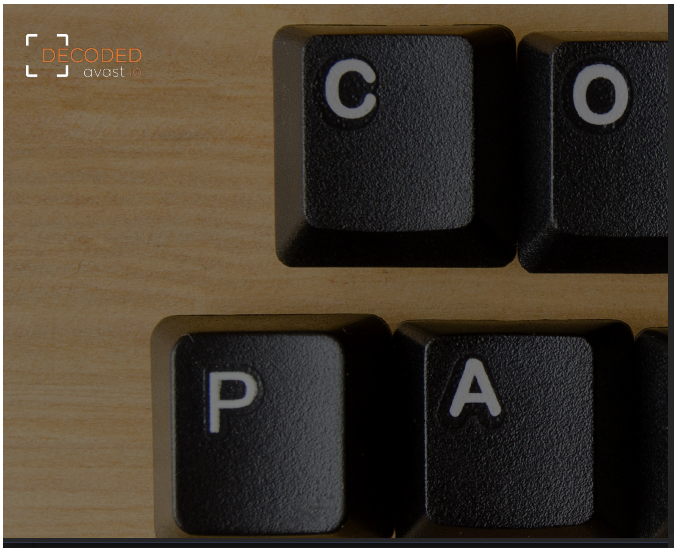

Overview

BluStealer is is a crypto stealer, keyloggei
C#.NET hack tools to steal credentials. Th
and referred to as a310logger. In fact, a31
ponent that appeared in the string artifa
"fresh malware", and recently it is mentior
to go with the BluStealer naming while p
inner workings.

a310logger is just one of the r

BluStealer is primarily spread through ma
come from a particular campaign that is
analysis of this loader is provided in this
first is a fake DHL invoice in English. The
metal company, in Spanish. Both samples
sages claim is a form that the lure claims
The attachments contain the malware exe

In the graph below, we can see a signific
10-11, 2021.

The daily amount

BluStealer Analysis

As mentioned, BluStealer consists of a co
Both components vary greatly among the
ize each component separately. The VB c
ject, hence the inclusion of "SpyEx" strings
have added the capabilities to steal cryp
board, find and upload document files, e:
well as anti-analysis/anti-VM tactics. On t
stealer that is patched together from a
derFox, ChromeRecovery, StormKitty, a
available in a single sample.

Obfuscation

Example of how t

Each string is encrypted with a unique key
the xor cipher, RC4, or the WinZip AES im
tion of the custom AES algorithm:

A utility to help decrypt all strings in IDA i

Anti-VM Tactics

BluStealer checks the following conditions

If property Model of Win32_ComputerSy

VIRTUA (without L), VMware Virtual Plat
vmw

If property SerialNumber of Win32_BaseB

If the following files exist:

- C:\\Windows\\System32\\drivers\\vmh
- C:\\Windows\\System32\\drivers\\vmn
- C:\\Windows\\System32\\drivers\\vmn
- C:\\Windows\\System32\\drivers\\vmr
- C:\\Windows\\System32\\drivers\\VBo
- C:\\Windows\\System32\\drivers\\VBo
- C:\\Windows\\System32\\drivers\\VBo
- C:\\Windows\\System32\\drivers\\VBo

If any of these conditions are satisfied, Blu

.NET Component

The BluStealer retrieves the .NET payload
WinZip AES algorithm using a hardcode
utilities to launch the .NET executable(s):

- C:\Windows\Microsoft.NET\\Microsoft
- C:\Windows\\Microsoft.NET\\Framew

Examples of two .NET executables loaded b

The .NET component does not communic
popular browsers and applications then
filename (i.e credentials.txt). The VB core
is better explained in the next section.

The .NET component is just a copypasta
information on their respective Github pag

- ThunderFox: github.com/V1V1/Sharp
- ChromeRecovery: github.com/Elysian
- StormKitty: github.com/swagkarna/St

June 2020
May 2020
April 2020
December 2019
September 2019
August 2019
July 2019
April 2019
March 2019
February 2019
January 2019
August 2018
January 2018
October 2017

Meta

Log in
Entries feed
Comments feed
WordPress.org

- Firepwd:github.com/lclevy/firepwd

Information Stealer

Both the VB core and the .NET component plates folder. Each type of stolen data is core sets up different timers to watch ove size increases, the VB core will send it to t

Handler	Arbitrary file
.NET component	credentials
.NET component	Cookies.z
VB Core	CryptoWalle
VB Core	FilesGrab ber\\Files.z
VB Core	Others

BluStealer VB core also detects the crypto the attacker's predefined ones. Collective cash, Ethereum, Monero, Litecoin.

Data Exfiltration

BluStealer exfiltrates stolen data via SMT of server-side code. The Telegram token sendDocument and sendMessage as shov

- https://api.telegram.org/bot[BOT [MY_MESSAGE_TEXT]
- https://api.telegram.org/bot[BOT TO [MY_CAPTION]

The SMTP traffic is constructed using Micr

E

.NET Loader Walkthrough

This .NET Loader has been used by famil
Stealer, RedLine, as well as BluStealer.

Demo sample: 19595e11dbccfbfeb9560e

First Stage

The first stage of the .NET loader has a g
known .NET obfuscator. However, one r
crypted module in the resource:

By looking for this module's reference with
loaded into memory as shown below

Prior to loading the next stage, the loade
through the Startup folder and registry rur

- C:\Users*\AppData\Roaming\Microsc
- HKEY_CURRENT_USER\Software\Mic
- C:\Users*\AppData\Roaming\Microsc
- HKEY_CURRENT_USER\Software\Mic
- HKEY_CURRENT_USER\Software\Mic
s\Startup
- HKEY_CURRENT_USER\Software\Mic
tartup
- C:\Users*\AppData\Roaming\Microsc

In the samples we looked at closely, the r
key is obfuscated by a string provider fun
tail jump that resides within the same nar
cases, it usually is the call to the external f
ples:

Second stage

Inside the Data() function of the second stage

The second stage has the function calls a
as helpful. However, there are two resou
Their getter functions can be easily found
the breakpoint on the Ehiuuvbfrnprkuyuxc
it is gzip decompressed revealing a PE file.

Ehiuuvbfrnp

On the other hand, the breakpoint on t

leaves us in the middle of the Data() funct
into CompareComparator function that wi

ComareCompara

In order to understand what is going on, w
the experience working with **MassLogger**
in the resource section, which in this case,

Note that it is important to find out wher
get us directly to the designated functior
field-method binding process. So when
solver.GetCodeInfo() will be called to buil
modification only consists of replacing sor
the same, it is sufficient enough to obfusc

Dic.Attr is inte

The search of the "Dic.Attr" string leads u
value represents the method token that w
for the method tokens start with 0x4A, ju
are the chosen ones to be modified for obf

With all the function calls revealed, we c
First, it loads a new assembly that is the
an instance of an object named SmartA
method called "RegisterSerializer" is invok
At this point, we can assume that the pur
file and execute it.

Heading to the newly loade
ca13649d15f5c7d36b69274a76efdac), w
cation features labeled as shown below.

Overview of the decompressed Ehiuuvbfrnprkuyuxqv.
bly

The unpacking process will not be much
code virtualization. From static analysi
SmartAssembly.Queues class is instantiat

The functio

The function content after instantiated.

Fast forward to whe

Lucky for us, the code looks fairly straight
is passed to a function that RulesListener
the field token to method token map file w
searching for the GetManifestResourceSt
where the map is established:

The resource file Params.

RulesListener.IncludeState has token 0x0
this function, the decryption algorithm is re

Data from L

Then it

In fact, all the samples can be unpacked s
ded in the second stage. Hopefully, ever
will remain useful at showing you how to

Conclusion

In this article, we break down BluStealer f
extract its IOCs. We also highlight its code
data to disk and without a proper C2 fun
half of the blog, we show how the BluSt
unique .NET loader. With these insights, w
ing and analyzing BluStealer.

IOCs:

The full list of IoCs is available at https://g

BluStealer

SHA-256

678e9028caccb74ee81779c5dd6627fb6f
3151ddec325ffc6269e6704d04ef206d62
49da8145f85c63063230762826aa8d85d
7abe87a6b675d3601a4014ac6da843924

Crypto Address List

Bitcoin:
1ARtkKzd18Z4QhvHVijrVFTgerYEoopjLP
1AfFoww2ajt5g1YyrrfNYQfKJAjnRwVUsX
1MEf31xHgNKqyB7HEeAbcU6BhofMdwL
38atNsForzrDRhJoVAhyXsQLqWYfYgodd
bc1qrjl4ksg5h7p70jjtypr8s6cjpngzd3kerfj
bc1qjg3y4d4t6hwg6h22khknlxcstevjg2qk
1KfRWVcShzwE2Atp1njogAqH8qodsif3p
3P6JnvWtubxbCxgPW7GAAj8u6CLV2h9
13vZcoMYRcKrDRDYUyH9Cd4kCRMZVjF

Bitcoincash:
qrej5ltx0sgk5c7aygdsvt2gh7fq04umvusxl
qrzakt59udz893u2uuwtgrwrjj9dhtk0gc3m

Ethereum:
0xd070c48cd3bdeb8a6ca90310249aae9
0x95d3763546235393B77aC188E5B08d
0xcfE71c720b7E99e555c0e98b725919B7

Monero.address:
46W5WHQG2B1Df9uKrkyuhoLNVtJouMf
wYRXhBYVjLRbpDu8CK2UN2xzenr
43Q4G9CdM3iNbkwhujAQJ7TedSLxYQ8h
caQeoSF86eFE2fL9njU59dQRfPHFnv

Litecoint address:
LfADbqTZoQhCPBr39mqQpf9myUiUiFrDE

LY5jmjdFnvgFjJET2wX5fVV6Gv89QdQRv

Telegram Tokens:

1901905375:AAFoPAvBxaWxmDiYbdJW
1989667182:AAFx2Rti45m06IscLpGbHo

SMTP

andres.galarraga@sismode.com (smtp.1a
info@starkgulf.com (mail.starkgulf.com)
etopical@bojtai.club (mail.bojtai.club)
fernando@digitaldirecto.es (smtp.ionos.es
baerbelscheibll1809@gmail.com
dashboard@grandamishabot.ru (shepher
shan@farm-finn.com (mail.farm-finn.com)
info@starkgulf.com (mail.starkgulf.com)

.NET Loader SHA-256:

ae29f49fa80c1a4fb2876668aa38c8262d
35d443578b1eb0708d334d3e1250f6855
097d0d1119fb73b1beb9738d7e82e1c73
c783bdf31d6ee3782d05fde9e87f70e9f3c
42fe72df91aa852b257cc3227329eb5bf4
1c29ee414b011a411db774015a98a897
81bbcc887017cc47015421c38703c9c261
6956ea59b4a70d68cd05e6e740598e76e
6322ebb240ba18119193412e0ed7b325
9f2bfedb157a610b8e0b481697bb28123
e2dd1be91c6db4b52eab38b5409b39421

Tagged as

Cryptostealer Malware Analysis

Share:

Furth

PC

DirtyMoe: Code Signing Certifica

26 min read

The Windows kernel allows loading drivers signed
voked certificates that are moreover widely abused
mechanism...

PC

DirtyMoe: Rootkit Driver

38 min read

The DirtyMoe malware is a complex malicious backd
One of the more significant safeguards is a rootkit. Th