Notable Droppers Emerge in Recent Threat Campaigns

fortinet.com/blog/threat-research/notable-droppers-emerge-in-recent-threat-campaigns

July 7, 2022

Droppers are malicious files that deploy malware payloads to a victim's device, and are used in many threat campaigns. During the second quarter of 2022, FortiGuard Labs observed some active droppers, including Microsoft Excel files, as well as Windows shortcut files and ISO image files. We captured these samples from phishing emails that were combined with social engineering to trick victims into loading the malware onto their devices. Recently, we found common malware families involving these samples to be Emotet, Qbot, and Icedid. In addition, a malware called Bumblebee, a previously rarely observed malware loader, was also found in some ISO files.

This blog reveals how droppers are delivered to a victim's device and how they drop malware payloads onto the victim's local disk.

Affected Platforms: Microsoft Windows
Impacted Users: Windows users
Impact: Controls victim's device and collects sensitive information, plus delivers other malware
Severity Level: Critical

Malicious Files Delivered Via Phishing Email

The droppers are spread through phishing emails in three ways. An email may:

- Contain the dropper or a password-protected ZIP as an attachment
- Contain an HTML file attachment that extracts a dropper when opened
- Have a link to download the dropper in the body of the email

Each way delivers the malicious file to victims and tricks them into opening it. See the examples below.

Figure 1: Email with a password-protected ZIP archive attachment

Figure 2: Email with an HTML file attachment

Figure 3: Email with a malicious download link

We observed the attached HTML file and the webpage of the download link use a technique called HTML smuggling, which leverages legitimate HTML5 and JavaScript features to encode the malicious data. As shown in Figure 4, The HTML smuggling file converts the blob data into a dropper when opened in the web browser.

Figure 4: HTML smuggling file

The first observation was in May. The download link in the email pointed to a web page containing HTML smuggling. By June, the HTML smuggling file was sent directly to victims as an HTML attachment.

Analyzing the Droppers and Their Behaviors

This quarter, we captured three different samples active in the threat campaign. The first sample is an Excel file with Excel 4.0 macros. The second is an LNK file (Windows shortcut file). The third sample is an ISO file (optical disk image).

Excel file with Excel 4.0 macros

This Excel sample is not new. It has been heavily used in Emotet campaigns since last year, as mentioned in the previous blog. Some sheets of this sample are hidden, as shown in Figure 5, including an Excel 4.0 macro sheet "IJEIGOPSAGHSPHP" that contains the

malicious formulas. Cell A1 in this macro sheet is named "Auto_Open99396895368995693577959485894894696364868989538953963789439 86" and includes a built-in macro that automatically runs the formula from that cell once the file is opened.

This macro sheet includes formulas that call the API "URLDownloadToFileA" to download the malware payloads from several different URLs. The malware payloads are actually DLL files and executed using "regsvr32.exe".

Figure 5: The malicious formulas in the hidden macro sheet

LNK file

A Windows shortcut file (commonly referred to as LNK) is created to point to a specific target. Double-clicking on the shortcut file will execute the target.

As shown in Figure 6, this sample includes a PowerShell code snippet in its target field. The PowerShell code converts a base64 string into a script that contains multiple URLs to download the malware payload. Next, it attempts to download the malware payload from each URL and execute it with "Regsvr32.exe" until it succeeds.

Figure 6: The target of the shortcut file

We also captured other samples containing different malicious code in their target field. As shown in Figure 7, there is a command line to download a malware payload from a URL and execute it with "Regsvr32.exe".

Figure 7: The malicious code in the target field of captured sample

Figure 8 shows another malicious PowerShell code in the target field. The data is decoded to a .hta URL and executed using "mshta.exe". Next, the VBScript code in the web page of the .hta URL extracts a PowerShell code that includes encrypted data. In the end, the encrypted data is transformed into script code to get the payload URL and download malware.

Figure 8: The malicious code in the target field of a captured sample

All three examples above download and execute a malware payload, despite the differences.

ISO file

An ISO file (often called an ISO image), is an archive file that stores the contents of a physical disk. In Windows 10, opening an ISO file by double-clicking it mounts the file on a virtual optical disc drive. Once mounted, the contents of an ISO file can be accessed in File Explorer.

Threat actors store a malware DLL file and a malicious LNK file in the ISO file. As shown in Figure 9, the DLL file is set to a hidden attribute, so it is not visible in File Explorer by default. On the other hand, the shortcut file is used to execute the DLL file using "Rundll32.exe".

Figure 9: The malware DLL file and malicious LNK file are stored in the ISO file

Conclusion

In recent threat campaigns, all droppers mentioned in the previous section are very active and used by more than one malware family. Below is the malware payload of each captured dropper.

Malware Dropper	Payload
Excel file	Emotet and Qbot
LNK file	Emotet, Qbot, and Icedid
ISO file	Qbot, Icedid, and Bumblebee

Figure 10 shows the notable malware activities during the past three-month period. In early April, Microsoft Excel files were the only file type used to spread malware. We then captured a shortcut file with the Emotet malware payload, which first appeared on April 23. This new malware attack technique was soon followed by Qbot and Icedid, spreading using shortcut files as well in early May. Later, ISO files for droppers began appearing in the middle of May, and the malware families involved included Qbot, Icedid, and Bumblebee. Next, HTML smuggling attacks emerged in late May and June, including web pages and HTML file attachments. This builds malware locally instead of delivering malicious files directly through the network to bypass the firewall.

Figure 10: Timeline of dropper usage in recent threat campaigns

Microsoft Office files have been a favorite vehicle for threat actors because of the macros. However, things seem to be changing as Microsoft has added more security controls in Office files with macros. In July of 2021, Microsoft disabled Excel 4.0 macros by default when opening an Excel file. In early April 2022, Microsoft created another setting to block VBA macros in files from the internet by default. With more restrictions on the use of macros for Microsoft Office files, threat actors turn to other types of files to increase compromise rates. At this point, shortcut files provide a solid option due to double-click execution. ISO files can be automatically mounted and opened on modern versions of Windows with just a double click. In addition, ISO files take advantage of bypassing the Mark-of-the-Web trust control,

making them easier to evade antivirus detection than other archive files. The HTML smuggling technique creates malicious files locally to bypass the restrictions on receiving files from the internet and emails. This explains the proliferation of shortcut files and ISO files, as well as HTML smuggling used for malware deployment at this time.

Fortinet Protections

Fortinet customers are protected from this malware by FortiGuard's Web Filtering, Antivirus, FortiMail, FortiClient, FortiEDR, and Content Disarm & Reconstruction (CDR) services as follows.

The phishing email with its attached malicious file can be disarmed by the FortiGuard CDR service.

FortiEDR detects the Excel, shortcut, ISO, and malware payload DLL files as malicious based on their behavior.

Fortinet customers are protected from these malicious files and malware by FortiGuard Antivirus, which is included in FortiMail. It detects all malicious macro file types, including Excel 4.0 macro samples.

All malicious samples described in this report are detected by FortiGuard Antivirus as follows:

XF/CoinMiner.Z!tr
LNK/Agent.APX!tr
LNK/Agent.PE!tr
LNK/Agent.VPIX!tr.dldr
LNK/PSRunner.VPHQ!tr
JS/Agent.BLOB!tr.dldr

The malware payloads are detected by FortiGuard Antivirus as follows:

W64/GenKryptik.FWMO!tr
W32/Emotet.C!tr
W32/Qbot.D!tr
W64/GenKryptik.FWBH!tr
W64/GenKryptik.FVFR!tr
W64/Bumblebee.E!tr
W64/IcedID.HG!tr

In addition, Fortinet has multiple solutions designed to train users on how 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.

We also suggest that organizations have their end users go through our FREE NSE training: NSE 1 – Information Security Awareness. It includes a module on internet threats to train end users on how to identify and protect themselves from phishing attacks.

IOCs

Malicious sample (SHA256):

2fe44042cfc6602b43204e38bcbc2773d1e4f87be6aa16073625bc1b33af6877
8fda14f91e27afec5c1b1f71d708775c9b6e2af31e8331bbf26751bc0583dc7e
262f963f949671f429ba3c4233f493a064c08e1361d0c0689f7d3de205d5f7b1
2abfb434d9f16888332ecb2d6eb7660b28e544ad67130d0050330bdb104502c3
adf8cb3421c726efbadff60e97a07f6df6de98818e0978382ec388e7d32a2128
4b582f38e3376346cb066e36ff8dfa32b268154bb2de13870702e8bbf366a023
467bc7ff93d75009d3ba7633662dc9109297ac0f64abb078fd9c8e181abe6cca

Malware payload (SHA256):

00dcc4642d488643856259cd3c576d9e24045b48783fc21ebdccd5fb4de66f8c
71c9cc11c107b0716eff86de98b3fbd77add1e35ceadf86519eb84b473cb862d
9d4bf3e9577884295102e5dd673b81065d21d348da8ba5a3249e8f5f4c40d5d6
424815ec0a4c06cb7e063c3540919f8f4b1ee369f977448b7eeaa248ef187431
9eea56f945cc00c5216b3250326f8b79d3d2cac5165b250b606729e72bd2647c
90576eb6754dd1c38fb4cea4bf3f029535900436a02caee891c057c01ca84941

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