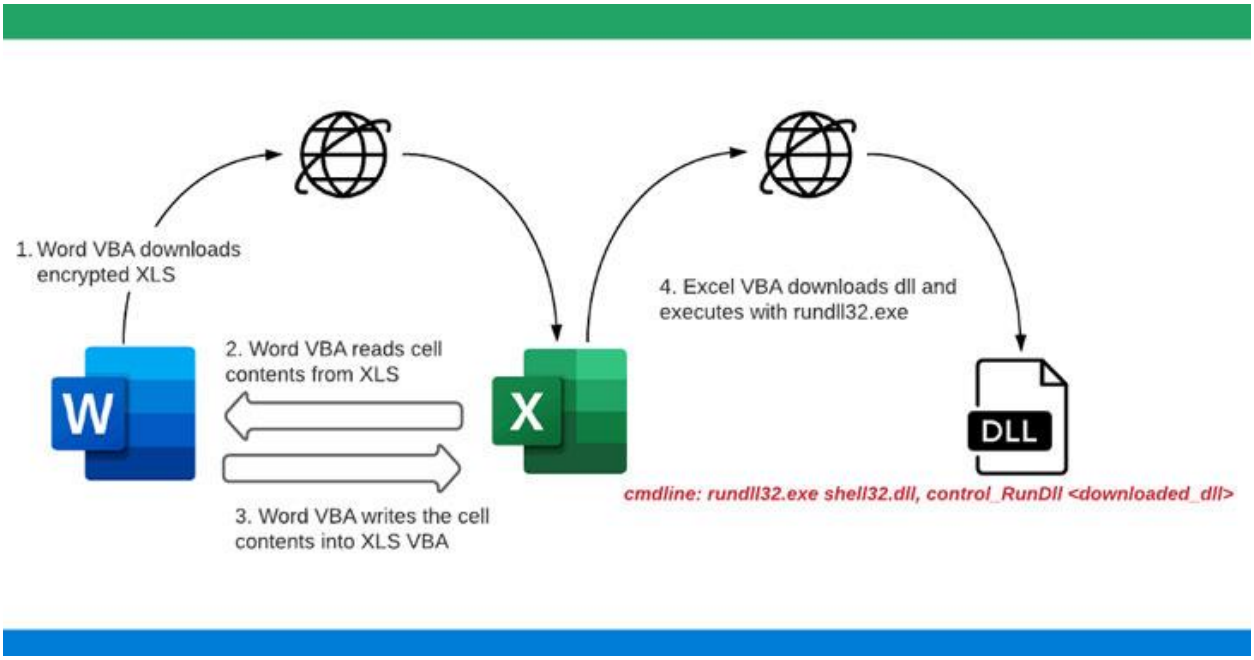
Hackers Use New Trick to Disable Macro Security Warnings in Malicious Office Files

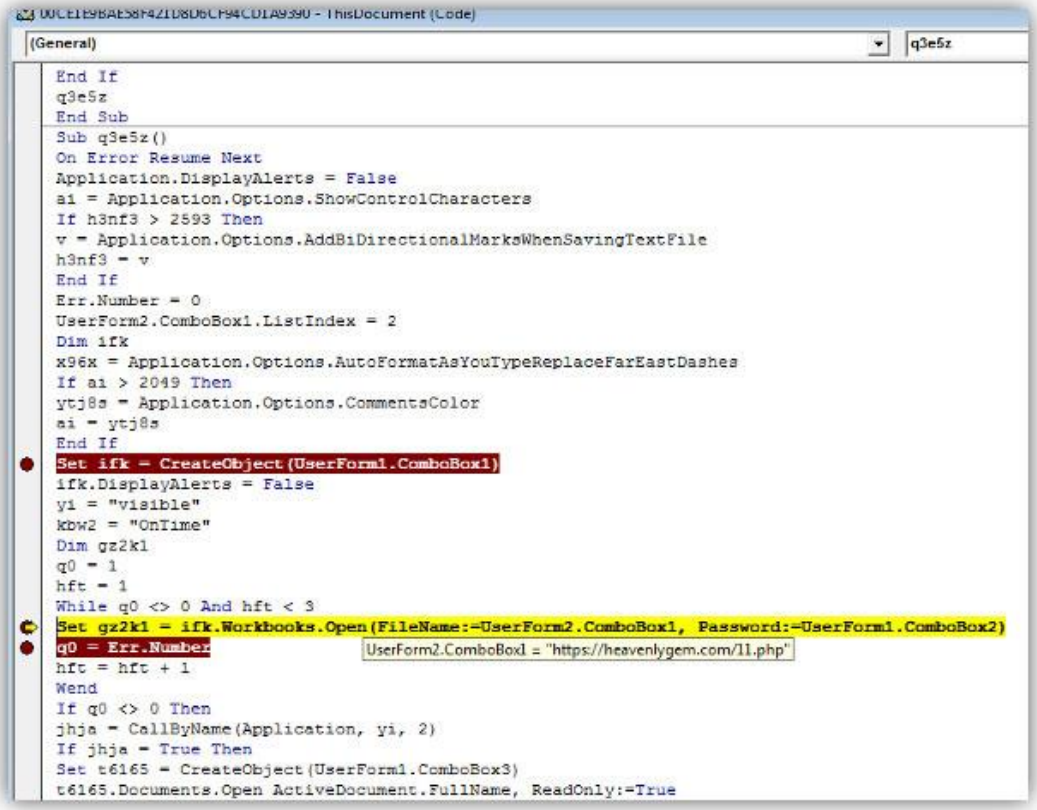


While it's a norm for phishing campaigns that distribute weaponized Microsoft Office documents to prompt victims to enable macros in order to trigger the infection chain directly, new findings indicate attackers are using non-malicious documents to disable security warnings prior to executing macro code to infect victims' computers.

In yet another instance of malware authors continue to evolve their techniques to evade detection, researchers from McAfee Labs stumbled upon a novel tactic that "downloads and executes malicious DLLs (ZLoader) without any malicious code present in the initial spammed attachment macro."

ZLoader infections propagated using this mechanism have been primarily reported in the U.S., Canada, Spain, Japan, and Malaysia, the cybersecurity firm noted. The malware — a descendant of the infamous ZeuS banking trojan — is well known for aggressively using macro-enabled Office documents as an initial attack vector to steal credentials and personally identifiable information from users of targeted financial institutions.

In investigating the intrusions, the researchers found that the infection chain started with a phishing email containing a Microsoft Word document attachment that, when opened, downloaded a password-protected Microsoft Excel file from a remote server. However, it's worth noting that macros need to be enabled in the Word document to trigger the download itself.



"After downloading the XLS file, the Word VBA reads the cell contents from XLS and creates a new macro for the same XLS file and writes the cell contents to XLS VBA macros as functions," the researchers said. "Once the macros are written and ready, the Word document sets the policy in the registry to 'Disable Excel Macro Warning' and invokes the malicious macro function from the Excel file. The Excel file now downloads the ZLoader payload. The ZLoader payload is then executed using rundll32.exe."

Given the "significant security risk" posed by macros, the feature is usually disabled by default, but the countermeasure has had an unfortunate side-effect of threat actors crafting convincing social engineering lures to trick victims into enabling them. By turning off the security warning presented to the user, the attacks are noteworthy because of the steps it takes to thwart detection and stay under the radar.

"Malicious documents have been an entry point for most malware families and these attacks have been evolving their infection techniques and obfuscation, not just limiting to direct downloads of payload from VBA, but creating agents dynamically to download payloads," the researchers said. "Usage of such agents in the infection chain is not only limited to Word or Excel, but further threats may use other living off the land tools to download its payloads."

Recommendations:

- Use the latest version of Office.
- Use an anti-malware product that integrates with the Anti Malware Scan Interface (AMSI) on Windows 10.
- Disable macros unless they are in trusted files.
- Block macros from the Internet.
- Reduce your dependency on macros.
- Disable macros across Office apps, and ensure users cannot re-enable them.
- Only enable macros for staff that rely on them every day.

References:

https://www.odysseycs.com/threat-alert/new-technique-for-disabling-macro-security-warnings-in-malicious-office-files-found

https://newsnationusa.com/news/technology/cyber-security/hackers-use-new-trick-to-disable-macro-security-warnings-in-malicious-office-files/

https://howtoremove.guide/new-technique-to-disable-office-files-macro-security-warning/

https://www.itsecuritynews.info/hackers-use-new-trick-to-disable-macro-security-warnings-in-malicious-office-files/

https://www.ncsc.gov.uk/guidance/macro-security-for-microsoft-office