Given the current fluctuations in the energy market and the related rise in prices to consumers, it should be no surprise that threat actors are using lures to exploit the global interest in this issue.

FortiGuard Labs recently discovered an e-mail using this tactic. The message was delivered to a coffee company in Ukraine that was seemingly sent by an oil provider in Saudi Arabia. Purporting to be a purchase order, the partial PDF file image displayed in the body of the email was actually a link to an ISO file hosted in the cloud that contained an executable for GuLoader. Also known as CloudEye and vbdropper, GuLoader dates to at least 2019 and is generally used to deploy other malware variants, such as Agent Tesla, Formbook, and Lokibot.

What makes this case interesting is that the executable in question uses NSIS (Nullsoft Scriptable Install System), a free, script-driven installer authoring tool for Microsoft Windows, to deploy itself.

Part one of this blog will detail our examination of the phishing e-mail and a static analysis of the embedded malware, while part two will provide a dynamic analysis of the malware along with its shellcode file, "rudesbies.Par".

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

The Phishing E-mail

Inviting a recipient to review an invoice or purchase order is a common phishing lure, which this attack path follows as well.

Figure 1. Phishing e-mail.

The e-mail claims to come from a known oil company in Saudi Arabia (this information has been redacted along with the recipient's details). Even without reviewing the e-mail headers, it is apparent straight away that the origins of this message may not be as claimed. Note the "From" address is actually "info@zoneofzenith[.]com", which has little resemblance to the domain of any petroleum-based business.

Figure 2. Email HTML

The headers confirmed our initial suspicions about the origins of this e-mail and show that it was indeed sent from the "zoneofzenith[.]com" domain.

Investigating the e-mail further, we find that the recipient is provided with what is meant to look like a PDF document containing a supposed purchase order that is embedded in the body text (see Figure 1). A review of the underlying HTML of the e-mail, however, shows this not to be the case. The embedded "document" is instead a hypertext-linked image that connects to a Microsoft OneDrive cloud storage location.

Figure 3. Microsoft OneDrive link.

If clicked, the link delivers the recipient to a OneDrive location and asks them to download the "purchase order". Rather than a PDF, however, the file "PO#23754-1.ISO" is downloaded. This is the first step in the infection chain that will eventually deposit GuLoader onto the victim's system.

ISO

Microsoft Windows is generally designed to be as helpful as possible where known file types are involved. In this case, the .ISO file (optical disc image) that is downloaded is automatically mounted when clicked, thereby presenting the file contained within.

Figure 4. Mounted PO#23754-1.iso file.

As can be seen in Figure 4, a file with an identical name is presented. However, instead of being the expected PDF, this time the file is an executable. Because Windows does not display extensions by default, it is not immediately evident that this file is an executable, making it difficult to distinguish from the expected document with the same name (aside from the "Type" column indicating an Application).

This file is the NSIS executable that will deploy GuLoader.

PO#23754-1.exe File Attributes

Figure 5. Exif data of the NSIS executable.

PO#23754-1.exe presents itself as a 32-bit Windows executable. As can be seen in Figure 5, several false items have been entered into the comment and description fields along with copyright and product name.

Figure 6. Digital signature information for PO#23754-1.exe.

An effort to provide a digital certificate has also been made. Figure 6, however, shows that the included information is obviously false, in addition to having been signed via an untrusted root.

PO#23754-1.exe Static Analysis

Originally developed as an installer to distribute the Winamp music player, the Nullsoft Scriptable Install System (NSIS) has been around since 2000. It is effectively a container (like a Zip file) that uses a script to deploy files to desired locations on a system.

A tool such as 7Zip can extract most of the files held within the container.

Figure 7. Executing 7Zip on PO#23754-1.exe.

For this executable, 7Zip deposits 13 files and 1 directory (which contains one file as well) into the extraction location of choice. Quite interestingly, all the files (except for rudesbies.Par and System.dll, which are stored inside $PLUGINSDIR) are chaff for investigators — decoys that attempt to waste time for anyone attempting to trace what the file does. Each of these other files, some of which are legitimate, is harmless. (An examination of rudesbies.Par will take place a little later in the blog.)

Unfortunately, a standard install of 7Zip is unable to expose the key component needed for further investigation of PO#23754-1.exe — the NSIS script. Another tool is required for this. 7z-build-nsis (https://github.com/myfreeer/7z-build-nsis) is one such tool. And as the name implies, it is a modified build of 7Zip designed to extract an NSI script.

Figure 8. The now extracted NSIS script.

The NSIS structure and syntax are entirely open source and available to review. In this case, the NSIS script provides a fair bit of information to anyone examining it.

Figure 9. Head of the NSIS script file.

Figure 9 shows the head of the NSIS script with accompanying string declarations.

Figure 10. Install directory highlighted as $TEMP and registry key to be created during the execution of the script.

As can be seen from Figure 10, the script will use $TEMP as an install directory and creates the registry key “HKCU Software\stemningsfulderes\DISINTENSIFI “Expand String Value” %WINDIR%\PARALLELIZING.log”

Figure 11. Multiple obfuscated Windows system calls.

The script makes several Windows system calls. Some of these have a basic level of obfuscation (for example, starting at line 260 in Figure 11 above). The file rudesbies.Par (mentioned above) is also featured. The calls used are as follows:

- KERNel32::CreateFileW(t $\"$INSTDIR\rudesbies.Par$\", i $0, i 0, p 0, i 4, i $1, i 0)i.R1
- KERNel32::GetFileSize(i R1, *i 0)i.r7
- KERNel32::VirtualAllocEx(i -1,i 0,i 0x100000, i 0x3000, i 64)p.R3
- KERNel32::ReadFile(i R1, i R3, i r7,*i 0, i 0)
- KERNel32::CloseHandle(i R1)
- user32::EnumWindows(i R3 ,i 0)

Effectively, the script wishes to read “rudesbies.Par” into a memory buffer and then checks to see if a window exists for it. The calls are made to “System.dll”, which contains the requisite Windows library functions. It is stored in the “$PLUGINSDIR”, shown in Figures 7 and 8, and will be deposited into a temporary directory upon execution.

Since “rudesbies.Par” is involved in the system calls within the NSIS script, a logical step at this stage in the investigation would be to examine it for further information. Unfortunately, the file is heavily encoded and therefore obfuscated from reading without further processing. This will be addressed in Part 2 of this series.

Figure 12. rudesbies.Par as it exists natively without processing.

Conclusion

This blog covered an examination of a phishing e-mail and a static analysis of the attached executable containing GuLoader. While not unheard of, the less common use of the Nullsoft Scriptable Install System made the sample more interesting than usual to examine.

Part two of this blog will cover the dynamic analysis of the executable and subsequent shellcode injection via the data stored in the “rudesbies.Par”.

Please stay tuned!

Fortinet Protections

The GuLoader sample mentioned in this blog is detected by the following (AV) signature:

NSIS/Injector.AOW!tr

The URL zoneofzenith.com is categorized as a Spam URL by our Web Filtering Client.

Fortinet customers are protected from this malware through FortiGuard’s Web Filtering, Antivirus, and CDR (content disarm and reconstruction) services and FortiMail, FortiClient, and FortiEDR solutions. All network-based URI’s are blocked by the Web Filtering client.

Due to the ease of disruption, damage to daily operations, potential impact to the reputation of an organization, and the unwanted destruction or release of personally identifiable information (PII), etc., it is important to keep all AV and IPS signatures up to date.

Fortinet also 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 that is designed to help end users learn how to identify and protect themselves from various types of phishing attacks.

IOCs

Filename	SHA256
PO#23754-1.ISO	c4debff9c0ec8a56aea5cd97215c6c906bd475ea8bd521fb9a346a4c992a0448
PO#23754-1.exe	14d52119459ef12be3a2f9a3a6578ee3255580f679b1b54de0990b6ba403b0fe
rudesbies.Par	4a1b6b30209c35ab180fa675a769e3285f54597963dd0bb29f7adb686ba88b79

Network IOCs

bounceclick.live/VVB/COrg_RYGGqN229.binb

Thanks to Fred Gutierrez who helped contribute to this blog.

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