Headers

Date: `Mon, 28 Jul 2025 14:26:59 -0500`
Subject: `Action Required: Unusual Activity Detected on Your Account`

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

Reply-To: `N/A`
Return-Path: `abarry@live.com`

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

URLs

- No URLs were found in the email.

Attachments

Attachment Name: `AR_Wedding_RSVP.docm`
MD5: `590d3c98cb5e61ea3e4226639d5623d7`
SHA1: `91091f8e95909e0bc83852eec7cac4c04e1a57c3`
SHA256: `41c3dd4e9f794d53c212398891931760de469321e4c5d04be719d5485ed8f53e`

Description

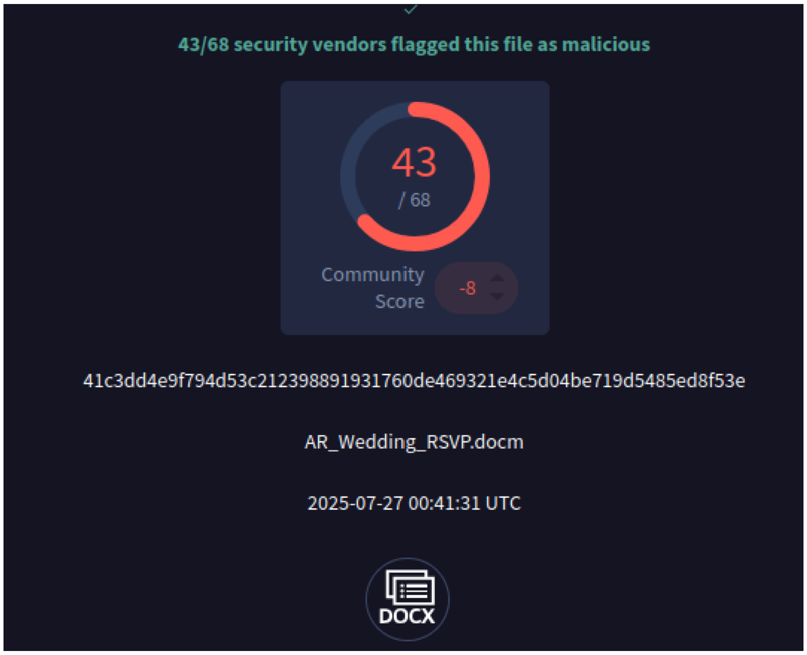
The SOC received an alert about a quarantined email that was flagged by the company's email gateway solution. The email was sent to Emily Nguyen, a member of the marketing team, from her friend Alexia Barry.

Summary

- The email is a malicious attempt to trick the user into executing a `.docm` downloader macro that would have installed a trojan onto the device. The attachment is a known malicious file on VirusTotal and malware bazaar, and is likely part of an automated mass email campaign.

Artifact Analysis

- A quick scan on VirusTotal using the MD5 hash of the artifact reveals it to be malicious.



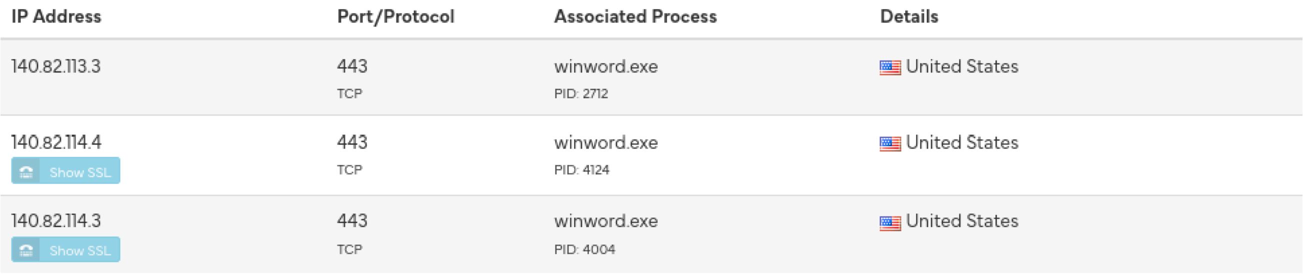
43/68 security vendors flagged this file as malicious

41c3dd4e9f794d53c212398891931760de469321e4c5d04be719d5485ed8f53e

AR_Wedding_RSVP.docm

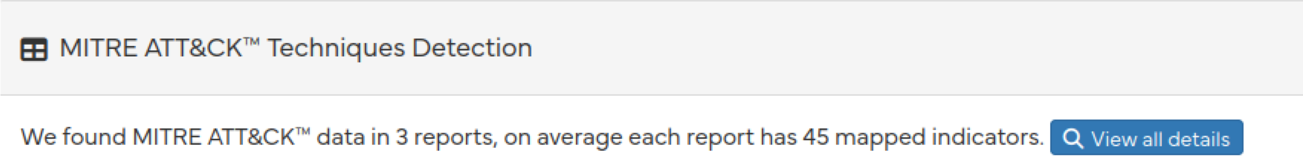
2025-07-27 00:41:31 UTC

- Using the sha256 hash, a match was found on malware bazaar, providing further evidence that the email is malicious.
- VirusTotal found the malicious attachment to be a trojan downloader imbedded in a Microsoft word macro document.
- An analysis done on the sandboxing website **Hybrid Analysis** reveals that the malicious document made numerous connection attempts, likely exploiting a vulnerability inside Microsoft Word itself.



IP Address	Port/Protocol	Associated Process	Details
140.82.113.3	443 TCP	winword.exe PID: 2712	United States
140.82.114.4 Show SSL	443 TCP	winword.exe PID: 4124	United States
140.82.114.3 Show SSL	443 TCP	winword.exe PID: 4004	United States

- The behavior of the attachment and malicious email was mapped to 45 MITRE ATT&CK framework IOC indicators


MITRE ATT&CK™ Techniques Detection

We found MITRE ATT&CK™ data in 3 reports, on average each report has 45 mapped indicators.

- The malicious attachment itself relied on user execution to initiate a connection and download a trojan.

Sender Analysis

- Talos intelligence discovered the source email `abarry@live.com` to have a trusted reputation.
- The email body references the recipient by name, which may indicate a handwritten phishing attempt.
- However, if there is no evidence of port scanning or active reconnaissance, its more likely that the sender programed the email to create a custom message in a mass phishing campaign.
- At a quick glance, the email also appears to be written by an AI program, with the phrase `I hope this message finds you well`, being a common introduction when prompted.
- The email also passed all SPF and DKIM checks.

Verdict

- The email is a malicious attempt to deliver malware onto a user's device. It is not an attempt at phishing for credentials, rather it relies on tricking the user into executing a seemingly innocent document that contains macros to retrieve files and make http requests.
- A `.docm` file is a type of Microsoft Word macro file, containing sequenced commands for the operating system to execute. The attacker relied on user inexperience with `.docm`, and disguised the file as a wedding RSVP Microsoft Word document. If the user opened the file, they would download a trojan and infect their machine.

Defensive Actions

- If the user has clicked on the email and downloaded more malware, the user's endpoint has to be contained and analyzed. The incident response playbook beings with a confirmation that the source email is malicious.

- The target endpoint has to be disconnected from the internet, and investigated thoroughly for indicators of compromise and other sources of malware. A forensic analysis of the endpoint and other devices on the network must also be conducted in case of lateral movement from the user's endpoint. Domain controllers, file shares, and systems recently accessed by the user have to be prioritized. The investigation must be conducted while minimizing the effect on business operations, so it is recommended to temporarily migrate operations to a parallel infrastructure hot site while the network can be cleared.
- Given the delivery of the malicious content via email, it would be prudent to implement **Technical Security Controls** to enforce restrictions on email communications from **external sources**, especially targeting high-risk user groups. Implement domain whitelisting where appropriate. The email passed DMARC, DKIM, and SPF tests, so more robust malware detection tools such as **Endpoint Detection and Response (EDR)** and real time **File Integrity Monitoring (FIM)** should be considered for future implementation.
- The malicious attachment was indexed in VirusTotal and malware bazaar. Real time threat intelligence tools or an email client with built in sandboxing and scanning may prevent similar threats.
- **Administrative Security Controls** must also be implemented, to teach endpoint users about malicious phishing and malware delivery methods. Including how to identify phishing attempts, macro document behavior, and common adversary behavior.