Author: Jack Fitzgerald

Official Incident Report

Date: Apr, 26, 2021, 11:03 PM

Event ID: 90

Rule Name: SOC143 - Password Stealer Detected

Table of Contents

Alert Details

Severity: Medium

Type: Exchange

SMTP Address: 180.76.101.229

Source Address: bill@microsoft.com

Destination Address: ellie@letsdefend.io

E-mail Subject: .

Device Action: Allowed

Based on the information provided in the alert, it appears that a suspicious email, potentially containing a **password stealer**, sent to **ellie@letsdefend.io**, has been detected. The alert is triggered by rule SOC143 - Password Stealer Detected.

Upon reviewing the alert, it is observed that an email with the subject **.** was sent from **bill@microsoft.com** with an SMTP of **180.76.101.229**.

The device action is marked **allowed**, indicating that the email was delivered to the **ellie@letsdefend.io** inbox.

Overall, it appears that the email may be suspicious, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

Detection

Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a **false positive** or a **true positive** incident is to analyse the logs collected from the host by our security products.

According to the ASD, information stealer malware, also known as info stealers, is a type of malware designed to secretly collect information from a victim's device.

In general, info stealers can steal:

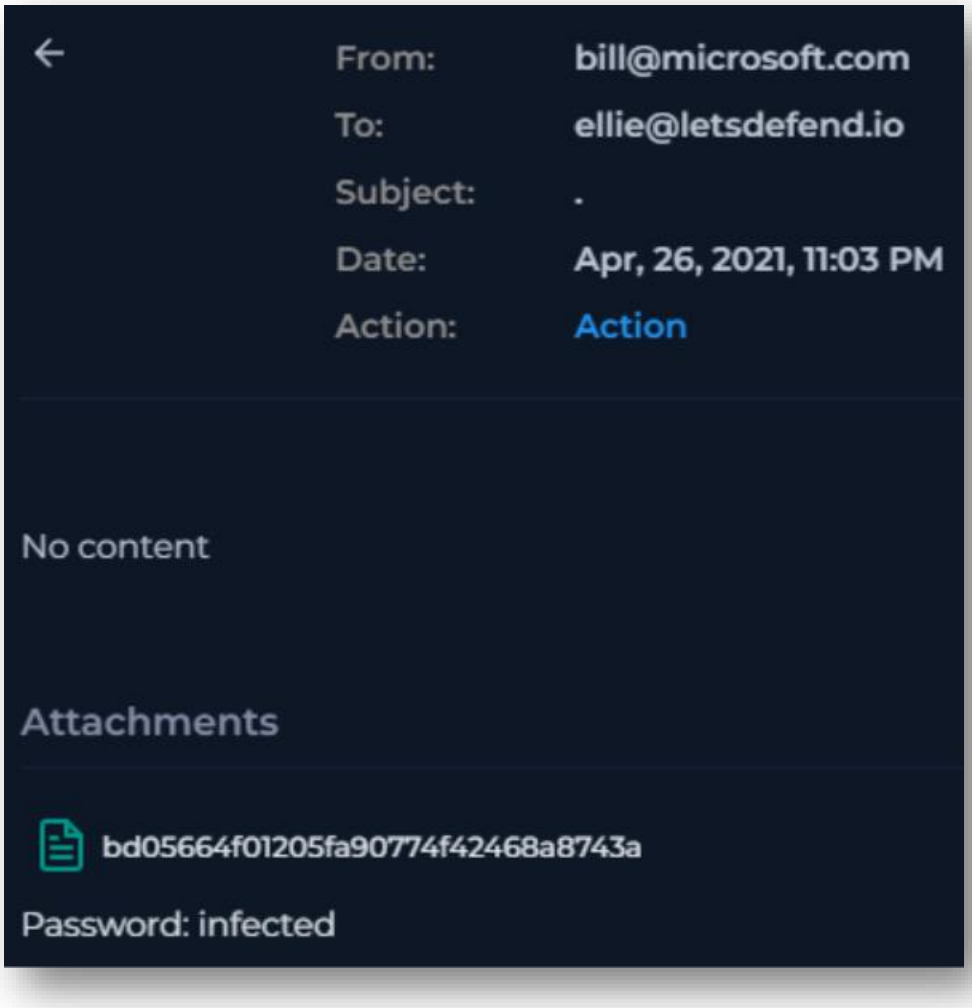
- **User Credentials:** computer session logins and passwords, browser login links, usernames, passwords, secret keys, Two-Factor Authentication (2FA) backup codes, server passwords, Virtual Private Networks (VPNs) and File Transfer Protocol (FTP) details
- **Browser Data:** browser history, search history, session cookies, and autofill data, such as saved credit/bank card details
- **Communication Data:** messaging and email chat logs
- **Documents and Text Files:** financial information, corporate data, crypto private keys and crypto wallets
- **Computer Information:** including operating system details, metadata, Internet Protocol (IP) addresses, applications installed on the computer, anti-virus software used, and end-point detection capabilities
- **Images:** including screenshots of the desktop taken by the malware.

Cybercriminals use many techniques to infect victim devices with info stealer malware.

These include:

- **Phishing campaigns** – such as adding malicious attachments or links to emails or spreading the malware via fake messages
- **Non-phishing methods** – such as malicious advertising and websites laced with malicious software, including cracked and pirated software, as well as search engine poisoning

By searching for the email sender of **bill@microsoft.com** in Email Security, we can find the email and some further details.



The first step we take when investigating a suspicious email is to parse the email information.

When was it sent?

Apr, 26, 2021, 11:03 PM

What is the email's SMTP address?

180.76.101.229

What is the sender's address?

bill@microsoft.com

What is the recipient's address?

ellie@letsdefend.io

Analysis

The next step is to determine whether there are any **Attachments** or **URLs** in the email. If the email is malicious, the recipient may be exposed to an attack. In this case, there is an Attachment, with file hash **bd05664f01205fa90774f42468a8743a** identified.

The first step is to analyse the SMTP address **180.76.101.229** provided. We upload this to online analysis tools such as **VirusTotal** and **AbuseIPDB** to determine its behaviour and whether this address is malicious.

https://www.virustotal.com/gui/ip-address/180.76.101.229

1 detected file embedding this IP address

https://www.abuseipdb.com/check/180.76.101.229

This address originates from Beijing, China. The provider is clearly not related to Microsoft's SMTP services. It is understood that the attacker is spoofing their email address to appear as coming from a Microsoft address to look legitimate.

The next step we want to perform is to analyse the Attachment MD5 hash **bd05664f01205fa90774f42468a8743a** contained within the email.

https://www.virustotal.com/gui/file/58c45547bccce5eb16d84bae13eb0c2813ffe03e34eae622b65468a6b289ca37

23/62 security vendors flagged this file as malicious

The file is identified as **Ellie@letsdefend.io_63963965Application.HTML**. The file contacts **dl.dropboxusercontent.com**, which has been detected as a malicious domain, as well as **204.79.197.203**, which has been detected as a malicious IP address.

The next step is to sandbox the malicious file using **Triage**.

https://tria.ge/251105-gdh5xssqhj

The file brings the user to a bare login page, requesting the user to login with username and password. This is clearly not an official Microsoft login page, and users should NOT enter any information in these fields.

Upon trying to login with credentials, the page tries to access **https://tecyardit.com/wp-content/card/post.php** but can't reach the page.

As part of the analysis, we can investigate deeper by searching for Log Management to see if we can find any extra information. However, no information was found regarding this alert.

Another part of the analysis is to investigate Endpoint Security. However, no device was identified as being associated with **ellie@letsdefend.io**.

As no activity was found regarding this alert, we can say the malicious file was **not opened**.

Containment

Based on the information gathered during the investigation, it is highly unlikely that the system has been compromised. Isolation of the system from the network is not required.

Summary

The incident involves no compromised system. The alert was triggered by the detection of a suspicious email containing a **password stealer**, sent to **ellie@letsdefend.io**, based on the rule SOC143 - Password Stealer Detected.

Upon further analysis, it was discovered that the suspicious email contained an Attachment with MD5 hash **bd05664f01205fa90774f42468a8743a**. The MD5 hash was confirmed as malicious by various security vendors and online analysis tools.

The email was sent from a spoofed email address originating from China, appearing as a Microsoft domain. The file sends the user to an online login page impersonating Microsoft, where an unsuspecting user would enter their login credentials to login, giving the attacker the user's credentials.

However, no activity was found regarding this alert, suggesting the file was never opened.

Lessons Learned

- Perhaps users are becoming more accustomed to not opening suspicious email attachments
- Email filtering rules did not block the malicious attachment

Remediation Actions

- If an account is compromised, immediately change its password. If the same password was used elsewhere, change those as well
- Block the IP address of the attacker or any other suspicious sources of login attempts at both the network and application levels
- Run a full scan on all endpoints using anti-malware software and configure your endpoint detection and response (EDR) to block malicious artifacts and run in automated remediation mode
- Follow your established incident response plan, which should include alerting the team and performing a post-incident analysis
- Require strong, complex, and unique passwords for all accounts and enforce policies that limit the number of failed login attempts
- Enable MFA on all accounts to provide an extra layer of security beyond just the password
- Conduct regular training on how to spot phishing emails, avoid downloading malicious attachments, and recognize social engineering tactics

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Initial Access	T1566.001 - Spearfishing Attachment
Execution	T1204.002 - Malicious File
Execution	T1059 - Command and Scripting Interpreter
Credential Access	T1056 - Input Capture
Command and Control	T1041 - Exfiltration Over C2 Channel

Artifacts

Value	Comment	Type
https://tecyardit.com/wp-contet/card/post.php	Impersonating Microsoft login page	URL Address
bill@microsoft.com	Spoofed email address	E-mail Sender
microsoft.com	Spoofed domain, originates from Beijing, China	E-mail Domain
180.76.101.229	SMTP address	IP Address
bd05664f01205fa90774f42468a8743a	Ellie@letsdefend.io_63963965Application.HTML	IP Address

LetsDefend Playbook

LetsDefend Event ID: 90