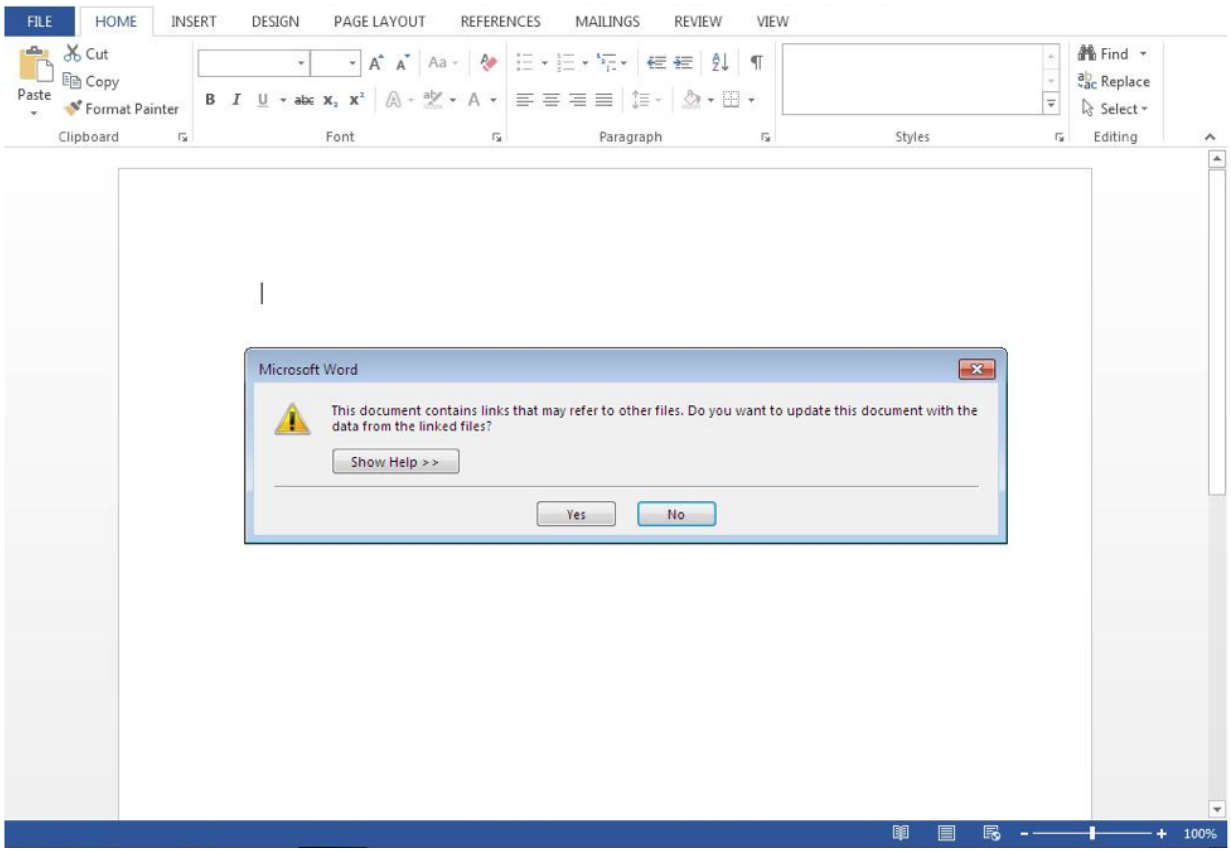
Microsoft patches document exploit vulnerability

April 12 2017, by Nancy Owano



Dialog box that appears when users open the document on vulnerable systems. Credit: Proofpoint

(Tech Xplore)—Many malware stories take the same story line, spread when computer victims open email attachments that enable installation

of malware on their devices.

Would you say that in 2017 there is anyone who has not heard the warning not to open email attachments from sources one is not sure about? Probably not if they have been working with computers for years. Still, socially engineered malware stories continue to flourish and this latest one is all about malware vis a vis Microsoft Word.

The BBC and numerous other sites carried the news that a bug in Word was apparently targeted by scammers trying to steal banking logins. Expectations were that Microsoft would get on it and it would be patched.

The latest on this from *Threatpost*: Microsoft on Tuesday released a patch for the zero-day vulnerability used to spread the Dridex banking Trojan.

Dan Goodin in *Ars Technica* had already alerted readers that "Researchers from multiple security companies have said the company plans to release a security update for the critical Word flaw on Tuesday as part of the company's normal Patch Tuesday routine."

Proofpoint discovered the Dridex spam campaign delivering Word documents weaponized with this zero-day malware. The BBC reported the bug was apparently targeted by spammers anxious to get at banking logins. "Dridex is designed to infect a victim's computer and snoop on banking logins."

The vulnerability had been reported and Proofpoint said it had discovered an email campaign —distributing Microsoft Word RTF [Rich Text Format] documents to recipients that had Dridex.

In other words, the Microsoft Office RTF documents in the wild were

exploiting the vulnerability.

Proofpoint's report: "This weekend saw multiple reports a new zero-day vulnerability that affected all versions of Microsoft Word. Today, Proofpoint researchers observed the document exploit being used in a large email campaign distributing the Dridex banking Trojan."

Interestingly, the recipients were across numerous organizations primarily in Australia, according to Proofpoint. And the perpetrators meant business. *BleepingComputer* said that the Dridex malware version delivered through the emails, which mimicked document scans, "contained configurations to target a slew of Australian banks."

The flaw was identified in versions of Microsoft Word for Windows, that would enable Dridex to be installed.

On Monday, Proofpoint posted an article, "Dridex Campaigns Hitting Millions of Recipients Using Unpatched Microsoft Zero-Day."

In *BleepingComputer*, Catalin Cimpanu referred to a statement from a Microsoft spokesperson, who said, "We plan to address this through an update on Tuesday April 11."

According to the BBC, Proofpoint also urged Microsoft Word users to install the security updates quickly. Considering a rapid weaponization of the exploit, it was critical that users and organizations applied the patch as soon as it became available, the firm said.

Lucian Constantin , IDG News Service, said that "Security vendors have also recommended that Microsoft Word users enable the Protected View mode, which can block this exploit from working."

Does all this attention mean that people will get wise to not opening

attachments from people they are not expecting to get such attachments? To be fair to victims who still do, the digital world is not that simple, where you have cautious users on one side and careless users on the other.

BleepingComputer made a case for a middle zone, where some work environments make it difficult to ignore attachments.

"The advice of not opening files from the people you don't know is not really that helpful for employees working with scanned documents on a daily basis in a business environment, where they regularly have to open scanned documents and Word files from unknown (potential) business partners."