Serianu Cyber Security Advisory

Malicious Attachments

Serianu SOC Advisory Number:

TA – 2020/014

Date(s) issued:

22nd September, 2020

Overview

Malicious attachments continue to be a top threat vector in the cybercriminal world even as public awareness increases. While attachment threat vectors are one of the oldest malware-spreading tricks, email users are still clicking on malicious attachments that hit their inbox, whether it's an alleged job offer or a pretend critical invoice.

According to our research, the reason why threat actors are still relying on this age-old tactic, is that the attack is still working. Even with widespread public awareness about malicious file attachments, attackers are upping their game with new tricks to avoid detection, bypass email protections and more. The attack vector is still widespread enough, where tech giants are re-inventing new ways to try to stomp it out, with Microsoft rolling out a feature for Office 365 that aims to protect users against malicious attachments sent via email.

Email attachments such as PDF or Office files, are an easy vector to deliver malicious content to end users. For enterprises, the risk is that malicious actors can use these attachments to establish a toe-hold at the outermost edges of the enterprise and then wait and wind their way to the crown jewels in their data stores.

New Tactics

According to our research, email attachment tops the malware vector list. This leads to data breaches, with almost 20 percent of malware attacks being deployed via email attachments. Email links are the top vector with 40 percent of attacks using this method. While malware-laced attachments such as ZIPs, PDF and MS office files, including DOC and XLSM file attachments are more commonly used attachments. Serianu warns that threat actors are starting to look for newer attachments like disc image files (ISO or IMG files that store the content and structure of an entire disk, like a DVD or Blue-Ray) as a way to increasingly spread malware.

The use of social engineering to convince targets to open the attachment is also evolving. We noted huge spikes in spam campaigns last year that were utilizing DOC and XLSM (macro-enabled spreadsheet created by Microsoft Excel) files to deliver the Trickbot, a modular banking trojan. It got

worse this year with the current pandemic, as cyber attackers look to send malicious attachments under the guise of Covid information, work from home related resources and other critical information.

Updated Defenses

Even while threat actors step up their email-based attacks, email providers and productivity application companies are also taking steps forward to stomp out this common threat vector.

In 2019, Microsoft banned almost 40 new types of file extensions on its Outlook email platform, in hopes that the move would prevent users from downloading email attachments with various file extensions, including ones associated with Python, PowerShell, digital certificates and Java. Google has a similar policy for its Gmail email service and has blocked certain types of files, including their compressed form like .gz or .bz2 files or when found within archives .zip or .tgz files.

Microsoft rolled out a long-anticipated Office 365 feature, Application Guard for Office, which isolates Office 365 productivity application files including Word, PowerPoint and Excel that are potentially malicious. The tool takes aim at a common attack vector, spear phishing campaigns and other web-based attacks which will use Word documents or other Office based attachments as a vehicle for malware. The feature is currently available on public preview. This is a status where the Microsoft product or service isn't complete but is made available on a preview basis so that customers can get early access and provide feedback.

Application Guard specifically protects against files that are downloaded from domains that aren't part of either the local intranet or trusted sites domain on a user's device, files that were received as email attachments from senders outside the user's organization, files that were received from other kinds of internet messaging or sharing services or files opened from a OneDrive or SharePoint location outside the user's organization.

Recommendations.

- Users to update their softwares in order to get all the necessary upgrade features.
- Organisations need to properly configure their Active Directory.
- User training and the willingness of corporates to prioritize protecting against attachment-based threat vectors, are important steps in defending against these types of attacks.
- Users to check that the sender's email address is correct. Remember that domain names and display names can easily be spoofed.
- Do not open attachments from unknown sources. Users should immediately alert IT security when they observe unsolicited emails containing attachments.
- Install endpoint and server-based antivirus scanners
- Make sure spam filtering is enabled on your email account.

Information Sharing

As a means of preventing such attacks from occurring, we encourage any organisation or individual that has access to malicious attachments share it with us through our email: info@serianu.com to allow us analyze and share IOC's.