mimecast®

EMAIL SECURITY ADVISORY

Office File Macro Threats Delivered by Email

Mimecast has recently detected a sharp increase in the use of Microsoft® Office™ document VB Macros as a mechanism to deploy malware to target hosts; reinforcing an upward trend in this tactic over the last twelve months.

Cyber criminals and hackers are utilizing the Visual Basic for Applications (VBA) macro functionality built into Microsoft Office (Word, Excel, PowerPoint etc.) documents to bypass traditional signature based anti-malware detection, and to download malware to an end user's computer when the file is run.

Typically the Microsoft Office Word 'dot doc' (.doc) file format is used by attackers, which while no longer supported is still a file type recognized and opened by Office applications.

Cyber criminals and hackers are emailing these weaponized attachments to their targets as normal email attachments. Macros are the easiest way to weaponize an attachment, but are only one of many types of attachment threat.

The attachments, containing a macro, are not malicious in themselves but are used as the downloader or dropper for the actual malware, which is downloaded automatically by the macro when the end user runs the file or enables the macro.

This tactic was first observed in the late 1990s, as utilized by successful macro viruses such as Melissa (or the ILOVEYOU virus) and Love Bug. Microsoft effectively hobbled the threat as a result of these viruses which forced hackers to turn to other tactics. Today, the threat has returned as hackers turn to weaponized attachments combined with social engineering to aide their success with malware. Malware such as Dridex, Shifu, Bartallex and Adnel demonstrate this threat well.

Figure 1: : Office 2013 Macro security warning

VBA Macros are disabled by default in most modern Microsoft Office applications; such as Office 2010, 2013 & Office 365, with "Protected View" (see figure 1). However, older desktop versions (Office 2000, 2003 & 2007) do not enjoy the same protection. Network administrators may also enable macros across their Office applications for ease of use; lowering the security as a result.

Targeting Summary

How a Macro Works

Macros provide an embedded code or program which acts as a legitimate mechanism to automate many of the routine and repetitive tasks in an Office document. Macros are frequently used by power users of Microsoft Word and Excel such as finance teams to process large amounts of data or automate tasks within those documents.

A macro, when run, can perform many tasks automatically within an office document, it is this functionality that cyber criminals and hackers are using to automate the download of their malware from within the office file itself. These 'weaponized attachments' use the macro functionality, often without the end users knowledge to infect the host.

Malicious Marcos as Weaponized Attachments

Email has become the attack vector of choice, allowing attackers to reach many victims easily and cheaply. Propagating their weaponized attachments through spam botnets primarily but also using compromised web-pages and drive-by downloads. Attackers have quickly learnt the techniques email security vendors use to detect their payloads and change their tactics frequently, as well as obfuscate the code within the macro using special CTRL (control) character conversion and encryption to avoid detection.

Weaponized attachments pass through normal (non-sandboxing) anti-malware gateways because the attachment behaves as a normal document and does not present any viral payload, malicious code or signature-able content. Code obfuscation within the macro enables the attackers to hide the links used to download their real malware and further avoid detection. This is a direct response to the use of malware signatures by security software.

> **CODE OBFUSCATION WITHIN THE MACRO ENABLES THE ATTACKERS TO HIDE THE LINKS USED TO DOWNLOAD THEIR REAL MALWARE AND FURTHER AVOID DETECTION.**

Attack Analysis

Macros Combined with Social Engineering

Because of the early threat from macro related malware during the 1990s, Microsoft took steps to remove the "auto-run" functionality from macros' and required end users to enable or run the macro themselves. This effectively removed the malware problem in macros for the next fifteen years.

More recently, as cyber criminals and hackers have learnt the effectiveness of social engineering, they have too learnt to combine this with a new breed of macro enabled malware. The result, to the end user or victim, is an innocent looking but convincing email and attachment urging them to open and run the macros.

Tactics include encouraging the end user to enable macros within the Office document. The image to the right (figure 2) is a well-publicized example of the typical social engineering used by attackers. Other examples noted by Mimecast include less obvious attachments claiming to be shipping documentation, Apple Store receipts (figure 3) resumes, sales invoices, fax notifications, payment requests, denied wire transfers; all fake of course.

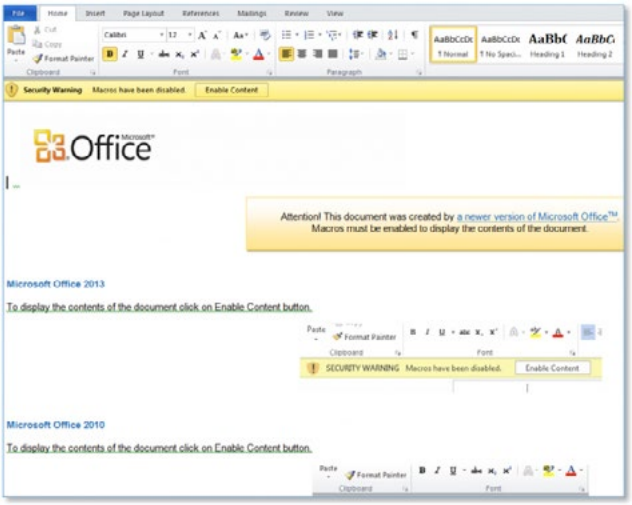

Figure 2: Example social engineering within an attachment.

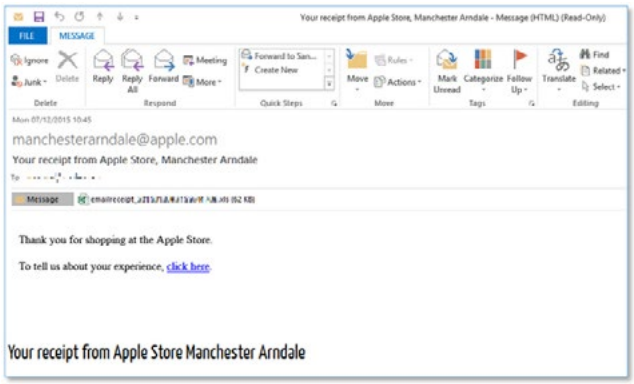

Figure 3: Example Apple Store receipt.

The resulting infection caused by the downloaded malware can serve a variety of purposes. Shifu as an example borrows techniques from other Trojans, such as Shiz, Zeus, Conficker, Vawtrak and Dyre as well as a desctructive capability that can render the host inoperable. Techniques include:

- Collecting data such as passwords, auth tokens, any clear-text credentials (e.g. FTP), certificates, files, bitcoin wallets.
- Capturing keyboard inputs through keyloggers and capturing screenshots and webcam images.
- Harvesting data from point of sale (POS) systems and banking platforms or websites.
- Creating local copies of itself and acting as P2P or C&C control nodes for a wider botnet or malware network.

- Destroying files and the resident OS, as well as avoiding AV and other malware.
- Downloading additional modules, which are often task-orientated and specific to certain processes or services, for further data exfiltration

Prevention & Mimecasts Recommendations

Mimecast makes the following recommendations in relation to weaponized attachments and macro-enabled malware:

- Ensure all email attachments are sandboxed by an appropriately advanced email security gateway. Remember non-sandboxing gateways are not able to recognize or signature macros, as the code is not a viral payload.
- Consider a secure email gateway that offers the capability to neutralize weaponized attachments, or strip active code from all inbound Office documents by transcribing them into safe file formats.
- Ensure macros are not enabled by default across your Microsoft Office application estate, and that 'Protected View' is enabled at all times.
- Consider disabling macros and VBA code all but essential applications.
- Train and educate end users to the changing nature of threats in email. Ensure they understand the risks presented to their inboxes, and how to handle unexpected email and attachments. Ensure they understand the hacker's tactics and how to recognize simple social engineering attacks.
- Consider automatically marking emails that have originated outside of the corporate network, or contains an attachment from an external source.
- Always use the latest versions of Microsoft Office applications. Old versions, pre-2010, offer no protection against weaponized attachments. Ensure all installations are fully patched and up to date.

Mimecast makes business email and data safer for more than 15,000 customers and millions of employees worldwide. Founded in 2003, the Company's next-generation cloud-based security, archiving and continuity services protect email and deliver comprehensive email risk management.