mitre.org/datasources/DS0012) Script Execution   
Monitor for any attempts to enable scripts running on a system would be considered suspicious. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious. Scripts should be captured from the file system when possible to determine their actions and intent.

**References**

[Validate DKIM record by using the DKIM record checker](https://www.dmarcanalyzer.com/dkim/dkim-checker/?dmarcdns%5Btype%5D=dkim&dmarcdns%5Bselector%5D=20210112&dmarcdns%5Bdomain%5D=gmail.com&g-recaptcha-response=03AD1IbLBHWPdHrBYoBh-oG3qG-9Dkf-r2odiQGNw4ZdhjbNoW72ntimSLUarg5cYHkYXcv7ZkIs362A4SVFHLOvw_qmUbw3qH443J1mt-D02RaYlf67dEZm_2Dzjnm9icBO1uHnxHFSTX3k-litvoBMYx52JMPEb0Pdwy5mqjlX6QjpRCSIbt1Wys1jy6xZjQYmMTb683KOkHUDCfCEjLMfIpThXW_zBOKGYbFbPchA9w2fmrRjbVZqn_31BELicO37O2WN1jQA1xh_Ecc3Jt3zCE8ZL31vqw2LpwYEaWF5wHwa1u89ZsalLTW0fAtUlwQ8NV0hiw5vaCckK6ggMr4hjSyq6dGnQFKqK4PgsAT6TnqzPdSBtrT8mOGg7ogK-RApZp6wvKkZwJ86HGv9Cay5Y7FDLVgsHS46UpPRW0dt7xPBUFHAKNEB-1Aq2iVf6JS1Xyr7MRDNJMMgLuZdCMbhKNS9GlLDoMRYFby_RnNiLxaQIwsaAqKADN73p88-4_evNWgMpuctZTRjT6zqGVHu5cuDkJMj--8F8sLn8Dy2U0I6UVwL2XTIifxRUmBoEKDa1C7aE36qdQOYVTvCymihN_tIpSI3i7HA), Mimecast, Accessed January 14, 2022.

**--End--**