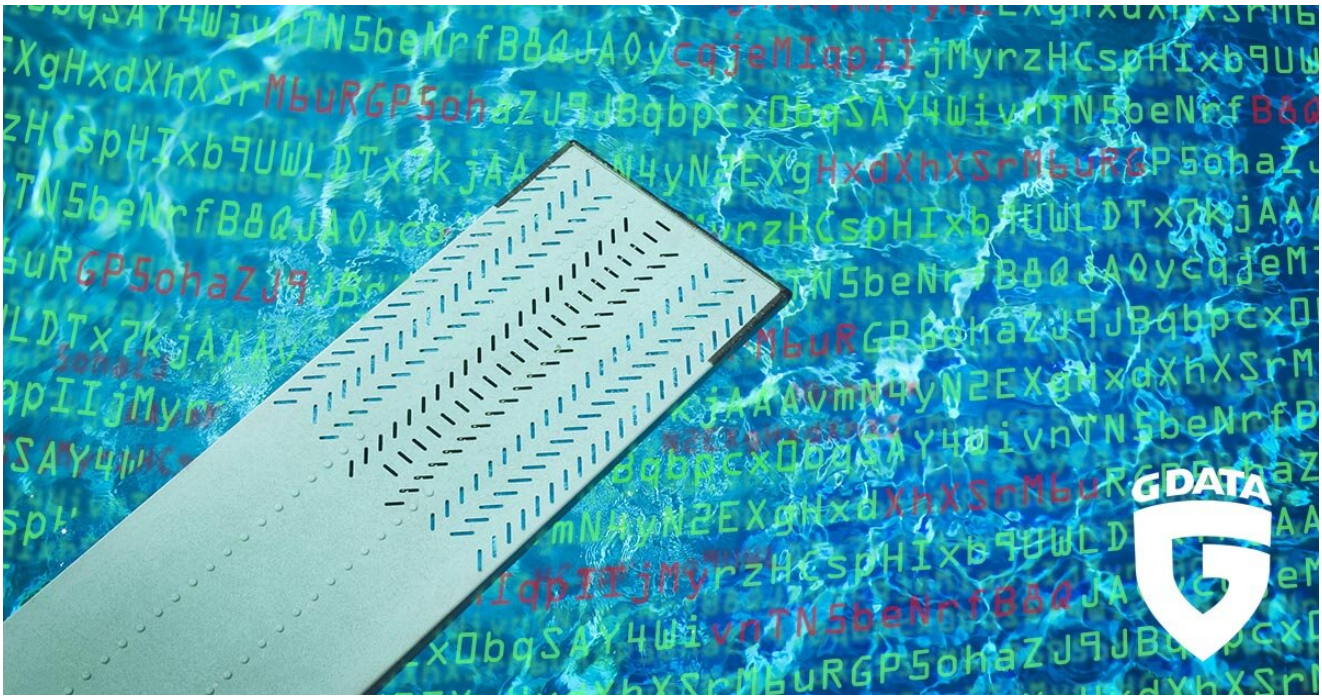
Harmful Logging - Diving into MassLogger

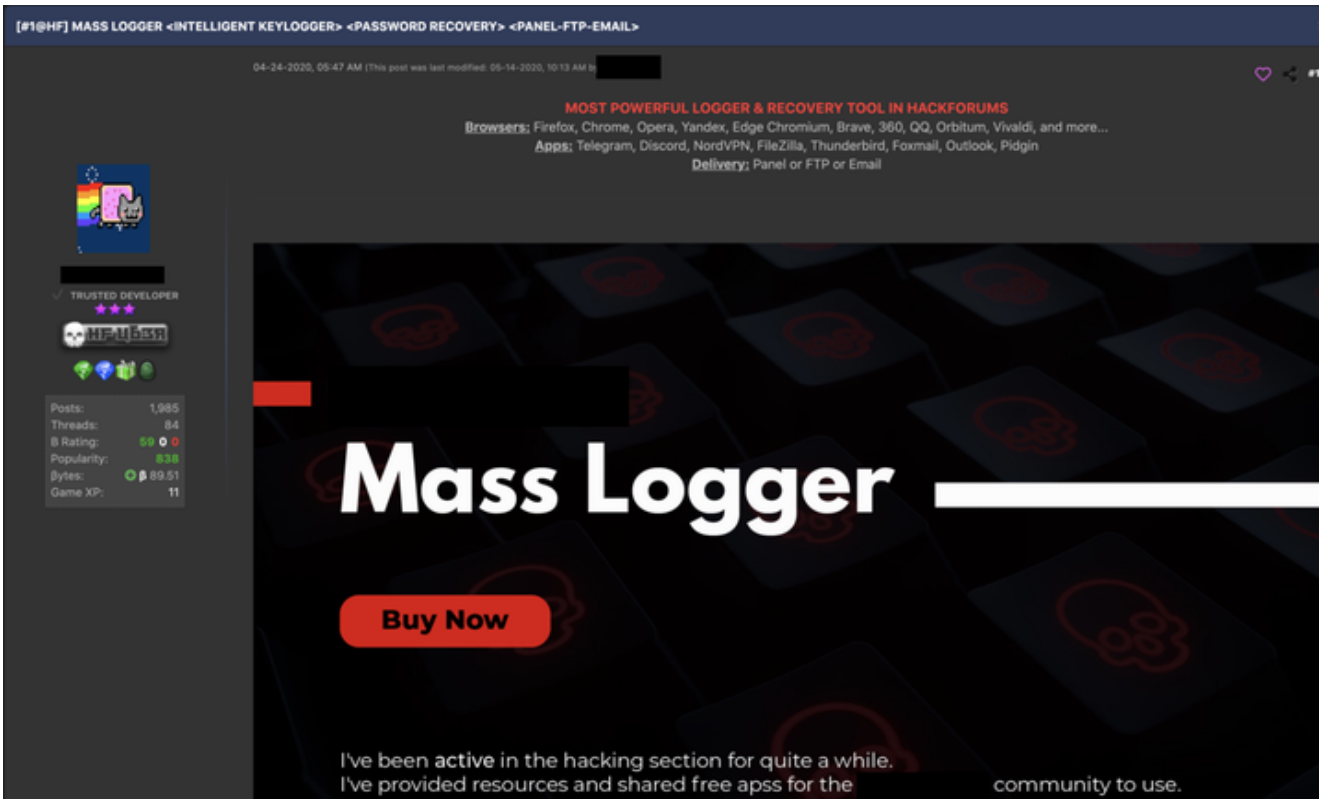
gdatasoftware.com/blog/2020/06/36129-harmful-logging-diving-into-masslogger



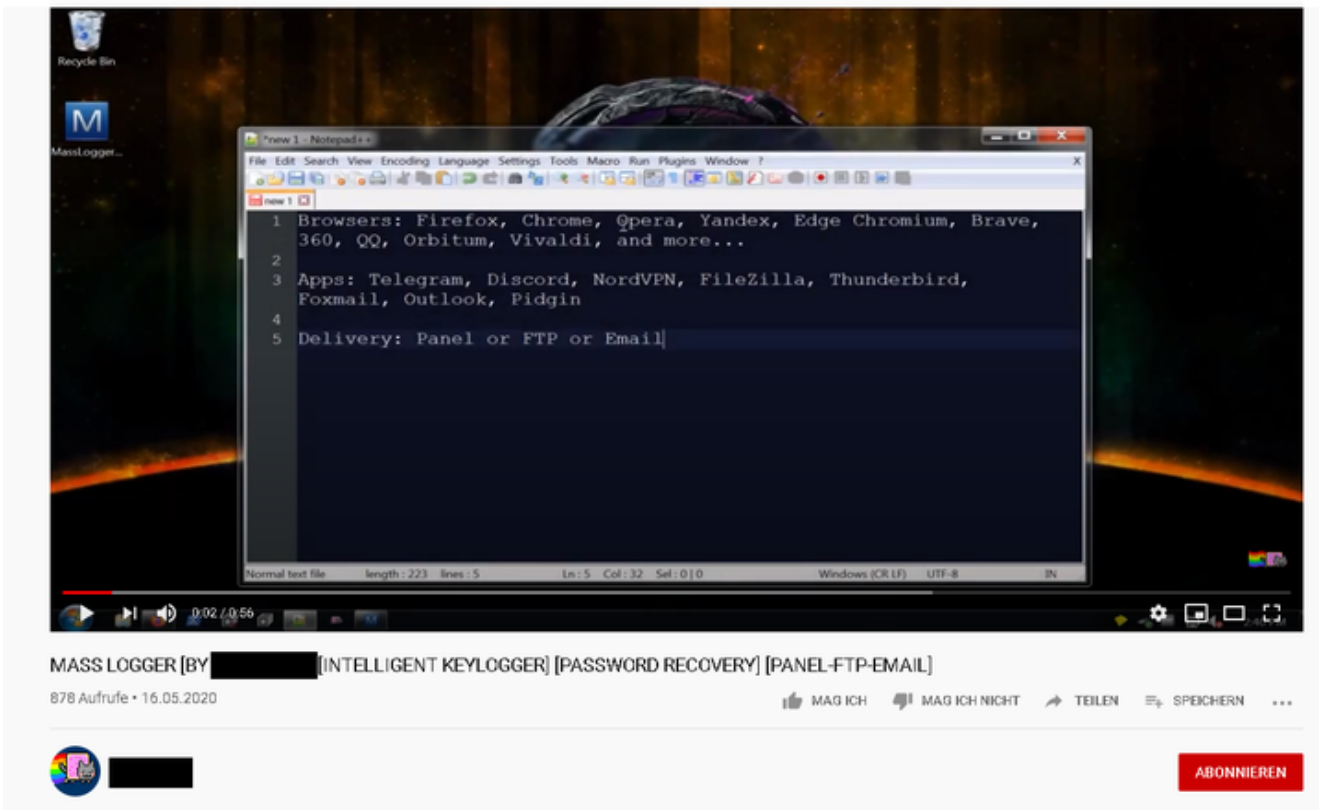
There are many things that can be logged on a computer. While not all logging data is useful for the average user, a lot of logging goes on in the background of any system. However: There is good logging and bad logging. We have looked at an example of logging you definitely would not want.

Over the last weeks we observed a malware variant named MassLogger which is sold on hacker forums and advertised via Youtube videos. It is a .NET malware classified as a credential stealer and spyware, being weaponized with a variety of routines to steal sensitive data from users, as well as spy on them.

The use cases for MassLogger vary a lot. However, we observed reports from other researchers and are confident that MassLogger is mostly distributed by phishing mails.



MassLogger advertisment on forums

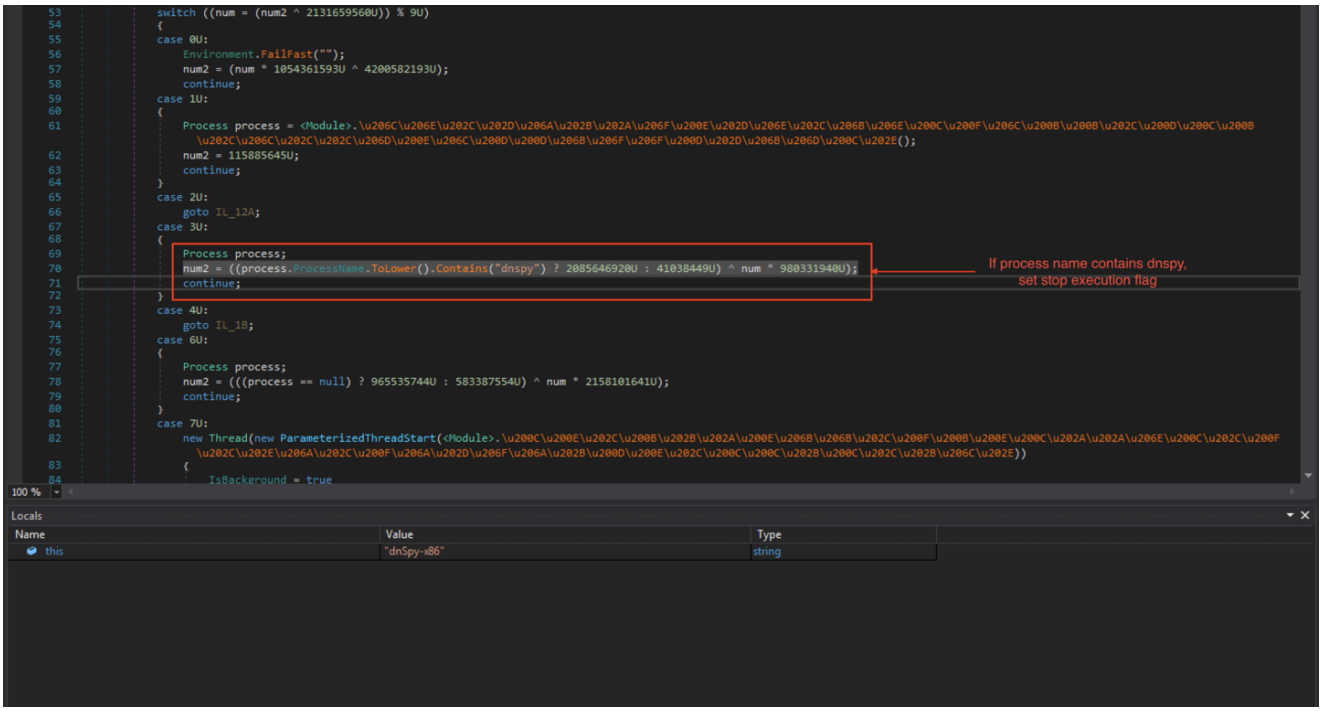


MassLogger advertisement on youtube

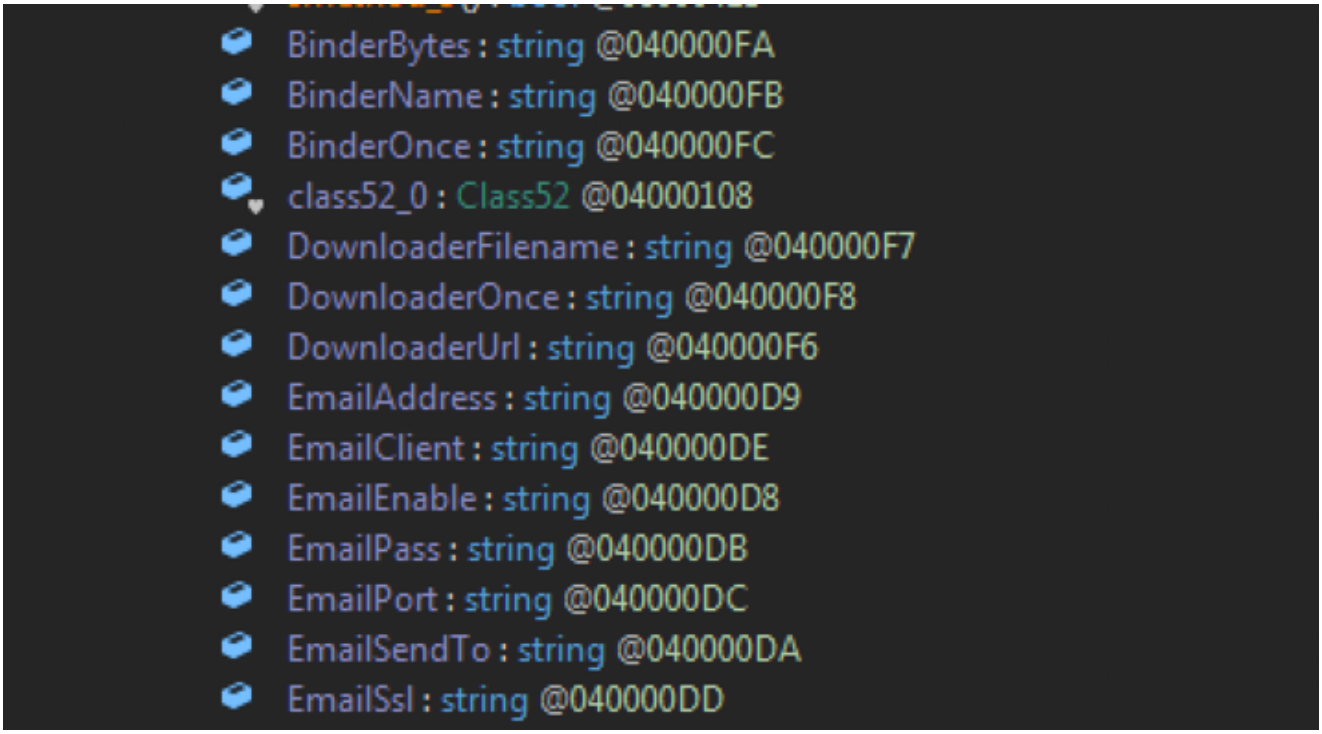
Modularity

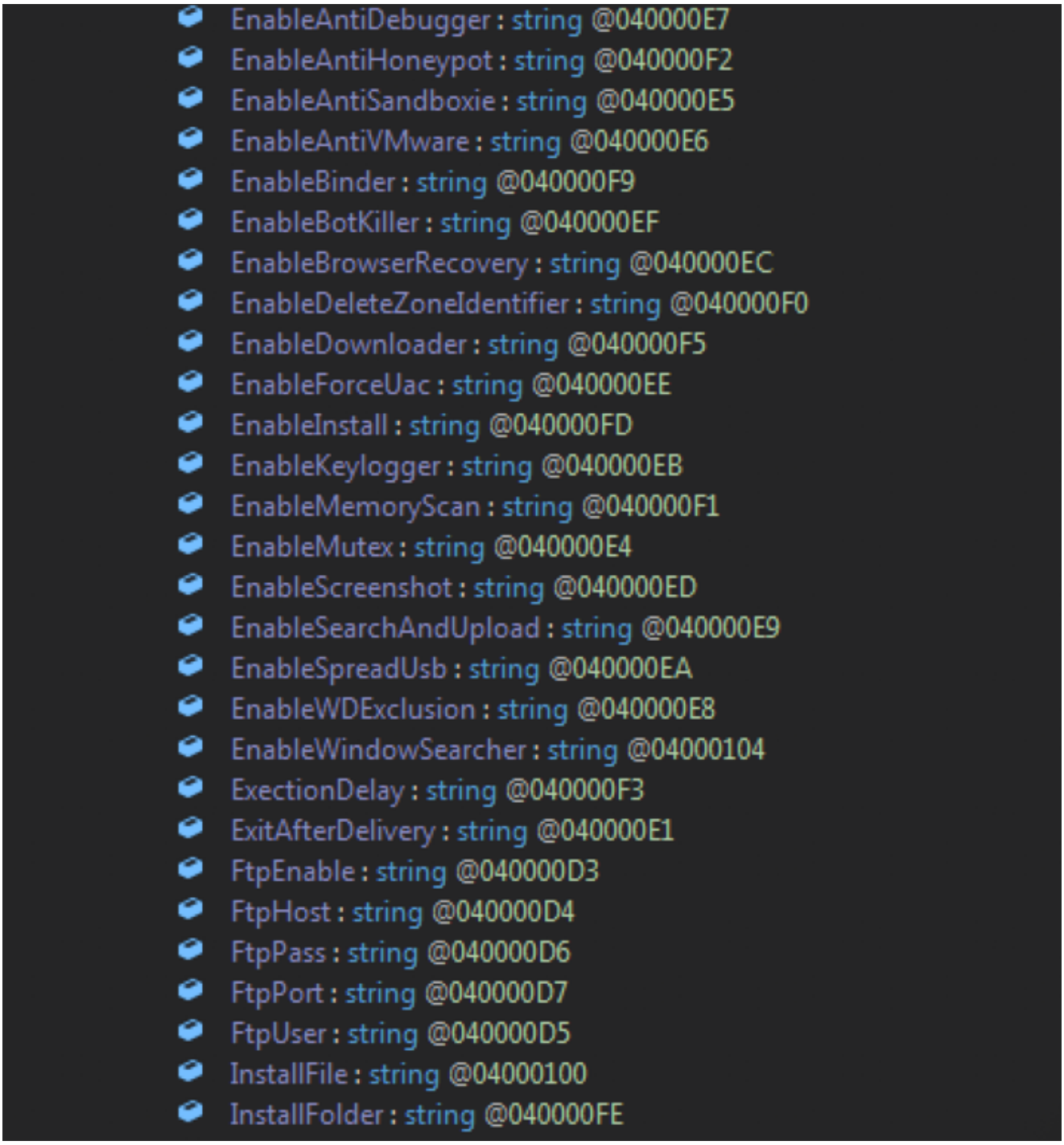
MassLogger is developed to be sold to a wide variety of criminals, therefore it is also highly modular. During our analysis, we found flags for various kinds of modules this malware has to offer. These modules are also introduced by the author. We are confident that customers are able to enable or disable certain features once a purchase is made.

Masslogger is usually packed with various packers which implement additional techniques to evade environments used to analyse malicious binaries. The sample we investigated was packed with at least the CyaX .NET Packer or reuses its code. One more packing stage was added which was able to detect whether the dnSpy debugger is attached to it.

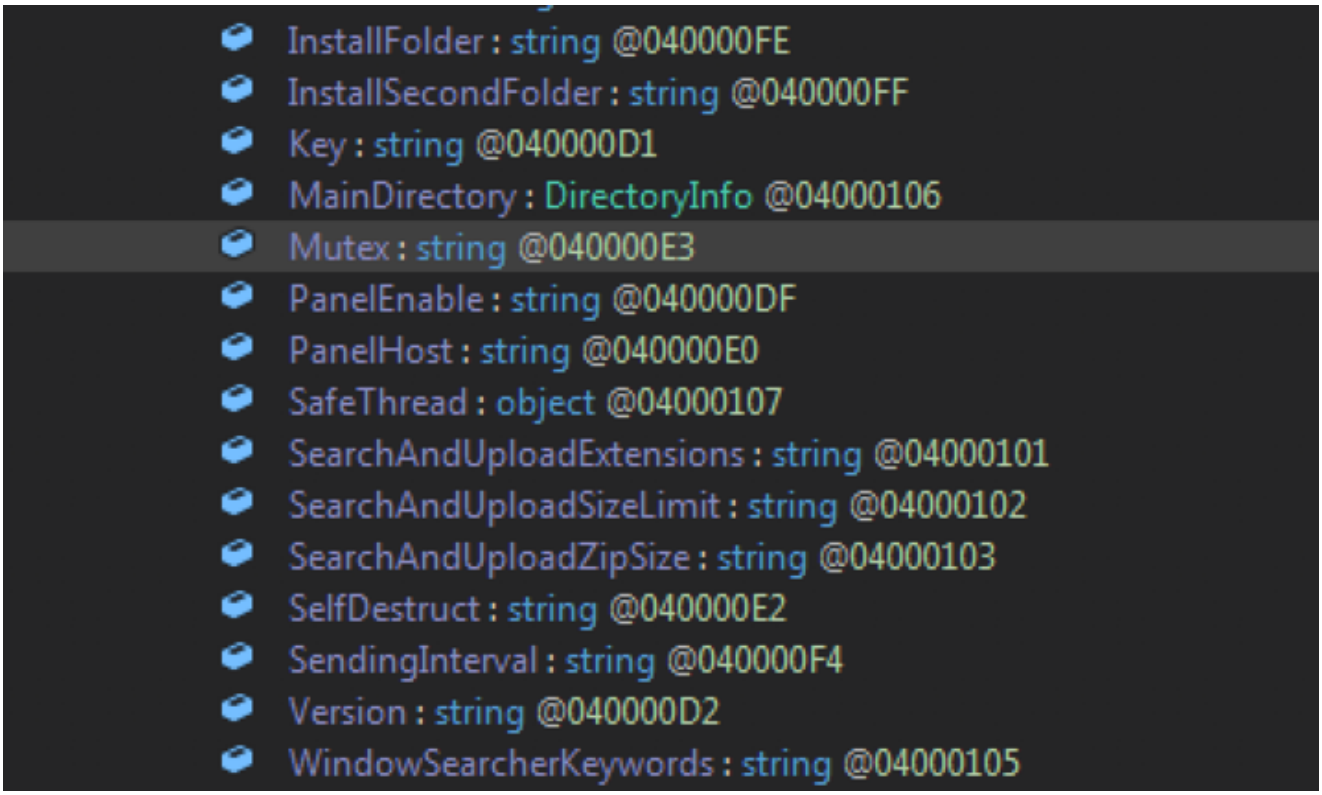


Packer stage looking for dnspy substring in process name





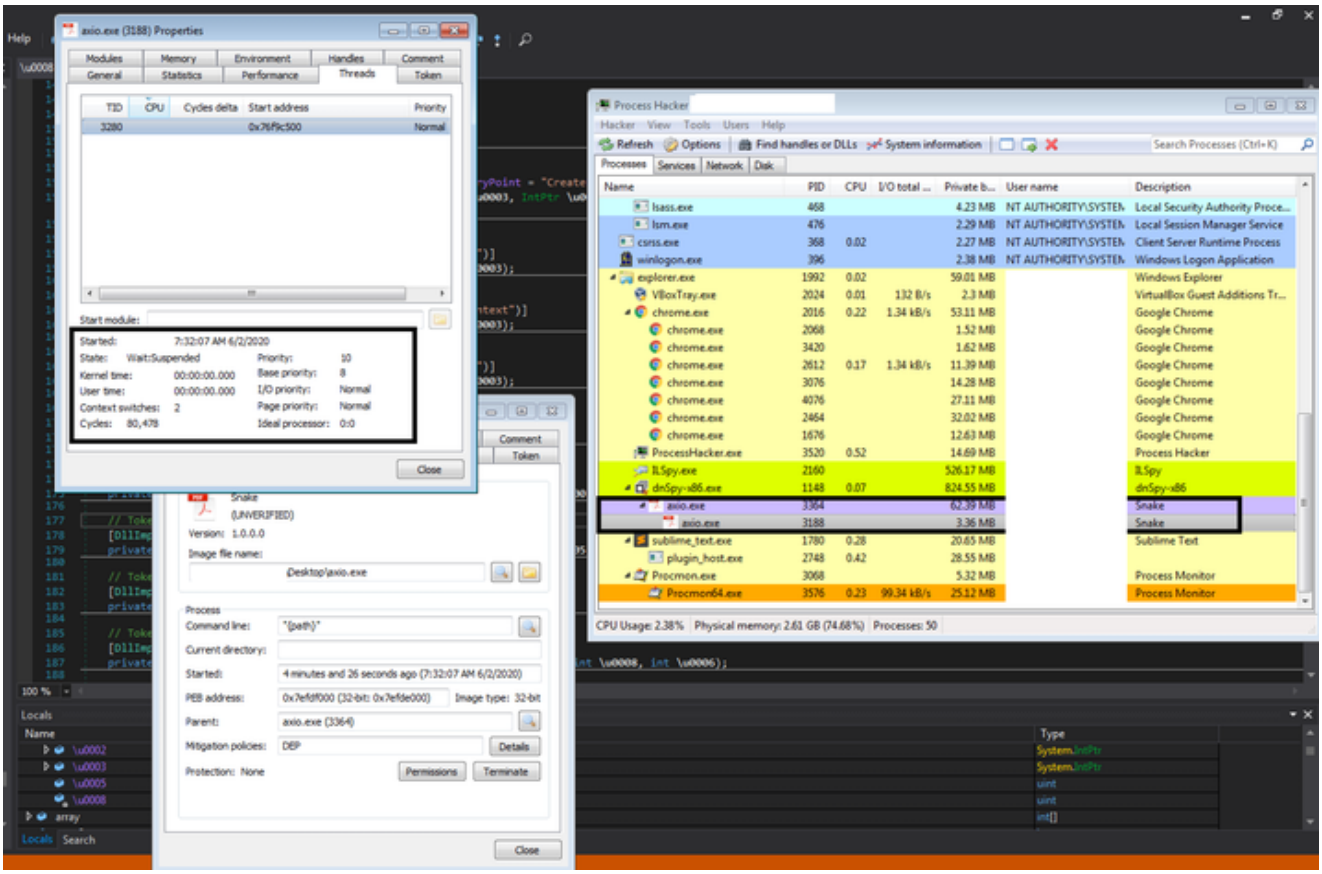
MassLogger's settings 1



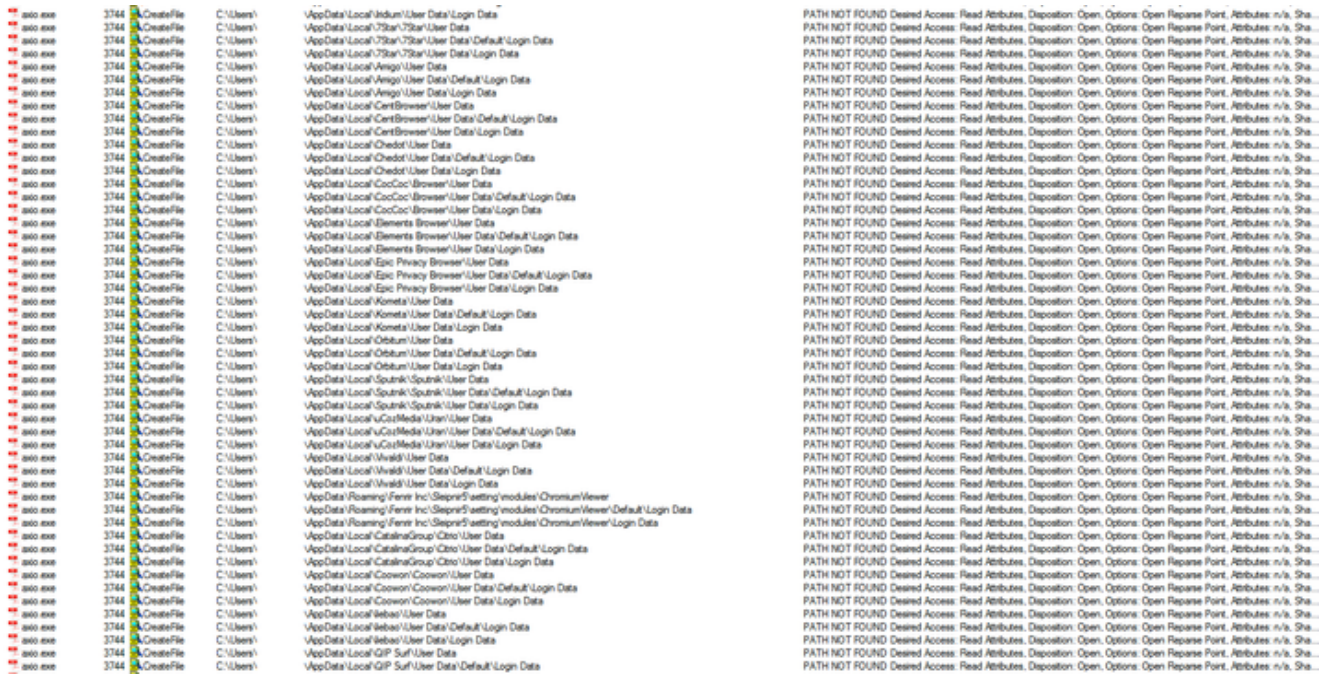
MassLogger's settings 2

Credential Logging

As the trend to execute malicious code in memory continues, MassLogger also makes use of this. The sample we investigated starts itself in a new process, allocates executable memory and injects the mentioned routine into the newly created process via Process Injection. The new process starts to iterate over files holding login credentials and writes them into a new file.

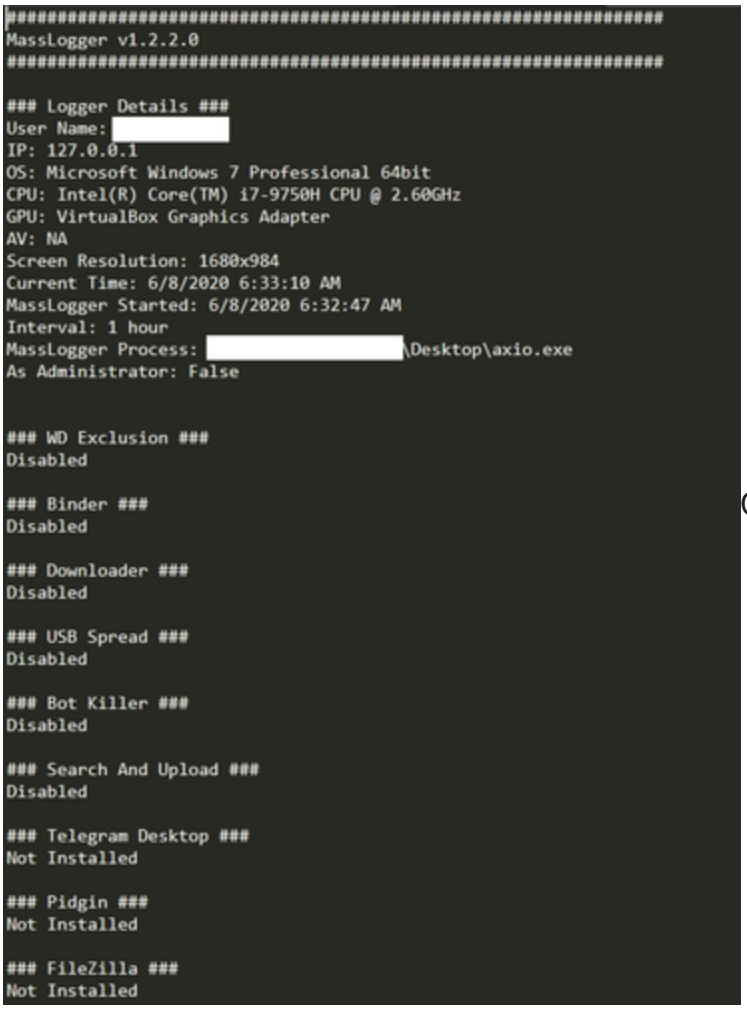


Created suspended process, ready for Process Injection



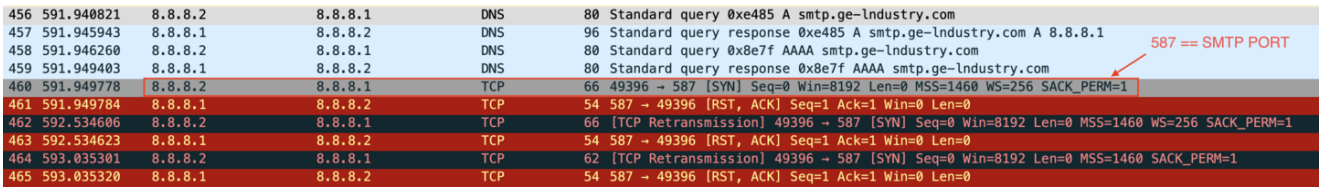
Iteration through files holding sensitive information

The sample writes credentials, as well as its configuration into a separate log file. It also has the capability to take screenshots.



Created log file holding information about victim's system and MassLogger's configuration

The C2 carrier protocol depends on the sample's configuration, the variant we investigated tried to send the results over SMTP to the c2 server. We also identified that MassLogger can atleast be configured to transfer the logging results via FTP to its control server.



Captured SMTP traffic to c2 domain

Preventing MassLogger infection and outlook

During the creation of this article, we continued to watch MassLogger and its distribution. We believe that MassLogger will spread and stay alive for at least the next months. So it is recommened to keep an eye on suspicious mails, because malicious email attachments are still the most popular way to distribute malware. Furthermore we suggest to stay updated on the current threat landscape and read cyber security news in order to proactively defend yourself against cyber security threats.

IoCs

Sha256
8978b5eb14061436a8d2249f9c92ac75d8307c83a09ea7aa3e6572f704b4335f
c994eb9b388217d028184b271dbd7fa098e0488f24af28d5a4ead55bf0c1a92f
25fa4b1716f5d2995ff28002601f7fd2fc76f03831bcd642b9a2e49e92c42238
786b5266ae016683f13abe07cb1e99c01b2d617d3ca7518da086571d9f158d1b
335d39ae0c6e633ba50441e0b482b11d0311d09ad9a286123e6a854660518715

Andreas Klopsch
Virus Analyst

Techblog