Subject: You're Invited!
From: Adam Barry <abarry@live.com>
Date: 5/15/24, 4:31 AM
To: emily.nguyen@glbllogistics.co

Hey Emily,

I hope this email finds you well! Richard and I are thrilled to extend an invitation to our wedding! We would be honored to have you join us on our special day.

Your presence would truly mean a lot to us. To assist with our planning, I've attached a short survey for your RSVP and meal preferences. Your response would be greatly appreciated.

Looking forward to hearing from you soon!

Warm regards,
Alexia Barry

Attachments:

AR_Wedding_RSVP.docm 140 KB

Phishing Email Analysis Report-1

Headers

Date: Tue, 14 May 2024 23:31:08 +0000
Subject: You're Invited!

To: emily.nguyen@glbllogistics.co
From: Adam Barry abarry@live.com

Reply-To: (Not Specified in the email.)
Return-Path: abarry@live.com

Sender IP: (Not explicitly provided but associated with Microsoft's infrastructure.)
Resolve Host: Not resolved from the email but matches Microsoft's infrastructure for Outlook.com

Message-ID:
SA1PR14MB737384979FDD1178FD956584C1E32@SA1PR14MB7373.namprd14.prod.outlook.com

Attachments

Filename: AR_Wedding_RSVP.docm
MD5: 590d3c98cb5e61ea3e4226639d5623d7
SHA1: 91091f8e95909e0bc83852eec7cac4c04e1a57c3
SHA256: 41c3dd4e9f794d53c212398891931760de469321e4c5d04be719d5485ed8f53e

Description

The email appears to be an invitation sent by Adam Barry to Emily Nguyen.

The email claims to include an RSVP survey and preferences for an upcoming event. However, upon further analysis, the attachment is flagged as malicious.

The attachment, a macro-enabled Word document (.docm), contains VBA macros that are designed to execute a series of malicious actions, including downloading an executable file from a remote URL.

Artifact Analysis

Sender Analysis:

Although the sender claims to be Emily Nguyen's friend, the analysis reveals no evidence supporting the email's legitimacy.

The email originated from Microsoft Infrastructure (Outlook.com), but the sender's email address is unaffiliated with any legitimate organization or purpose related to the recipient.

Attachment Analysis:

A reputation check of the attachment's SHA256 hash using VirusTotal and Cisco Talos flagged it as malicious.

The attachment is identified as a Trojan downloader ("downloader.autdwnlrner/w97m"), which is designed to deploy malicious payloads.

The VBA macros within the attachment save a file named shost.exe on the victim's device and attempt to download a malicious executable from hxxps[://]github[.]com/TCWUS/Pastebin-Uploader[.]exe.

Verdict

This email is a phishing attempt with a malicious attachment.

The attachment contains executable code designed to infect the user's machine, steal information, or further propagate the attack.

It is unsafe to release this email to the recipient.

Defense Actions

Email Gateway:

- Block the sender's email address (abarry@live.com).
- Flag and quarantine emails containing the filename AR_Wedding_RSVP.docm or similar macro-enabled attachments.

Endpoint Security:

- Block access to the URL hxxps[://]github[.]com/TCWUS/Pastebin-Uploader[.]exe across all endpoints.

Threat Intelligence Update:

- Add the identified SHA-256 hash to the organization's blocklist to prevent future attempts using this attachment.

Subject: Your account has been flagged for unusual activity
From: Outlook Support Team <social201511138@social.helwan.edu.eg>
Date: 11/1/23, 12:10 AM
To: dderringer@mighty-solutions.net

> **This message is sent from a trusted sender certified by Outlook Online Support Team.**

Microsoft

Action Required : Account Fraud Protection !

Dear Customer,

Your account has been flagged for unusual activity. To protect your account from unusual activity and fraudsters,

we have disabled your Online Access.

You need to re-verify your account with us in order to regain access and to keep enjoying our online services again

by clicking on the button below and once you've completed the required action,

we'll review and get back to you regarding the status of your account immediately.

- Log in to your Microsoft account

What happens next?

Once you've completed the required action, we'll review and get back to you regarding the status of your account immediately.

We appreciate your attention to this matter.

In case of ignorance, your services will be completely suspended within 24 hours according to the terms defined in our contracts.

Sincerely,

Fraud Department,

2023 Outlook

Phishing Email Analysis Report-2

Headers

Date: Tue, 31 Oct 2023 10:10:04 -0900
Subject: Your account has been flagged for unusual activity

To: dderringer@mighty-solutions.net
From: Outlook Support Team social201511138@social.helwan.edu.eg

Reply-To: social201511138@social.helwan.edu.eg
Return-Path: (Not specified in the email.)

Sender IP: 40.107.22.60
Resolve Host: mail-am6eur05on2060.outbound.protection.outlook.com

Message-ID: JMrByPl2c3HBo8SctKnJ5C5Gp64sPSSWk76p4sjQ@s6

URLs

hxxps[://]0[.]232[.]205[.]92[.]host[.]secureserver[.]net/lclbluewin08812/

Description

This email claims to be from the "Outlook Support Team," warning the recipient that their account has been flagged for unusual activity.

The content of the email attempts to create a sense of urgency by implying the user must take immediate action, even though there is no actual impact on the user's account access.

The email includes a URL redirecting to a suspicious page, likely a phishing attempt to steal the recipient's credentials.

Artifact Analysis

Sender Analysis:

The sender claims to be the Outlook Support Team, but the sender's email address originates from a completely unrelated domain (social.helwan.edu.eg), which has no connection to Microsoft or Outlook.

The SPF check results show **spf=pass** for the domain, but this does not verify the legitimacy of the sender's identity.

URL Analysis:

A reputation check of the URL using VirusTotal flagged it as malicious. Fortinet specifically labeled the URL as phishing.

The domain appears to host a credential capture page designed to steal sensitive information.

Verdict

This email is a clear phishing attempt.

The sender's domain and IP are unaffiliated with Outlook support. Additionally, the URL redirects to a malicious phishing page, as verified by VirusTotal.

Defense Actions

Email Gateway:

- Block the sender's email address (social201511138@social.helwan.edu.eg).
- Block all emails containing the URL **domain:0[.]232[.]205[.]92[.]host[.]secureserver[.]net**.

Web Proxy and EDR:

- Block user access to the domain **host[.]secureserver[.]net** across all endpoints.