Asruex Backdoor Infects Files Via Old Vulnerabilities

blog.trendmicro.com/trendlabs-security-intelligence/asruex-backdoor-variant-infects-word-documents-and-pdfs-through-old-ms-office-and-adobe-vulnerabilities/

August 22, 2019

Since it first emerged in 2015, Asruex has been known for its backdoor capabilities and connection to the spyware DarkHotel. However, when we encountered Asruex in a PDF file, we found that a variant of the malware can also act as an infector particularly through the use of old vulnerabilities CVE-2012-0158 and CVE-2010-2883, which inject code in Word and PDF files respectively. The use of old, patched vulnerabilities could hint that the variant was devised knowing that it can affect targets who have been using older versions of Adobe Reader (versions 9.x up to before 9.4) and Acrobat (versions 8.x up to before 8.2.5) on Windows and Mac OS X. Because of this unique infection capability, security researchers might not consider checking files for an Asruex infection and continue to watch out for its backdoor abilities exclusively. Awareness of this new infection method could help users defend against the malware variant.

Technical details

Asruex infects a system through a shortcut file that has a PowerShell download script, and spreads through removable drives and network drives. The diagram below illustrates the malware's infection chain.

Figure 1. Infection chain of Asruex

Infected PDF files We first encountered this variant as a PDF file. Further investigation revealed that the PDF file itself was not a malicious file created by the actors behind this variant. It was simply a file infected by the Asruex variant. Infected PDF files would drop and execute the infector in the background if executed using older versions of Adobe Reader and Adobe Acrobat. As it does so it still displays or opens the content of the original PDF host file. This tricks the user into believing that the PDF had acted normally. This behavior is due to a specially crafted template that takes advantage of the CVE-2010-2883 vulnerability while appending the host file. The vulnerability is found in the strcat function of Adobe's

CoolType.dll, which is a typography engine. Since this function does not check the length of the font to be registered, it can cause a stack buffer overflow to execute its shellcode. Finally, it decrypts the original PDF host file using XOR. This process is seen in the images below.

Figure 2. Vulnerability being exploited by the variant

Figure 3. Decrypting the original PDF host file

It will then drop and execute the embedded executable detected as Virus.Win32.ASRUEX.A.orig, as seen in figure 4.

Figure 4. The embedded executable dropped by the malware

This executable is responsible for several anti-debugging and anti-emulation functions. It detects if avast! Sandbox\WINDOWS\system32\kernel32.dll exists on any root, as an anti-debugging measure. It then checks the following information (listed below), to determine if it is running in a sandbox environment:

- Computer names and user names
- Exported functions by loaded modules
- File names
- Running processes
- Module version of running process
- Certain strings in disk names

The executable file also injects the DLL c982d2ab066c80f314af80dd5ba37ff9dd99288f (detected as Virus.Win32.ASRUEX.A.orig) into a legitimate Windows process memory. This DLL is responsible for the malware's infection and backdoor capabilities. It infects files with file sizes between 42,224 bytes and 20,971,520 bytes, possibly as a parameter to narrow down host files into which their malware code could fit.

Figure 5. Screenshot showing the added process

Figure 6. Template that the infector uses to infect PDF samples; the filename of the executable is highlighted

Infected Word documents As mentioned earlier, it uses a specially crafted template to exploit the CVE-2012-0158 vulnerability to infect Word documents. The template is highlighted in figure 7.

Figure 7. Template used to infect Word documents

The CVE-2012-0158 vulnerability allows possible attackers to execute an arbitrary code remotely through a Word document or web site. Similar to infected PDFs, it will drop and execute the infector in the background upon execution of the infected Word document file. At the same time, it will display the original

DOC host file, letting users believe that the opened document is normal. The infected file would use XOR to decrypt the original DOC host file, as seen in figure 8. The file would open like normal, with the only difference found in the filename used by the infector. It drops and executes itself as rundll32.exe (figure 9).

Figure 8. Use of an XOR to decrypt the original DOC host file

Figure 9. Use of a different file name to drop and execute the infector

Infected executables Aside from the Word documents and PDF files, the malware also infects executable files. This Asruex variant compresses and encrypts the original executable file or host file and appends it as its .EBSS section. This allows the malware to drop the infector, while also executing the host file like normal. For infected executable files, the filename used by the infector when dropped is randomly assigned, as illustrated in figure 11.

Figure 10. Code showing the host file being appended to the malware’s .EBSS section

Figure 11. Random filename used for the dropped infector

Conclusion and security recommendations

As mentioned earlier, past reports have tagged Asruex for its backdoor capabilities. The discovery of this particular infection capability can help create adequate defenses against the malware variant. This case is notable for its use of vulnerabilities that have been discovered (and patched) over five years ago, when we’ve been seeing this malware variant in the wild for only a year. This hints that the cybercriminals behind it had devised the variant knowing that users have not yet patched or updated to newer versions of the Adobe Acrobat and Adobe Reader software. Understandably, this could pose a challenge for organizations as updating widely-used software could result in downtime of critical servers, and it could be costly and time consuming. If patching and updating might not be a present option, organizations can consider security measures like virtual patching to help complement existing security measures and patch management processes. In general, users can take the necessary measures to defend against similar threats by following security best practices. We list down some of the steps users can take to defend against Asruex and similar malware:

- Always scan removable drives before executing any file that may be stored in it.
- Avoid accessing suspicious or unknown URLs.
- Be cautious when opening or downloading email attachments, especially from unknown or unsolicited email.

Users and enterprises can also benefit from a solution that uses a multilayered approach against threats that are similar to Asruex. We recommend employing endpoint application control that reduces attack exposure by ensuring that only files, documents, and updates associated with whitelisted applications and sites can be installed, downloaded, and viewed. Endpoint solutions powered by XGen™ security such as Trend Micro™ Security and Trend Micro Network Defense can detect related malicious files and URLs and protect users’ systems. Trend Micro™ Smart Protection Suites and Trend Micro Worry-Free™ Business Security, which have behavior monitoring capabilities, can additionally protect from these types of threats by detecting malicious files, as well as blocking all related malicious URLs.

Indicators of Compromise (IoCs)

SHA256	Detection Name
b261f49fb6574af0bef16765c3db2900a5d3ca24639e9717bc21eb28e1e6be77	Virus.Win32.ASRUEX.A.orig

Cyber Threats

Asruex has been known for its backdoor capabilities. However, when we encountered Asruex in a PDF file, we found that a variant of the malware can also act as an infector particularly through the use of old vulnerabilities.

By: Ian Mercado, Mhica Romero August 22, 2019 Read time: (words)

Content added to Folio