GuLoader delivers RATs and Spies in Disguise

labs.k7computing.com/

By K7 Labs April 13, 2020

Hackers have been taking advantage of the Coronavirus scare by employing a COVID theme in their phishing pages and spam emails. In this blog, we will dig deeper into the GuLoader malware which comes attached as a spam document in such emails. This malware is a VBdownloader that has been used in many such malicious campaigns and can be attributed to Gorgon APT, TA505 and TA542 threat groups among others.

GuLoader is a small VB5/6 file which typically downloads RATs, stealers or spies like Formbook, Agent Tesla, Lokibot, Remcos RAT, NetWire RAT etc. We recently analyzed a campaign which was using GuLoader to download and deliver Formbook from Google Drive. While analyzing this campaign we were able to locate around 2100 GuLoader samples which connect to multiple Google drive links and 130 samples which contact OneDrive, in February, and by end of March, we were able to locate around 3300 new samples which connect to Google drive and 250 samples which connect to OneDrive, which is around 60% increase than the previous month. In total the number of Guloader is around 6000+ samples in the past 3 months.

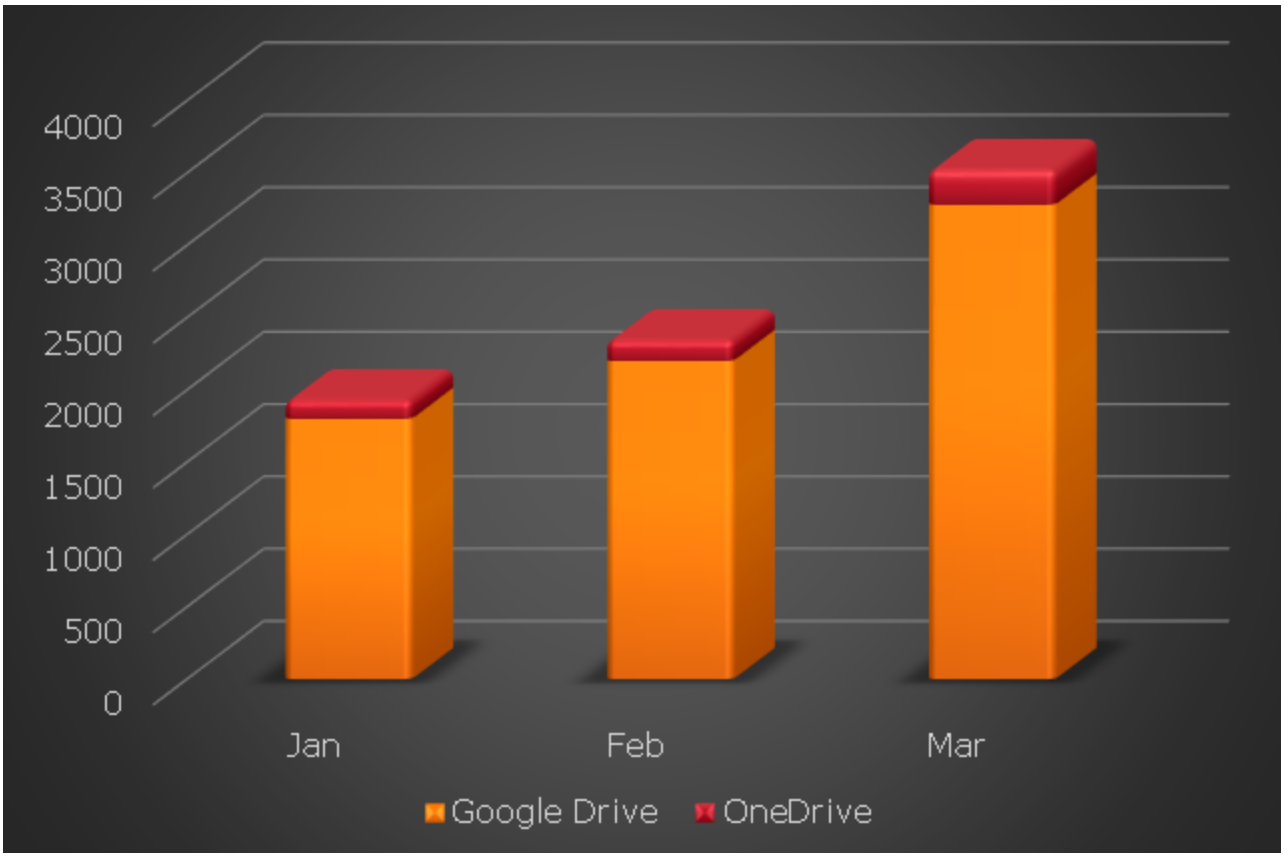

Figure 1: Graph showing month wise volume of collected samples

It is evident from the increasing numbers as shown in Figure 1, that this malware has gained popularity and is being used for nefarious activities by various threat actors. The popularity factor is because of some of its features like:

- It is small and can be embedded in ISO image files and RAR files.
- Stores its encrypted payload on Google Drive and OneDrive, which can later be downloaded and decrypted by a simple xor operation.

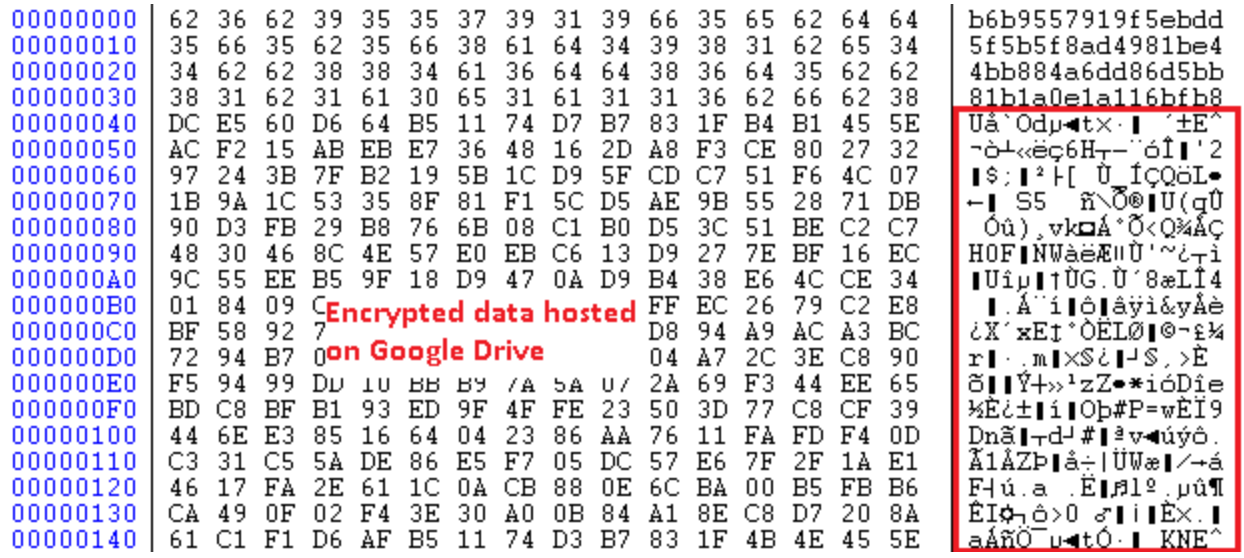

Figure 2: File hosted on cloud service.

- Injects the decrypted payload into the targeted processes.

- Predominantly used to deliver NanoCore RAT, Remcos RAT, Quasar RAT, NetWire RAT, Agent Tesla and Formbook malware.
- Uses anti-attach techniques.

GuLoader analysis

The infection chain of the campaign which downloads GuLoader is depicted in Figure 3.

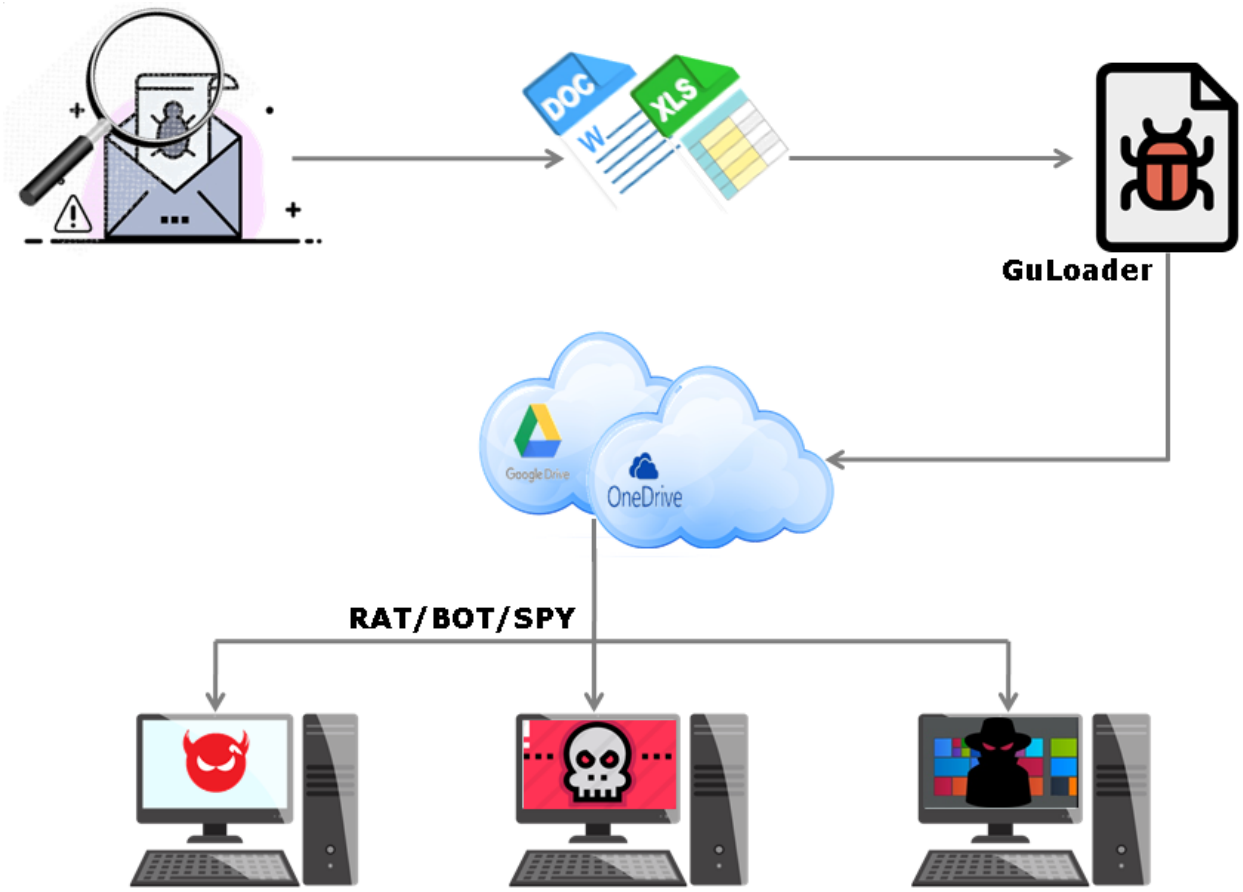

Figure 3: Infection chain of GuLoader

The malicious VB file allocates virtual space to decrypt and execute the code responsible for the following:

> Debugger Anti-attach technique: The malware uses **ZwSetInformationThread** API to detach itself from the debugger.
>
> Patching **ntdll.DbgBreakPoint** and **ntdll.RemoteUiRemoteBreakin**: When we attach a debugger to a running process it calls **DebugActiveProcess** API which in turn calls **RtlCreateUserThread** function to create a new remote thread into the targeted process with **DbgUiRemoteBreakin** function as its new thread's starting point. Therefore, a malware can easily hook ntdll.DbgBreakPoint and ntdll.DbgUiRemoteBreakin API and patch them to the point that will cause the process to exit or NOP (no operation) or to a point where it will call an unknown or non-readable location.

Unhooking user mode hook: For behavior-based detection most of the Anti-Virus products implement a user mode hook for some of the most common APIs used by malware. To do that, they simply modify the 1st 5 bytes (0xb8 ????????) of the API function with an unconditional (0xe9 ????????) jump to their hook handler. To avoid this, the malware tries to rewrite the 1st 5 bytes to its original state even if the hook is not in place.

Download payload from cloud storage: Downloads the file stored on Google Drive/OneDrive and decrypts it.

It then injects this decrypted payload to the targeted process or creates a child process of itself and overwrites the child process with the decrypted content from the image base 0x400000.

For more detailed reading about the above mentioned points, do have a look at this blog.

Given below are some of the paths in which the GuLoader is saved on the PC as per our telemetry reports

C:\USERS____\APPDATA\LOCAL\TEMP\SUBFOLDER\FILENAME.EXE

C:\USERS_____\APPDATA\LOCAL\TEMP\RAR$DIA4024.13665\QUOTATION REQUEST.SCR

C:\DOCUME~1_____\LOCALS~1\TEMP\RAR$EXA0.993\SCANDOC8383.EXE

C:\USERS____\APPDATA\LOCAL\TEMP\RAR$EX00.225\DOC981.EXE

C:\USERS___\APPDATA\LOCAL\TEMP\RAR$EXA0.418\CL MONA (13912-I0005) _HIRE STATEMENT_PAYMENT COPY_PDF.EXE

C:\USERS_____\APPDATA\LOCAL\TEMP\SUBFOLDER\WINDOW.EXE

C:\USERS_____\APPDATA\LOCAL\TEMP\RAR$DIA0.789\CONSIGNMENT DOCUMENTS.SCR

C:\USERS_____\APPDATA\LOCAL\TEMP\RAR$EX00.626\SWIFT COPY.EXE

C:\USERS_____\APPDATA\LOCAL\TEMP\RAR$EX00.251\PURCHASE ORDER-3647585PDF.EXE

C:\USERS_____\APPDATA\LOCAL\TEMP\RAR$EXA0.440\RFQ-21902.EXE

C:\USERS_____\APPDATA\LOCAL\TEMP\RAR$EX00.403\PAYMENT_0320.EXE

C:\USERS____\APPDATA\LOCAL\TEMP\RAR$EXA0.540\BRANCHE.EXE

C:\USERS_____\APPDATA\LOCAL\TEMP\RAR$EXA0.181\SCANDOC8383.EXE
C:\USERS_____\APPDATA\LOCAL\TEMP\RAR$DIA0.815\ATTACHED PO#19POGL1614-2020REF0088427.SCR

These GuLoader exe files get downloaded and saved to the system after the Coronavirus spam document is opened. This happens when macros are enabled by the victim or after successful exploitation of vulnerabilities like CVE-2017-11882 by the threat actors.

This is one of the major campaigns this year so far. Emails with the COVID theme, and with the impersonation of trustworthy agencies like WHO, UNICEF, Govt Health agency, etc., lure the recipient to open them and their attachments. With the ever growing concern related to the Corona pandemic and people's hunger for information, the COVID based spam has been quite successful in gaining victims. We sifted through our pan-India telemetry and we were able to find at least 60 hits for the last week of March and more than 800 unique hits in the past 30 days or so.

Security Guidelines

- Do not fall prey to any spam mails related to COVID19 or any other emails that you weren't expecting
- Cultivate the use of spam filters
- Pay close attention to the email address of the sender before downloading any attachment
- Install the latest service packs and hot fixes from Microsoft
- Install a reliable security product like K7 Total security and ensure it is enabled and kept up-to-date

Indicators of Compromise (IoCs)

Spam doc/xls

19B9749D417DD800042EEF6CE4831665 Trojan (0001140e1)

23B8E03D5F5B6F906006E43047E78EC1 Trojan (0001140e1)

5127D7FD0E929E157D9B9F677D8496D4 Trojan (0001140e1)

FFC54A5B610C781E9E6C7F15666FA026 Trojan (0001140e1)

GuLoader

06765254FA14E550E6BCEE092CB37B18 Trojan (005630331)

7580F80CE0B825EF8931F0B5A25FD131 Trojan (0056315b1)

9DBA8EEEE47B6F14B4E4814824397375 Trojan (00561ca31)

50B1D1DFECE17FE955BF9DA7942C5A73 Riskware (0040eff71)

1910E8659F87A0B9F62C78B829CF7295 Trojan (00561c181)

Malware downloaded by GuLoader

C949A9618462F5C83A93FDD2EB0DABF7 Password-Stealer (0052f96e1)

7573808E70745FCAF78117F420F67C73 Password-Stealer (0040f4f51)

4DD1308E8D02539221057684398D300D Trojan (005608181)

1899A6720B1E95E57BAB440524AD5B14 Trojan (005485311)