N. Shkoliar, PhD in Ped., As. Prof.
M. Bahrii, Student
Khmelnytsky National University

UNDERSTANDING THE TREAT OF DISGUISED MALWARE BEHIND A SOCIAL ENGINEERING

Social engineering is an attack vector that relies heavily on human interaction and often involves manipulating people to violate normal security procedures to gain unauthorized access to systems, networks, or physical locations or to gain financial gain.

Attackers use social engineering techniques to conceal their true goals and motives by posing as trusted individuals or sources of information. The goal is to influence, manipulate, or trick users into disclosing confidential information or access to the organization. Many social engineering experiments rely on people's willingness to be helpful or fear of punishment. For example, an attacker might pretend to be a colleague who has an urgent problem that requires access to additional network resources.

Social engineering is a popular tactic among attackers because it is often easier to exploit people than to find a vulnerability in a network or software. Hackers often use social engineering tactics as the first step in a large company to penetrate a system or network and steal sensitive data or spread malware [1].

Millions of spam messages are sent every day, and while most of them are harmless advertisements, one of them may eventually contain a malicious file. To get the recipient to click and open a file that downloads a malicious program, cybercriminals make it look interesting, useful, or important: a working document, a lucrative offer, a gift card with a well-known company logo, etc.

Cybercriminals like to hide malware in files such as ZIP and RAR. For example, they used ZIP files named Love_0123 (the digits may vary) to distribute the GandCrab ransomware on Valentine's Day. A few weeks later, a group of fraudsters sent files with the Qbot Trojan, which specializes in data theft [2].

Microsoft Office documents also have their own vulnerabilities. Microsoft Office files, all Word documents (DOC, DOCX), Excel spreadsheets (XLS, XLSX, XLSM), presentations, and templates are also very popular among cybercriminals. These files may contain embedded macros, small programs that run within the file that cybercriminals use as scripts to download malware [2].

Microsoft's response to the surge in malware attacks includes blocking Excel XLL add-ins online starting in March 2023, according to The Register. The move aims to reduce the risk posed by cybercriminals using this increasingly popular attack vector. Following the precedent set in July 2022 when Microsoft began blocking VBA macros in Word, Excel, and PowerPoint by default, hackers have adapted their tactics to turn to alternative methods such as LNK files and ISO and RAR attachments. Excel XLL files have become another security concern, as researchers have noted a significant increase in their use. Jake Moore, Global Security Advisor at ESET, emphasizes the attractiveness of Microsoft Office to cybercriminals due to its widespread use among computer users. Macros built into popular editors such as Excel and Word have become prime targets, often exploited through innocuous user actions such as clicking the

"Enable Macros" or "Enable Content" button. This single action can trigger a devastating attack that often leads to the compromise of a computer with a ransomware virus [3].

Many users are aware of the dangers of macros in Microsoft Office documents, but are generally unaware of the traps hidden in PDF files. In fact, this format can be used to create and run JavaScript files.

In addition, cybercriminals like to hide malicious links in PDFs. For example, in a spam campaign, fraudsters encouraged users to visit a "secure" page where they had to log in to their American Express account. Of course, the victims' credentials were sent directly to the fraudsters.

Compared to the previous formats, IMG and ISO files are not very often used for malware attacks, although cybercriminals have recently been paying attention to them. These files (disk images) are actually a virtual copy of a CD, DVD, or other type of disk.

Malware often uses social engineering techniques to disguise itself and deceive users. One common technique is to use specially created icons that resemble legitimate document files. Additionally, malware can use dual extensions, such as ".pdf.exe" or ".doc.exe", by exploiting Windows defaults that hide file extensions. It is also possible to use lesser known executable extensions such as ".scr" [2].

However, there are two less common tricks that can further mislead users: PIF extensions: this trick hides both the actual file extension and its original icon, even if the user has disabled the extension hiding feature in Windows. For example, an executable file named "file.txt.pif" will be displayed as "file.txt" with the hidden extension ".pif". Double-clicking on it will still run the file, as it functions as an "MS-DOS Program Shortcut". The PIF extension has been used in recent campaigns such as Petya/Mischa [4].

RTLO (right-to-left override): this trick takes advantage of the fact that certain languages are written from right to left, unlike most countries where writing is done from left to right. The Unicode character U+202e can be used to switch between these two writing modes. Attackers can use this character to replace the displayed extensions. To demonstrate the trick, you can create an executable file with the extension ".scr" and then use the Unicode character to make it look like it has the extension ".txt". By changing the file icon, it can look like a regular text file. However, after checking the details of the file, the actual file type, such as a screensaver, will be revealed. Renaming the file also shows a broken selection pattern [4].

Another way malware can mislead users is by using a misleading file name, such as "document.pdf.exe". In this case, the malware author uses standard Windows behavior to hide known file extensions. When a user receives a file named "document.pdf.exe", the ".exe" extension is hidden and it appears as "document.pdf", resembling a harmless PDF document [4].

Let's talk about what an .exe file is. Exe in this context is a file extension that denotes an executable file for Microsoft Windows. File names in Windows consist of two parts. The file name, followed by a period and the extension. The extension is a three- or four-letter abbreviation that indicates the type of file [5].

An .exe file may be a virus, but this is certainly not the case with all files. Although most exe files are safe, they can also pose a threat to your computer. If you are not sure which file to open, don't do it. If you download exe files from an unknown

source, you may encounter viruses or malware that can harm your computer. When it comes to downloaded files, it is always better to be careful [5].

Self-extracting archive files (SFX) are a special type of archive files that have the ability to automatically unpack their contents without requiring external unpacking software. They combine the functionality of an archive file and an executable file, allowing recipients to unpack the files they contain without the need for a separate unpacking tool. SFX archive files have a legitimate use, as they provide a convenient way to distribute compressed files to recipients who may not have the necessary software to unpack them. An SFX file contains both the compressed data and a program that can automatically decompress the files on startup. Hidden malicious functionality in SFX files can be designed to bypass traditional detection mechanisms. For example, the file can execute malicious code during the unpacking process, change system settings, or perform other unauthorized actions on the recipient's computer [6].

To summarize, malware can use a variety of methods to spoof extensions, and simply disabling the option to hide extensions in Windows is not a viable solution. It is very important to remain vigilant when downloading files, despite their seemingly harmless extensions and icons. To avoid falling victim to this trick, it is important to be careful when downloading or opening files. Always check the file type and beware of suspicious or unexpected file extensions, especially if they seem mismatched to the expected content.

REFERENCES

1. What is social engineering? [Електронний ресурс] https://www.techtarget.com/searchsecurity/definition/social-engineering.
2. What are the four most dangerous file types? [Електронний ресурс] https://www.perallis.com/blog/what-are-the-four-most-dangerous-file-types.
3. Microsoft Office: небезпечні надбудови Excel XLL. [Електронний ресурс] https://b2b-cyber-security.de/uk/microsoft-office-gefaehrliche-excel-xll-add-ins/
4. Lesser known tricks of spoofing extensions. [Електронний ресурс] https://www.malwarebytes.com/blog/news/2016/09/lesser-known-tricks-of-spoofing-extensions.
5. What is an .exe file? Is it the same as an executable? [Електронний ресурс] https://www.malwarebytes.com/blog/news/2021/10/what-is-an-exe-file-is-it-the-same-as-an-executable.
6. How Falcon OverWatch Investigates Malicious Self-Extracting Archives, Decoy Files and Their Hidden Payloads. [Електронний ресурс] https://www.crowdstrike.com/blog/self-extracting-archives-decoy-files-and-their-hidden-payloads/