



Passwords used for targeted attacks

Goodmorning,

I wanted to share with you a Symantec Security Response blog about password being used for targeted attacks. The blog can be found here and related information is available here.

Given below are a few key points I wanted to highlight to you from the blog.

For magicians, one of the most important tools in their bag of tricks is the concept of misdirection. As you watch one hand, the other hand pulls off the trick. Recently there has been an increase in the theft of logon data, such as user names, email addresses, and passwords being stolen from various websites. The primary concern is that logon data has been compromised. However, hackers today are modern magicians; you will see that there is more than meets the eye when you understand the true risk.

Symantec has continuously observed targeted attacks in the wild since around mid-July that utilize password-protection of malicious Excel spreadsheet files. This is not the first time that passwords have been used for targeted attacks. The purpose of the attacker using the password is most likely to enable malware to evade detection, whether on the gateway or on the desktop, since the password feature encrypts the files. It may also make security researchers' work or automatic analysis difficult since the password is required to decrypt the file before investigation can be performed. The usage of the password might also make the recipients feel safe about the file as passwords are generally used for security measures.

The attacks themselves are no different from typical targeted attacks except for the use of the password. Although scanning the typical password-protected file is not possible, security products can still prevent infection by detecting the dropped or downloaded files just like with other types of targeted attacks. With the implementation of multi-layered defense, one should not be in more danger than someone being attacked by typical targeted attacks. It is now more common to see password-protected malware attached to emails, so users need to watch out not only for Excel files, but any type of files with passwords that are attached to unsolicited emails.

Some attackers who steal logon data do not use it just for their own personal gain. They freely post plain-text passwords and password hashes online where other attackers can find them—in public forums or uploaded to torrent sites, for instance. So, it's not just one hand performing the magic trick, it's several hands.

If you have any questions or would like to speak with a security expert from Symantec, please let me know.

Thanks,

Aaron

For more information please contact: Aaron Crowther

Max Australia

+61 2 9469 5749

aaron.crowther@maxaustralia.com.au

Debbie Sassine

Symantec Corporation

+61 2 9086 2140

debbie_sassine@symantec.com