Life After Death—SmokeLoader Continues to Haunt Using Old Vulnerabilities

August 9, 2022

Vulnerability management and remediation are some of the most difficult problems to tackle within an organization. Multiple solutions, watchlists, and warnings are designed to ensure that companies and end users patch their software against known security vulnerabilities.

Unfortunately, even with tools available and teams forewarned with up-to-date information, this often does not happen in a timely manner or even at all. This is usually due to outdated software, overworked teams, or even negligence or incompetence—and threat actors know this. Patching is often mundane and tedious work. Organizations that are either late, inconsistent, or sloppy in applying patches often become victims by presenting an opening to threat actors searching for an exploitable foothold.

Case in point, CVE-2017-0199 and CVE-2017-11882 are almost over five years old, but they are still being exploited. Worse, both vulnerabilities have had official patches for some time, yet they continue to be exploited.

In this blog, we will examine a recent instance of SmokeLoader, a malware variant that exploits both of these CVEs in its deployment chain. SmokeLoader (also known as Dofoil) has been available on the market in one form or another since 2011. Its primary purpose is to support the distribution of other malware families, such as Trickbot. This latest sample drops zgRAT, a somewhat rare payload compared to what SmokeLoader usually delivers.

Affected Platforms: Windows
Impacted Users: Windows users
Impact: Potential to deploy additional malware for additional purposes
Severity Level: Medium

Looking at each element of the attack

I will examine each attack element in the following sections, including the initial email, attachments, and executables.

The phishing email

Like many phishing stories, this one starts with a lure urging the recipient to review a purchase order and check for dates related to shipping times to ensure they are correct. This email was sent to a webmail address hosted by a large telecommunications company in Taiwan. The phishing email's sender also used this service, making it impossible to trace the precise origin of the message. Oddly, and perhaps a tell that this is a phishing attempt, the sender spoofed the recipient's address and used it as the sending address.

The body text is a mix of Chinese and English and goes to some degree of trouble to look as legitimate as possible, showing a full signature with contact details.

Figure 1. Phishing email.

Figure 2. Phishing email translation to English.
As shown in Figure 1, the file "Purchase Order FG-20220629.xlsx" is attached to the email. Opening this file begins the process of infection.

Purchase Order FG-20220629.xlsx

Figure 3. Spreadsheet as it would appear to the recipient.
When opened, the recipient is presented with a fairly standard view of a pixelated image and faux Microsoft instructions on viewing protected content.

Given there aren't any macros, a closer look at the internals of the spreadsheet is needed. The lock icon for Sheet2 shows that there is likely an encrypted or protected sheet. A tool like oledump from Didier Stevens can help in a situation like this.

Figure 4. oledump output showing an encrypted stream.
After running oledump, it becomes evident that there is an encrypted stream in the file that most likely includes some details of interest. Another tool by Didier Stevens – msoffcrypto-crack.py – can be checked for obvious and well-used passwords.

Figure 5. msoffcrypto-crack.py output showing the password of the file.
In this instance, a return of “VelvetSweatshop” is given. This is interesting as this is effectively a default document password recognized by Excel. It allows data to be encrypted but won’t prompt a user to enter a password to access the file.

By combining the two tools mentioned above using a pipe (“|”), the full decrypted scope of the OLE stream in question is provided, and the target of the next stage of the attack is shown. This stage uses the first of the two exploits involved in this attack, CVE-2017-0199. It also includes an embedded link that will attempt to download the file “receipt.doc” from 192[.]227[.]129[.]26

Figure 6. The ultimate target for the spreadsheet after exploiting CVE-2017-0199.

Figure 7. Oddities in the file evident from the Exif data.
Initial analysis of “receipt.doc” turns up some interesting oddities. As shown in Figure 7, Exiftool (a tool for examining file metadata) returns an error when run against “receipt.doc”. Opening the file and viewing it directly shows the scope of what is being attempted.

Figure 8. “receipt.doc” as it would appear to anyone viewing it.
It becomes immediately apparent that this file is not a Microsoft Word document. Instead, it is a Rich Text File (RTF). This file is designed to take advantage of the second of the two vulnerabilities mention, CVE-2017-11882, a stack overflow vulnerability in the Microsoft Equation Editor that enables remote code execution on a vulnerable system.

Figure 9. The ultimate target for the spreadsheet after exploiting CVE-2017-11882.
The “receipt.doc” file reaches out again to 192[.]227[.]129[.]26 and downloads vbc.exe. This is SmokeLoader.

vbc.exe

Starting at the beginning with “vbc.exe” and viewing its details as seen by the operating system, this file presents itself as a Microsoft .NET executable.

Figure 10. Basic executable details for “vbc.exe”.
A review of the metadata for the file shows a basic level of misdirection.

Figure 11. Exif data showing “vbc.exe” obfuscating its true purpose.
The file is described as “WinRAR” (legitimate file compression and archiving software). In addition, the original and current file names do not match, which is highly suspicious given the circumstances up to this point.

Viewing the executable in a .NET debugger or IDE offers more explicit details on what the program attempts to do and how.

Figure 12. The ultimate target for “vbc.exe”.
An attempt to connect to the URL “sorathlions[.]com/wp-content/Vymxn_Zfbgctbp[.]jpg” will be made.

Figure 13. Packet capture showing multiple connections over a very short period.

If a connection cannot be made, numerous retries occur. However, they are done at a very fast rate (several per minute) that would present a detection opportunity given the uncharacteristic and ceaseless attempts to connect to this location.

Figure 14. If “vbc.exe” successfully connects to its C2, it will execute the above command.
A successful connection will pull the file “Vymxn_Zfbgctbp.jpg” from its remote location, and the command in Figure 14 will be executed.

Vymxn_Zfbgctbp.jpg

The code in Figures 12 and 14 indicates that “Vymxn_Zfbgctbp.jpg” may not be an image file as claimed.

Figure 15. Exif data confirms that “Vymxn_Zfbgctbp.jpg” is not an image.
A review of the file’s metadata shows that it appears to be a compressed GZip archive. Figure 12 appears to bear this out, with the code to decompress the file in memory. In the absence of that, the file can be decompressed manually using common tools like 7Zip.

Figure 16. Demonstrating “Vymxn_Zfbgctbp.jpg” can be decompressed manually.

Figure 17. The final file to be dropped is a DLL.
As Figure 17 shows, the file that gets dropped is a .NET DLL that would be executed by “vbc.exe”.

DLL

The DLL is heavily obfuscated. However, it’s still possible to pick out the primary namespace, class, and entry function.

Figure 18. Primary namespace.
Based on some of the non-obfuscated strings in this DLL, FortiGuard Labs believes this sample is zgRAT. Samples of zgRAT date back to 2021. It is a somewhat rare malware variant compared to other more established lines.

This particular sample makes no effort to communicate out and mostly idles without taking any further offensive action.

Conclusion

While CVE-2017-0199 and CVE-2017-11882 were discovered in 2017, they are still being actively exploited in this and other malware campaigns. This demonstrates that malware authors still achieve their aims by relying on aging vulnerabilities, often several years after coming to light, and banking on affected solutions not being fixed.

The staying power of SmokeLoader, shown by its relative longevity compared to other threats, shows no signs of slowing down for the foreseeable future.

Fortinet Protections

The samples mentioned in this blog are detected by the following (AV) signatures:

VBA/Agent.BMW!tr.dldr

MSOffice/CVE_2017_11882.B!exploit

MSIL/Agent.MJR!tr.dldr

MSIL/Injector.VZX!tr

FortiGuard IPS protects against all known exploits associated with the CVE-2017-0199 with the following signature:

MS.Office.RTF.File.OLE.autolink.Code.Execution

FortiGuard IPS protects against all known exploits associated with the CVE-2017-11882 with the following signature:

MS.Office.EQNEDT32.EXE.Equation.Parsing.Memory.Corruption

All network-based URIs are blocked by the WebFiltering client.

Fortinet has multiple solutions designed to help train users to understand and detect phishing threats:

The FortiPhish Phishing Simulation Service uses real-world simulations to help organizations test user awareness and vigilance to phishing threats and to train and reinforce proper practices when users encounter targeted phishing attacks.

In addition to these protections, we suggest that organizations also have their end users go through our FREE NSE training: NSE 1 – Information Security Awareness. It includes a module on Internet threats designed to help end users learn how to identify and protect themselves from various types of phishing attacks.

IOCs:

Filename	SHA256
Purchase Order FG-20220629.xlsx	eef3295bada101787ae4f1ebc92e17fc2c6cd8c39389a745c45943a019637ca1
receipt.doc	a1f59ebe9e8311267d831da649a8df44a3d747e9cf75e64a259b2fd917d2f587
vbc.exe	3223ae2c88753ce7268fa02213b76bdaf690ac37ec411ea8b7925c3b31e8822f
Vymxn_Zfbgctbp.jpg	104f88876b4d7c963d47afa63cfbb516d20e1cf9858d739f9c4023142b223fe2
Vymxn_Zfbgctbp.dll	4e4e32f6259b82e6b932ab81172c22560ec2ac46e85543d4851637a63eaace3e

Network IOCs:

sorathlions[.]com
dhemgldxkv[.]com
afrocalite[.]com
108[.]60[.]212[.]220

Learn more about Fortinet’s FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.