proofpoint.

How Threat Actors Are Adapting to a Post-Macro

Key Findings:

- In response to Microsoft's announcements that it would block macros by default in Microsoft Office applications, threat actors began adopting new tactics, techniques, and procedures (TTPs).
- Threat actors are increasingly using container files such as ISO and RAR, and Windows Shortcut (LNK) files in campaigns to distribute malware.
- Proofpoint has observed the use of VBA and XL4 Macros decrease approximately 66% from October 2021 through June 2022, based on campaigned data.

Overview

Microsoft previously announced it would begin to block XL4 and VBA macros by default for Office users in October 2021 and February 2022, respectively. The changes began rolling out this year. (There was some confusion in July over the implementation of the VBA macro blocking, but Microsoft announced it would continue rolling it out.)

Threat actors across the landscape responded by shifting away from macro-based threats. Based on Proofpoint campaign data from October 2021 through June 2022, threat actors have pivoted away from macro-enabled documents attached directly to messages to deliver malware, and have increasingly used container files such as ISO and RAR attachments and Windows Shortcut (LNK) files.

According to an analysis of campaigned threats, which include threats manually analyzed and contextualized by Proofpoint threat researchers, the use of macro-enabled attachments by threat actors decreased approximately 66% between October 2021 and June 2022.

VBA macros are used by threat actors to automatically run malicious content when a user has actively enabled macros in Office applications. XL4 macros are specific to the Excel application but can also be weaponized by threat actors. Typically, threat actors distributing macro-enabled documents rely on social engineering to convince a recipient the content is important, and enabling macros is necessary to view it.

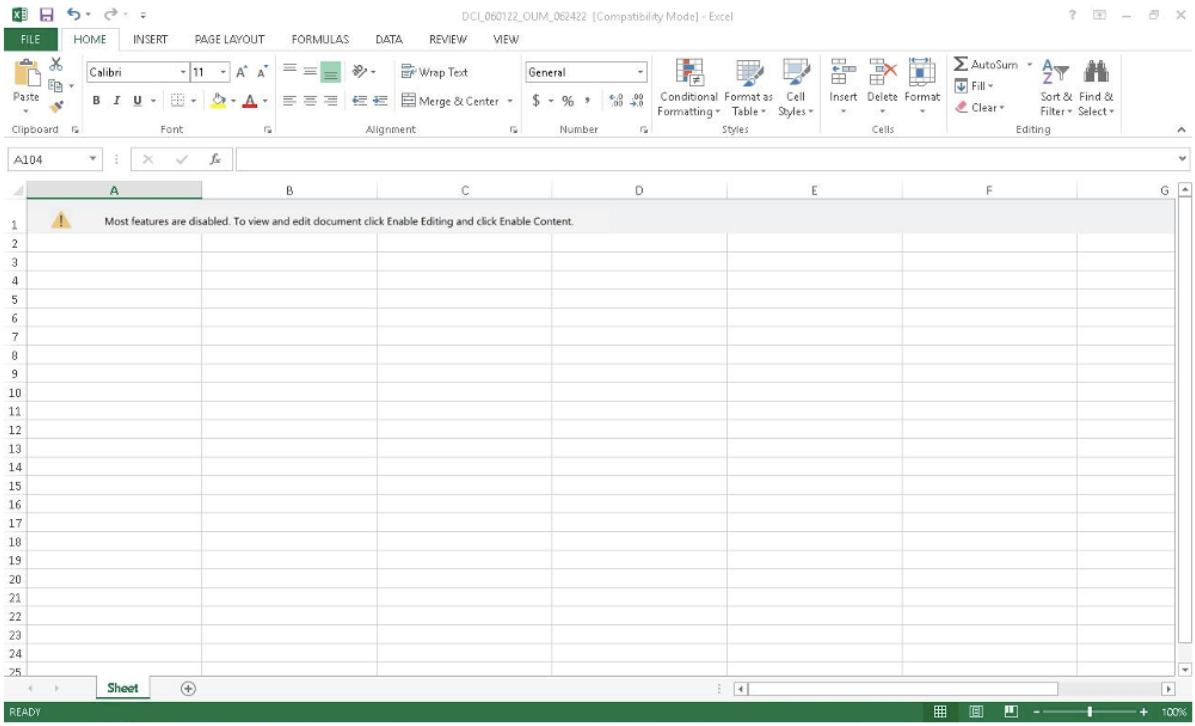

Figure 1: Emotet Excel attachment from a recent campaign.

Proofpoint researchers hypothesized threat actors would start transitioning away from macro-enabled documents directly attached to the message or downloaded via URL to bypass Microsoft's proposed defenses. While Proofpoint observed a notable increase in other attachment types, macro-enabled documents are still used across the threat landscape. Proofpoint researchers investigated the use of multiple filetypes since October 2021 through June 2022 to better understand the threat landscape and anticipate future behavior.

Bypassing Mark-of-the-Web

Microsoft will block VBA macros based on a Mark of the Web (MOTW) attribute that shows whether a file comes from the internet known as the Zone.Identifier. Microsoft applications add this to some documents when they are downloaded from the web. However, MOTW can be bypassed by using container file formats. IT security company Outflank detailed multiple options for red teamers to bypass MOTW mechanisms, and these techniques can be used by threat actors as well.

Threat actors can use container file formats such as ISO (.iso), RAR (.rar), ZIP (.zip), and IMG (.img) files to send macro-enabled documents. When downloaded, the ISO, RAR, etc. files will have the MOTW attribute because they were downloaded from the internet, but the document inside, such as a macro-enabled spreadsheet, will not. When the document is extracted, the user will still have to enable macros for the malicious code to automatically execute, but the file system will not identify the document as coming from the web.

Additionally, threat actors can use container files to distribute payloads directly. When opened, container files may contain additional content such as LNKs, DLLs, or executable (.exe) files that lead to the installation of a malicious payload.

Figure 2: Example attack chain using ISO attachments to deliver Bumblebee malware.

Proofpoint researchers initially hypothesized that XLL files may be increasingly favored in campaigns instead of macro-enabled documents. XLL files are a type of dynamic link library (DLL) file for Excel and are designed to increase the functionality of the Excel application. Proofpoint has seen a slight increase in the abuse of XLL files following Microsoft's announcement to disable XL4 macros in 2021, however these filetypes are still used significantly less than ISO, RAR, and LNK files, as well as macro-enabled documents.

Campaign Statistics

Proofpoint has observed a significant decrease in macro-enabled documents leveraged as attachments in email-based threats.

The number of these threats dropped over two-thirds between October 2021 and June 2022. In this same timeframe, the number of campaigns leveraging container files including ISO and RAR, and Windows Shortcut (LNK) attachments increased nearly 175%.

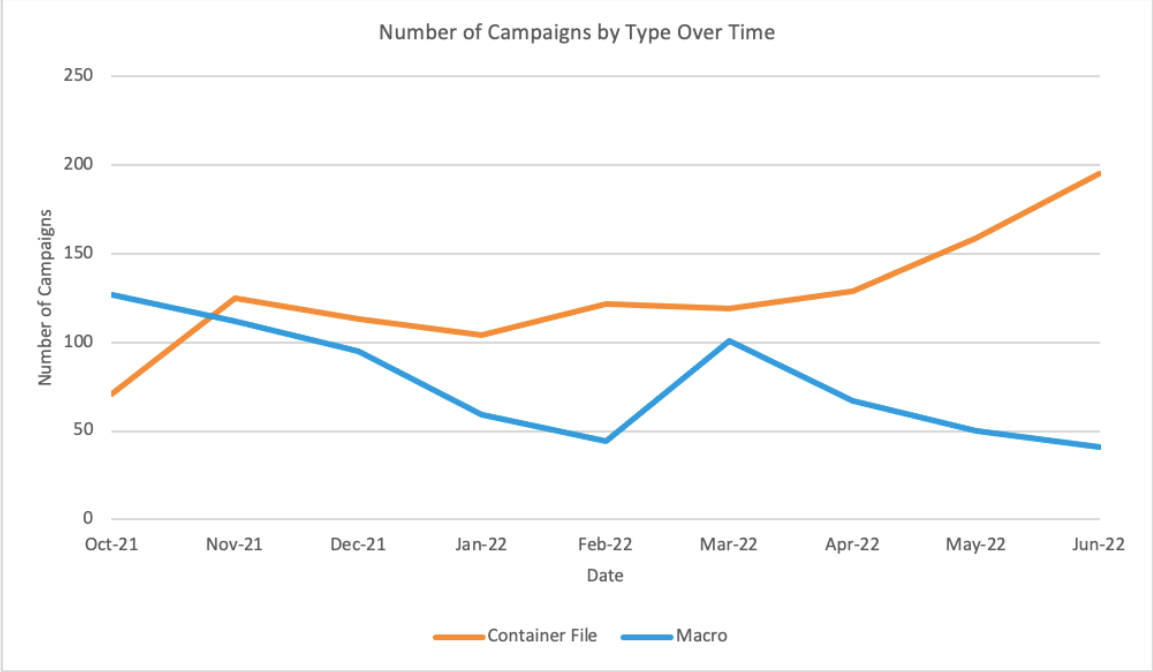

Figure 3: Number of campaigns leveraging container files vs macro-enabled documents as email attachments.

This increase is driven in part by the increased use of ISO and LNK files in campaigns. Cybercriminal threat actors are increasingly adopting these as initial access mechanisms, such as actors distributing Bumblebee malware. The use of ISO files increased over 150% between October 2021 and June 2022. More than half of the 15 tracked threat actors that used ISO files in this time began using them in campaigns after January 2022.

The most notable shift in campaign data is the emergence of LNK files; at least 10 tracked threat actors have begun using LNK files since February 2022. The number of campaigns containing LNK files increased 1,675% since October 2021. Proofpoint has tracked multiple cybercriminal and advanced persistent threat (APT) actors leveraging LNK files with increased frequency since October 2021.

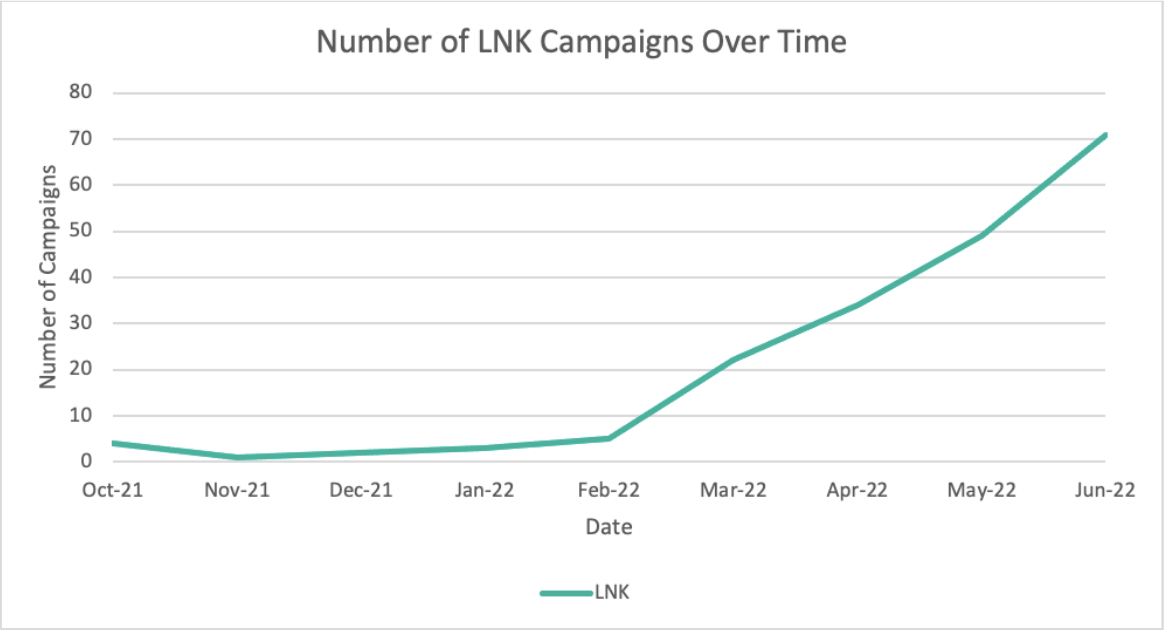

Figure 4: Number of campaigns leveraging LNK files.

Individual threat actor activities conducted by large cybercriminal groups have a notable impact on our data. For example, Proofpoint has observed a downward trend of threat actors using XL4 macros in campaigns. However, XL4 macro use spiked in March 2022. This is likely a result of TA542, the actor delivering the Emotet malware, conducting more campaigns with higher volumes of messages than preceding months. Typically, TA542 uses Microsoft Excel or Word documents containing VBA or XL4 macros. Emotet activity subsequently dropped off in April and it began using additional delivery methods including Excel Add In (XLL) files and zipped LNK attachments in subsequent campaigns.

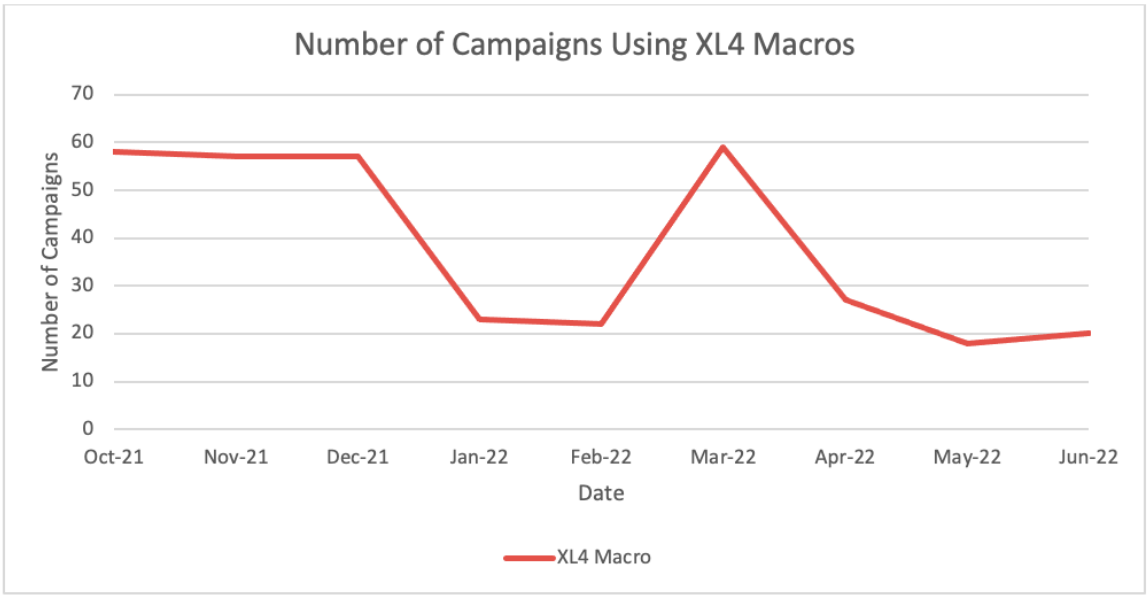

Figure 5: Number of XL4 macro-related campaigns October 2021 through June 2022.

The number of VBA macros also decreased overtime and included a small spike in March and April before dropping again in May and June 2022. This minor increase in Spring 2022 is not attributable to a single threat actor like TA542, rather multiple actors across the threat landscape were using VBA macros in this time.

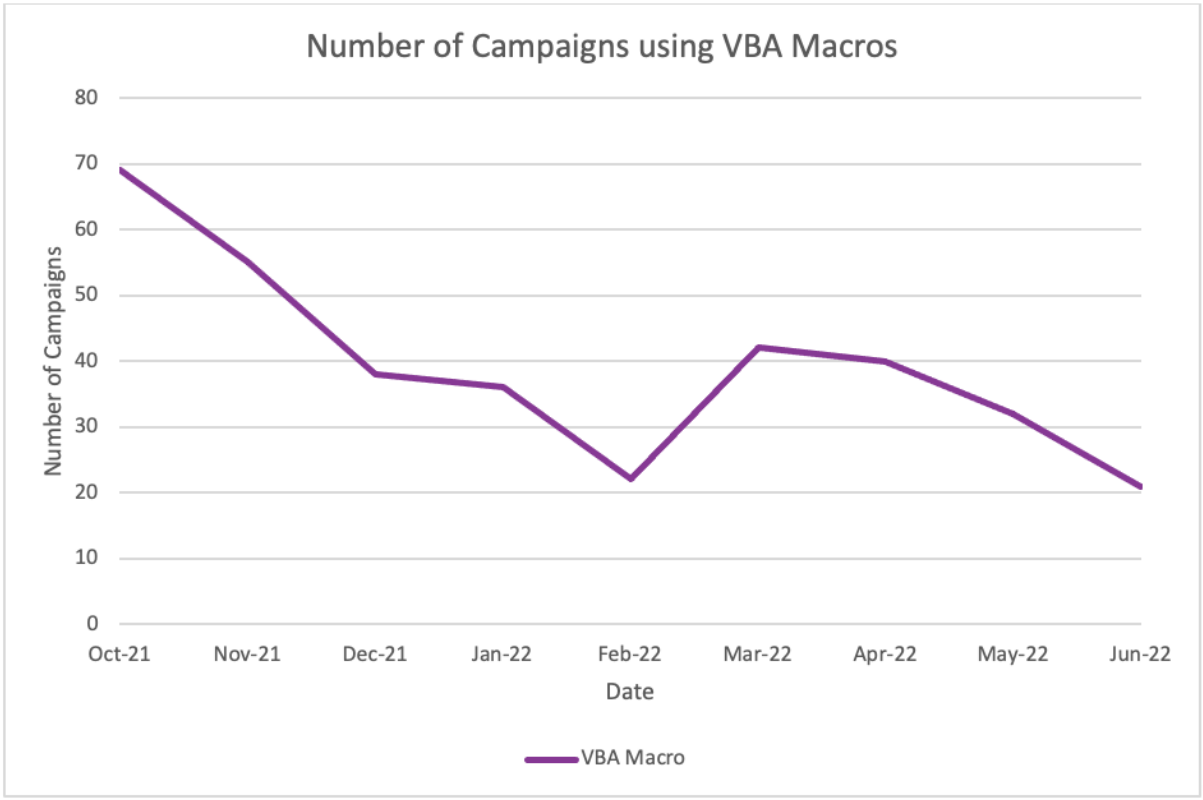

Figure 6: Use of VBA macros between October 2021 and June 2022.

Proofpoint has also observed a slight increase in threat actors using HTML attachments to deliver malware. The number of malware campaigns using HTML attachments more than doubled from October 2021 to June 2022, but the overall number remains low. Proofpoint researchers also observed threat actors increasingly adopt HTML smuggling, a technique used to "smuggle" an encoded malicious file within a specially crafted HTML attachment or web page.

Conclusion

Threat actors across the threat landscape are pivoting away from macro-enabled documents to increasingly use different filetypes for initial access. This change is led by the adoption of ISO and other container file formats, as well as LNK files. Such filetypes can bypass Microsoft's macro blocking protections, as well as facilitate the distribution of executables that can lead to follow-on malware, data reconnaissance and theft, and ransomware.

Proofpoint researchers assess with high confidence this is one of the largest email threat landscape shifts in recent history. It is likely threat actors will continue to use container file formats to deliver malware, while relying less on macro-enabled attachments.