

# Harmful Logging - Diving into MassLogger

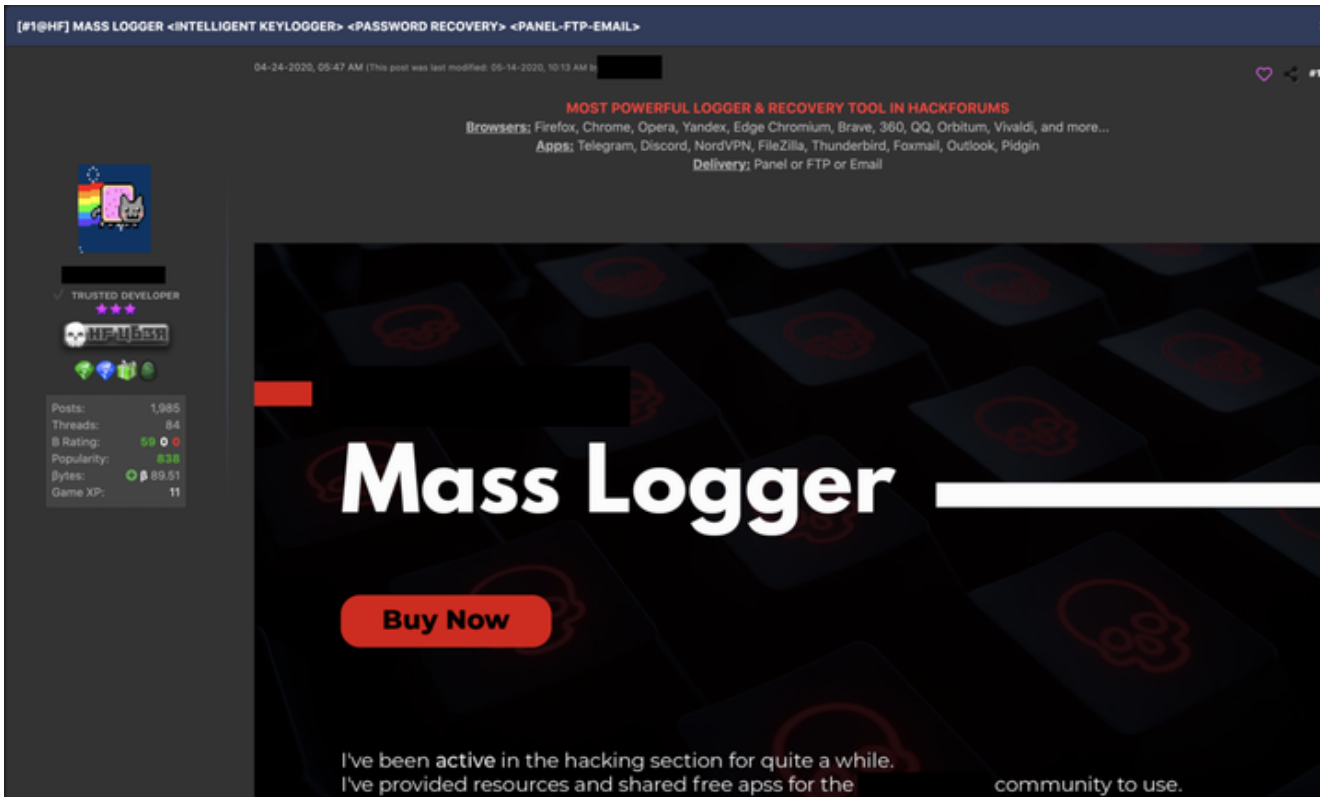
 [gdatasoftware.com/blog/2020/06/36129-harmful-logging-diving-into-masslogger](https://gdatasoftware.com/blog/2020/06/36129-harmful-logging-diving-into-masslogger)



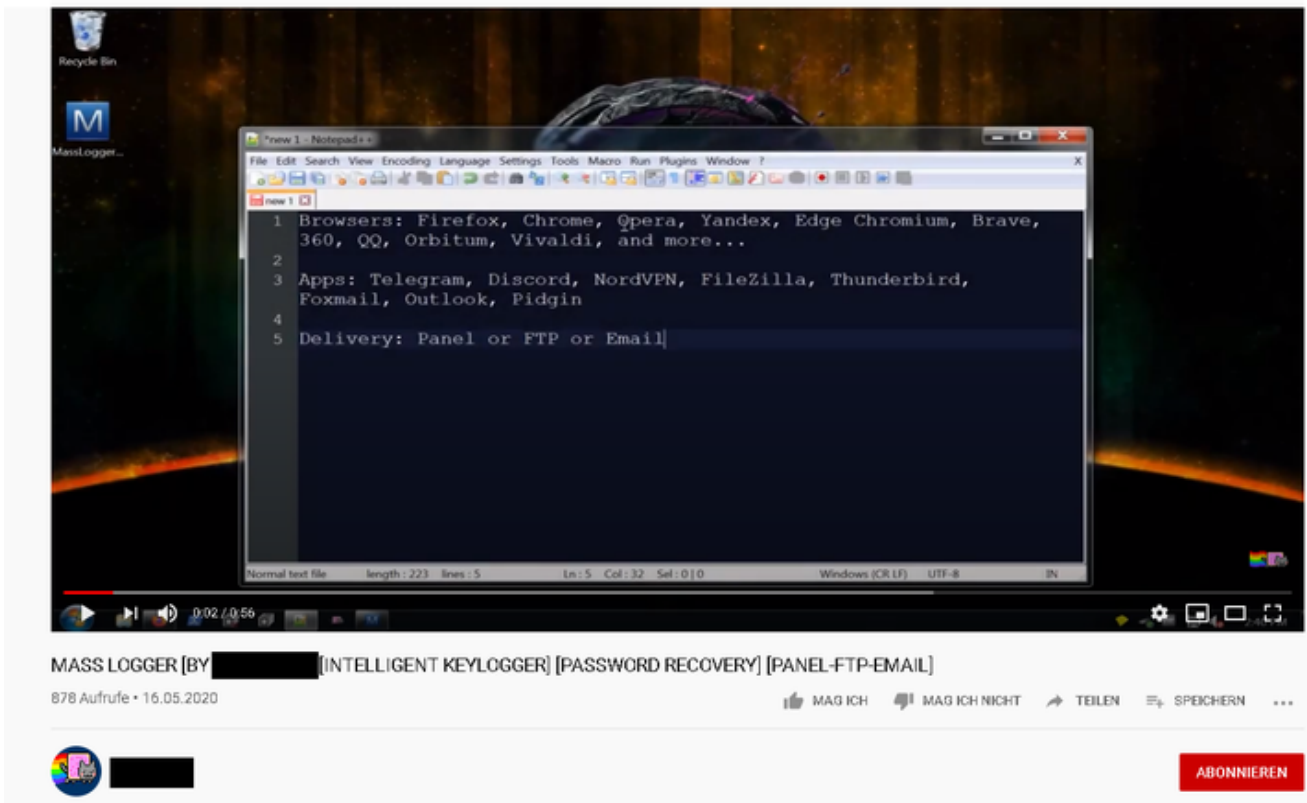
There are many things that can be logged on a computer. While not all logging data is useful for the average user, a lot of logging goes on in the background of any system. However: There is good logging and bad logging. We have looked at an example of logging you definitely would not want.

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 advertisement 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.

```

53 switch ((num = (num ^ 2131659560U)) % 9U)
54 {
55 case 0U:
56     Environment.FailFast("");
57     num2 = ((num * 1054361593U ^ 4200582193U);
58     continue;
59 case 1U:
60 {
61     Process process = <Module>.\u208C\u208E\u2082\u2082\u208A\u2082\u208A\u208F\u208E\u2082\u2082\u208E\u2082\u2086\u208E\u2082\u208C\u2086\u208E\u2082\u208C\u208F\u2086\u208C\u2088\u2088\u2082\u2082\u208D\u208C\u2088
62     num2 = 115885645U;
63     continue;
64 }
65 case 2U:
66     goto Il_12A;
67 case 3U:
68 {
69     Process process;
70     num2 = (((process.ProcessName.ToLower()).Contains("dnspy") ? 2085646920U : 41038449U) ^ num * 980331940U);
71     continue;
72 }
73 case 4U:
74     goto Il_1B;
75 case 6U:
76 {
77     Process process;
78     num2 = (((process == null) ? 965535744U : 583387554U) ^ num * 2158101641U);
79     continue;
80 }
81 case 7U:
82     new Thread(new ParameterizedThreadStart(<Module>.\u208C\u208E\u2082\u2082\u2088\u2082\u2082\u208A\u2082\u208E\u2082\u2086\u208E\u2082\u208C\u208F\u2088\u208E\u2082\u208C\u208A\u2082\u208A\u208E\u2082\u208C\u208F\u208E\u2082\u2086\u208E\u2082\u208C\u208F\u2086\u208C\u2088\u2088\u2082\u2082\u208D\u208C\u2088
83     {
84         IsBackground = true

```

Name	Value	Type
this	"dnSpy-x86"	string

Packer stage looking for dnspy substring in process name

```

BinderBytes : string @040000FA
BinderName : string @040000FB
BinderOnce : string @040000FC
class52_0 : Class52 @04000108
DownloaderFilename : string @040000F7
DownloaderOnce : string @040000F8
DownloaderUrl : string @040000F6
EmailAddress : string @040000D9
EmailClient : string @040000DE
EmailEnable : string @040000D8
EmailPass : string @040000DB
EmailPort : string @040000DC
EmailSendTo : string @040000DA
EmailSsl : string @040000DD

```

- EnableAntiDebugger : string @040000E7
- EnableAntiHoneyPot : string @040000F2
- EnableAntiSandboxie : string @040000E5
- EnableAntiVMware : string @040000E6
- EnableBinder : string @040000F9
- EnableBotKiller : string @040000EF
- EnableBrowserRecovery : string @040000EC
- EnableDeleteZoneIdentifier : string @040000F0
- EnableDownloader : string @040000F5
- EnableForceUac : string @040000EE
- EnableInstall : string @040000FD
- EnableKeylogger : string @040000EB
- EnableMemoryScan : string @040000F1
- EnableMutex : string @040000E4
- EnableScreenshot : string @040000ED
- EnableSearchAndUpload : string @040000E9
- EnableSpreadUsb : string @040000EA
- EnableWDEXclusion : string @040000E8
- EnableWindowSearcher : string @04000104
- ExecutionDelay : string @040000F3
- ExitAfterDelivery : string @040000E1
- FtpEnable : string @040000D3
- FtpHost : string @040000D4
- FtpPass : string @040000D6
- FtpPort : string @040000D7
- FtpUser : string @040000D5
- InstallFile : string @04000100
- InstallFolder : string @040000FE

MassLogger's settings 1

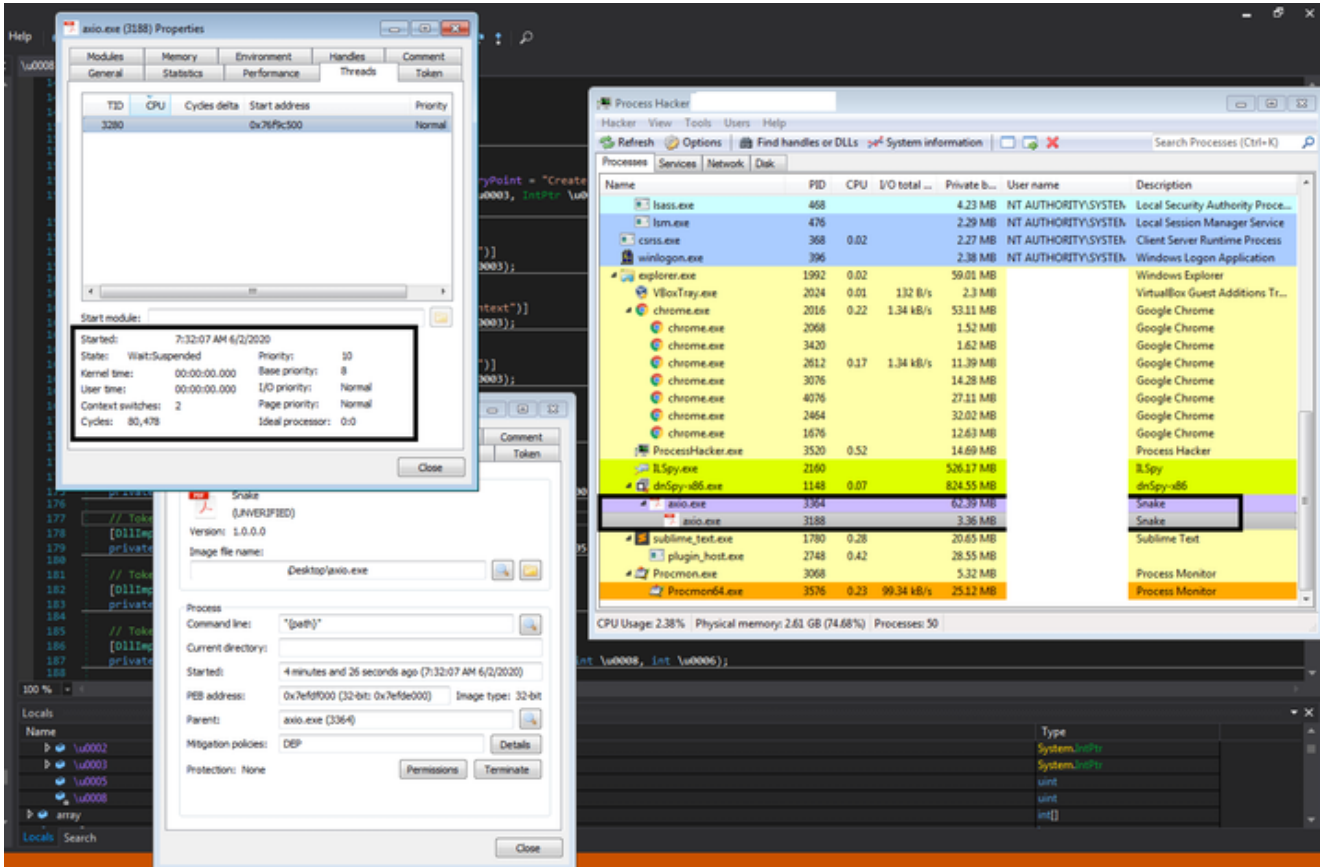
```
InstallFolder : string @040000FE
InstallSecondFolder : string @040000FF
Key : string @040000D1
MainDirectory : DirectoryInfo @04000106
Mutex : string @040000E3
PanelEnable : string @040000DF
PanelHost : string @040000E0
SafeThread : object @04000107
SearchAndUploadExtensions : string @04000101
SearchAndUploadSizeLimit : string @04000102
SearchAndUploadZipSize : string @04000103
SelfDestruct : string @040000E2
SendingInterval : string @040000F4
Version : string @040000D2
WindowSearcherKeywords : string @04000105
```

MassLogger's settings 2

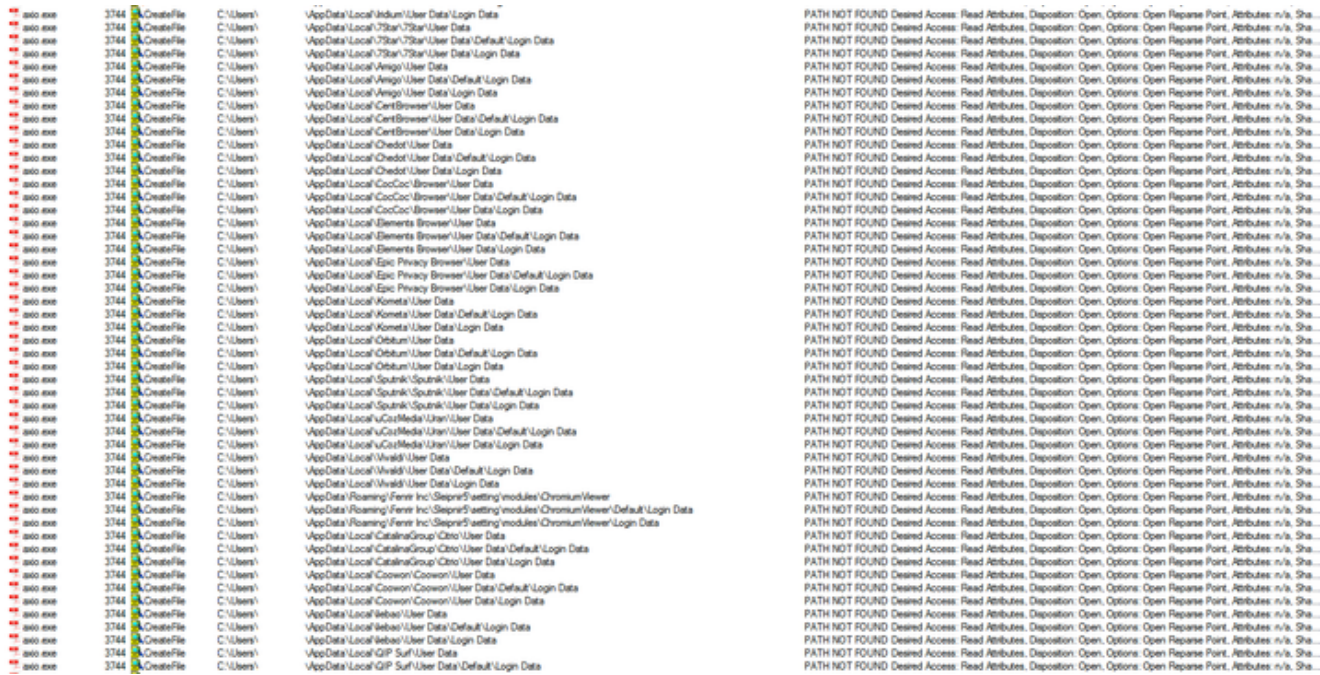
## Credential Logging

---

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.

```

#####
MassLogger v1.2.2.0
#####

### Logger Details ###
User Name: [REDACTED]
IP: 127.0.0.1
OS: Microsoft Windows 7 Professional 64bit
CPU: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz
GPU: VirtualBox Graphics Adapter
AV: NA
Screen Resolution: 1680x984
Current Time: 6/8/2020 6:33:10 AM
MassLogger Started: 6/8/2020 6:32:47 AM
Interval: 1 hour
MassLogger Process: [REDACTED]\Desktop\axio.exe
As Administrator: False

### WD Exclusion ###
Disabled

### Binder ###
Disabled

### Downloader ###
Disabled

### USB Spread ###
Disabled

### Bot Killer ###
Disabled

### Search And Upload ###
Disabled

### Telegram Desktop ###
Not Installed

### Pidgin ###
Not Installed

### FileZilla ###
Not Installed

```

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.

456	591.940821	8.8.8.2	8.8.8.1	DNS	80	Standard query 0xe485 A smtp.ge-lndustry.com
457	591.945943	8.8.8.1	8.8.8.2	DNS	96	Standard query response 0xe485 A smtp.ge-lndustry.com A 8.8.8.1
458	591.946260	8.8.8.2	8.8.8.1	DNS	80	Standard query 0x8e7f AAAA smtp.ge-lndustry.com
459	591.949403	8.8.8.1	8.8.8.2	DNS	80	Standard query response 0x8e7f AAAA smtp.ge-lndustry.com
460	591.949778	8.8.8.2	8.8.8.1	TCP	66	49396 → 587 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
461	591.949784	8.8.8.1	8.8.8.2	TCP	54	587 → 49396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
462	592.534606	8.8.8.2	8.8.8.1	TCP	66	[TCP Retransmission] 49396 → 587 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
463	592.534623	8.8.8.1	8.8.8.2	TCP	54	587 → 49396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
464	593.035301	8.8.8.2	8.8.8.1	TCP	62	[TCP Retransmission] 49396 → 587 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
465	593.035320	8.8.8.1	8.8.8.2	TCP	54	587 → 49396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

587 == SMTP PORT

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 recommended 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](#)