What's happening in the world of crimeware: Emotet, DarkGate and LokiBot

SL securelist.com/emotet-darkgate-lokibot-crimeware-report/110286/

Authors

Expert GReAT

Introduction

The malware landscape keeps evolving. New families are born, while others disappear. Some families are short-lived, while others remain active for quite a long time. In order to follow this evolution, we rely both on samples that we detect and our monitoring efforts, which cover botnets and underground forums.

While doing so, we found new Emotet samples, a new loader dubbed "DarkGate", and a new LokiBot infostealer campaign. We described all three in private reports, from which this post contains an excerpt.

If you want to learn more about our crimeware reporting service, please contact us at crimewareintel@kaspersky.com.

DarkGate

In June 2023, a well-known malware developer posted an advertisement on a popular dark web forum, boasting of having developed a loader that he had been working on for more than 20,000 hours since 2017. Some of the main features, which went beyond typical downloader functionality, supposedly included the following:

- Hidden VNC
- Windows Defender exclusion
- Browser history stealer
- Reverse proxy
- File manager
- Discord token stealer

The full list of the touted capabilities is available in our private report.

The sample we obtained is missing some of these features, but that doesn't mean much, as they are enabled or disabled in the builder anyway. We were, however, able to reconstruct the infection chain, which consists of four stages, all the way to loading the final payload: DarkGate itself.

1. **VBS downloader script**: The script is fairly simple. It sets several environment variables to obfuscate subsequent command invocations. Two files (Autoit3.exe and script.au3) are then downloaded from the C2, and Autoit3.exe is executed with script.au3 as an argument.
2. **AutoIT V3 script**: AutoIT V3 is a BASIC-like freeware scripting language, which is often used by malware authors, as it can simulate keystrokes and mouse movements, among other things. The script that is executed is obfuscated, but ultimately allocates memory to the embedded shellcode and finally executes the shellcode.
3. **Shellcode**: The shellcode is pretty straightforward: it constructs a PE file in the memory, resolves imports dynamically and transfers control to it.
4. **DarkGate executor** (the PE file constructed by the shellcode): The executor loads the script.au3 file into the memory and locates an encrypted blob within the script. The encrypted blob is then decrypted (using a XOR key and a final NOT operation). This results in a PE file, whose import table is dynamically resolved. The final result is the DarkGate loader.

The DarkGate loader has several global variables, actually a Delphi TStringList, comprising 17 variables that describe the core functionality of the malware:

1. Variable that is set if an AV is found
2. Variable that is set if a virtual environment is found
3. Variable that is set if a Xeon processor is found
4. C2 port number

The full list of variables is available in our private report. The core functionality does not include malware loading, which is implemented in a separate module.

What also stands out is the way strings are encrypted. Each string is encrypted with a unique key and a custom version of Base64 encoding using a custom character set.

LokiBot

LokiBot is an infostealer that first surfaced in 2016 and remains active today. It is designed to steal credentials from various applications, such as browsers, FTP clients and others. Recently, we detected a phishing campaign targeting cargo ship companies that drops LokiBot.

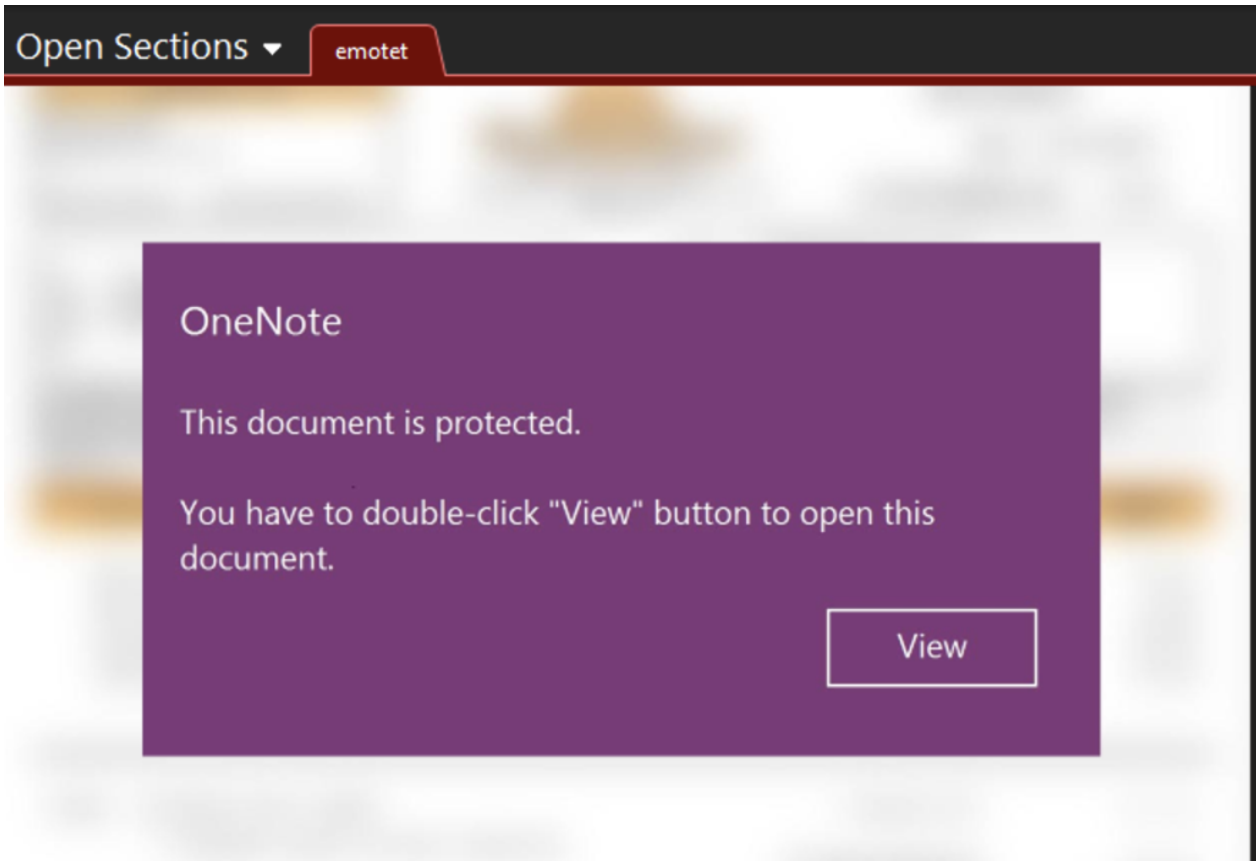
In the cases we investigated, the victims received an email appearing to come from a business contact and stating port expenses that needed to be paid. Attached to the email was an Excel document. As expected, when opening the document the user was asked to enable macros. However, this was a fake warning, as the document did not contain any macros, trying to exploit CVE-2017-0199 instead.

That vulnerability makes it possible to open a remote document by providing a link. This results in downloading an RTF document, which in turn exploits another vulnerability, namely CVE-2017-11882. By exploiting this other vulnerability, LokiBot is downloaded and executed.

Once executed, it collects credentials from various sources and saves into a buffer inside the malware, after which it sends them to the C2. Data is sent via POST requests compressed with APLib. After sending out system information, the malware listens for additional C2 commands. These commands can be used to download additional malware, run a keylogger, and so on.

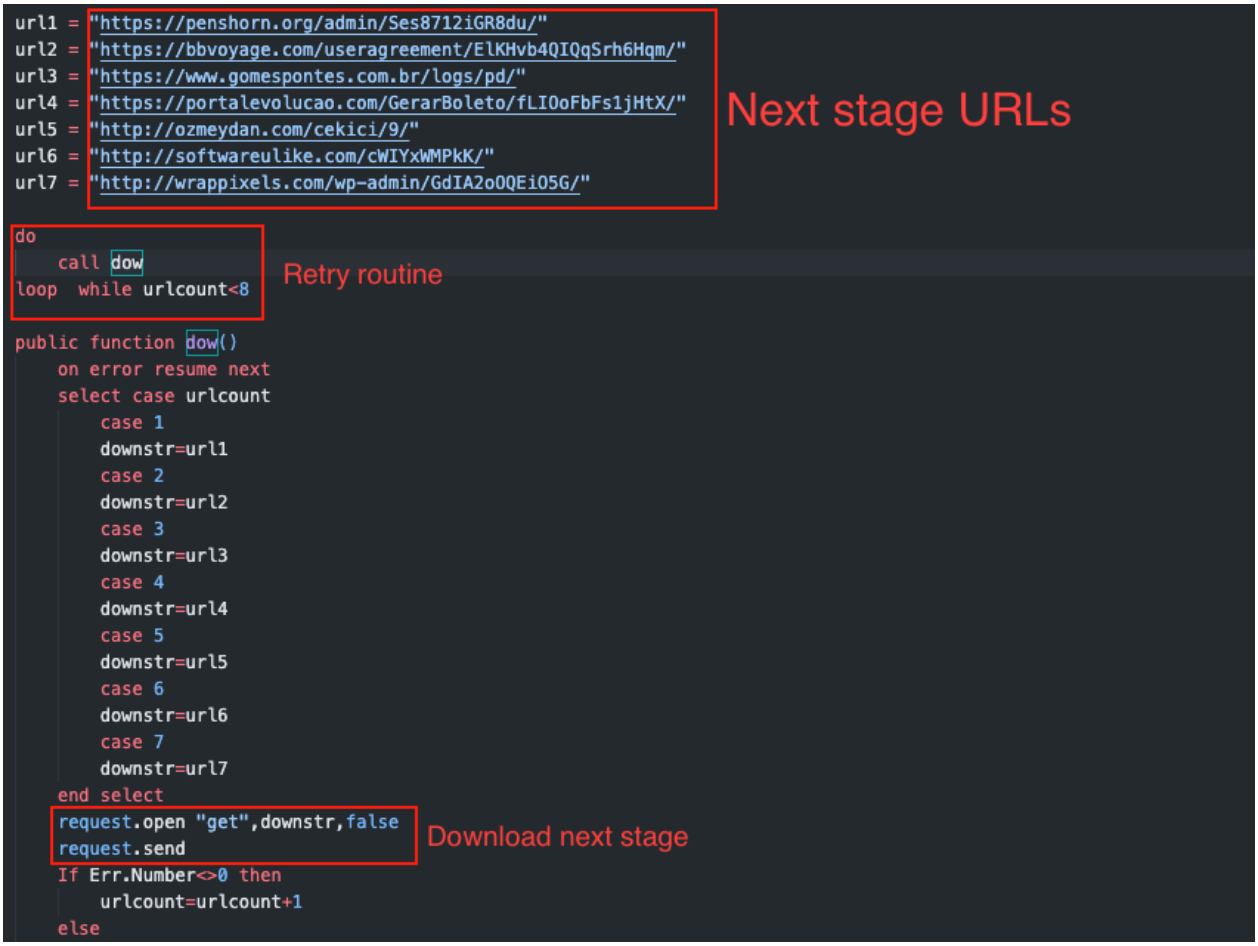
Emotet

Emotet is a notorious botnet that, despite being taken down in 2021, resurfaced later. In their recent wave of attacks, they jumped on the OneNote infection bandwagon,sending emails with malicious OneNote files. Opening one of these displays an image similar to the one below.



Emotet OneNote decoy document

Clicking on the view button executes the embedded and obfuscated malicious VBScript. The deobfuscated code is fairly simple.



Deobfuscated downloader script

As one can see, there are several sites containing the payload. The script tries each of them until it succeeds, and then saves the payload, a DLL, in the temp directory, executing it with regsvc32.exe. The executed DLL then loads a resource (LXGUM) from its resource section and decrypts it with a simple rolling XOR algorithm as illustrated below.

Resource decryption code

The decrypted payload is actually shellcode that does a typical import by hash. Two of the resolved functions are LdrLoadDll and LdrGetProcedureAddress, frequently used by malware authors to evade dynamic analysis of well-known APIs: LoadLibrary and GetProcAddress in this case. Next, memory is allocated, and a blob (a PE file) from the resource section is written to the allocated memory, which is the final Emotet payload. DLL dependencies are resolved, and the Import Address Table (IAT) is reconstructed. The shellcode then overwrites the DOS header of the PE file, in order to make it more difficult for EDR solutions to detect the binary in the memory. Finally, Emotet is executed.

The Emotet payload itself remains the same as in the previous waves of attacks.

Conclusion

Malware continuously evolves, and TTPs change, hindering detection. Besides, it can be difficult for an organization to decide which type of malware threat to defend from first. Intelligence reports can help you to identify the threats relevant to your business and to stay protected against these. If you want to keep up to date on the latest TTPs used by criminals, or if you have questions about our private reports, reach out to us at crimewareintel@kaspersky.com.

Indicators of compromise (MD5s)

LokiBot
31707f4c58be2db4fc43cba74f22c9e2
2c5cf406f3e4cfa448b167751eaea73b

DarkGate
1B9E9D90136D033A52D2C282503F33B7
149DA23D732922B04F82D634750532F3

Emotet
238f7e8cd973a386b61348ab2629a912
df3ee4fb63c971899e15479f9bca6853

- crimeware
- Cybercrime
- Emotet
- Malware
- Malware Descriptions
- Malware Technologies
- Trojan
- Trojan-stealer

Authors

GReAT

What’s happening in the world of crimeware: Emotet, DarkGate and LokiBot

---

Your email address will not be published. Required fields are marked *