UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00167

NEW MALWARE-PROTECTION BYPASS IN OFFICE

DATE ISSUED: 12th July 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

By using older versions of Microsoft Word and Excel documents, a new email threat campaign is able to bypass security detections using novel techniques and enable macros when users attempt to access the attachment.

BREAKDOWN

Leveraging Microsoft Office's Dynamic Data Exchange (DDE) and Windows-based Visual Basic for Applications (VBA) is enabling attackers to download the Zloader banking trojan on systems that support the legacy XLS format. When the user attempts to access the document attached to the phishing email a VBA-based instruction hidden within the document reads a bespoke Excel cell to create a macro which will then populate other cells in the same XLS document with another VBA macro that is able to immobilize Office defences. The macros then alter the policy in the registry to remove alerts that macros have been enabled in the documents. Thereafter, the excel file begins to download the Zloader and execute it using rundll32.exe. As a safety precaution, Microsoft Office normally disables macros but by clicking the "Enable Editing" or "Enable Content" button when a message pops up stating the document is an older version of Word, macros will become active.

REMEDIATION STEPS

- Educate users on social engineering techniques and how to identify phishing emails and what to do if they receive a suspicious email.
- Instruct users not to open attachments in emails from unexpected sources.
- Instruct users to always view attachments in protected view and not to enable content or editing when accessing attachments from email.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/microsoft-office-malware-protection-bypass/167652/
McAffee Blog https://www.mcafee.com/blogs/other-blogs/mcafee-labs/zloader-with-a-new-infection-technique/