Maryland
INFORMATION SHARING
AND ANALYSIS CENTER

POWERED BY ANOMALI

THREAT BULLETIN

AR20230127-003 [Advisory Report]: OneNote Attachments Used To Spread Malware

TLP
White

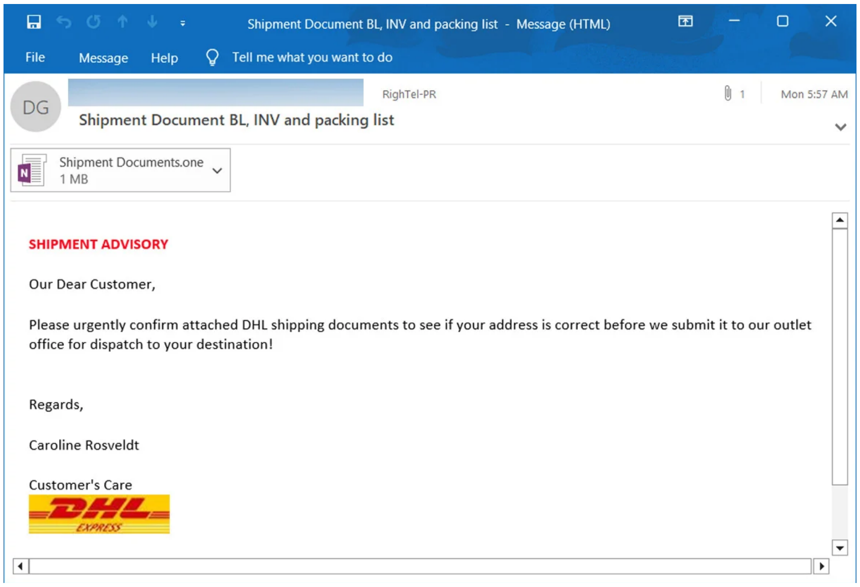
DESCRIPTION

Summary

Threat actors are the resourceful and creative kind. Finding new and more enticing ways to exploit and steal information is what they do. Methods of using macros enabled Word and Excel attachments in malicious emails have been used for years. Recent changes by Microsoft have required attackers to shift their attention and use alternative, albeit just as effective, methods of attack. One new method is using Microsoft OneNote attachments in spam and phishing email messages. OneNote is a free application and is included with Office 2019 and Microsoft 365, so its file format is available for use by most Microsoft Office users and threat actors are starting to abuse that more and more.

Technical Details

Microsoft OneNote is a digital notebook application where users can take notes, share ideas, mix in media files and add to-do tags. Since it is installed by default in most newer Office installations and free to access for other Microsoft users, it only makes sense that the format used by OneNote would be exploited by attackers. The file format can be opened by unsuspecting victims, even if they are not OneNote users but are users of other Microsoft applications such as Outlook, Word or Excel.


Shipment Document BL, INV and packing list - Message (HTML)
File
Message
Help
Tell me what you want to do

DG [redacted] RighTel-PR 1 Mon 5:57 AM

Shipment Document BL, INV and packing list

Shipment Documents.one
1 MB

SHIPMENT ADVISORY

Our Dear Customer,

Please urgently confirm attached DHL shipping documents to see if your address is correct before we submit it to our outlet office for dispatch to your destination!

Regards,

Caroline Rosveldt

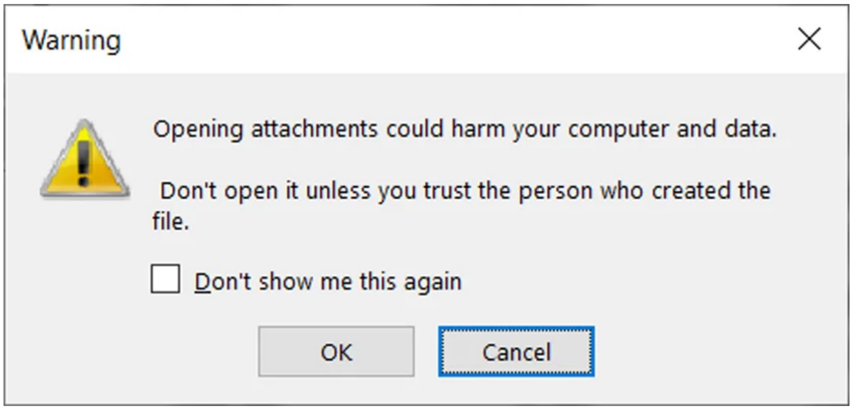
Customer's Care

DHL EXPRESS

Fake DHL email with a OneNote Attachment - Source: Bleeping Computer

True to form, attackers send malspam and phishing emails in the form of shipping notifications or documents, detailed mechanical drawings, and invoices pretending to be legitimate businesses or messages that victims might expect from potential recent purchases. Threat actors are exploiting the insert attachments feature within OneNote by including VBS attachments within the message. The attachment is a script, so that when the program or document is launched, the script automatically runs. A method used by threat actors to get the unsuspecting victim to launch the script is by putting a large “Double Click to View File” banner over the information, which is either blurred or obfuscated in some manner. The victim then double clicks to view the document and inadvertently launches the malware. Typical malware used by threat actors in these types of attacks is called remote access trojans (RAT) that access a victim’s files, browser passwords and in some cases cryptocurrency wallets.

A feature of OneNote that should be taken into account is the fact that there is a warning window that comes up when a user wishes to launch an attachment within OneNote. Though, this security feature is historically ignored by most users. They just click the OK button to get to the document. Threat actors count on this type of behavior to enable their malware by user execution.



Opening attachments could harm your computer and data.

Don't open it unless you trust the person who created the file.

☐ Don't show me this again

OneNote Security Warning for opening attachments - Source: Bleeping Computer

Protecting against these threat actors

One of the best practices users can do is to not open attachments from people that are unknown to them. If an attachment is opened mistakenly, heed the warnings that are displayed. Should the attachment show a warning message that it could harm your computer, do not click the OK button and then close the application. If users are questioning whether the email or the attachment came from a legitimate source, they should share it with their security personnel to investigate it further. User training should be conducted on a regular basis to show how easy one can become a victim of such threats. Users being proactive and watchful can assist organizations in combating these types of threats.

Incident Response

If administrators discover signs of attack or system compromise, the MD-ISAC recommends they:

- Immediately isolate affected systems.
- Collect and review relevant logs, data, and artifacts.
- Consider soliciting support from a third-party incident response organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.
- Report activity related to this bulletin to the MD-ISAC via Maryland's 24/7 Operations Center (md-isac@maryland.gov or (410) 697-9700 - option #5).

Contact Information

To report suspicious or criminal activity related to information found in this Threat Bulletin, contact the Maryland Security Operations Center at (410) 697-9700 or by email at md-isac@maryland.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. Please state in the report if you are requesting incident response resources or technical assistance related to the incident.

Reference