sekoia

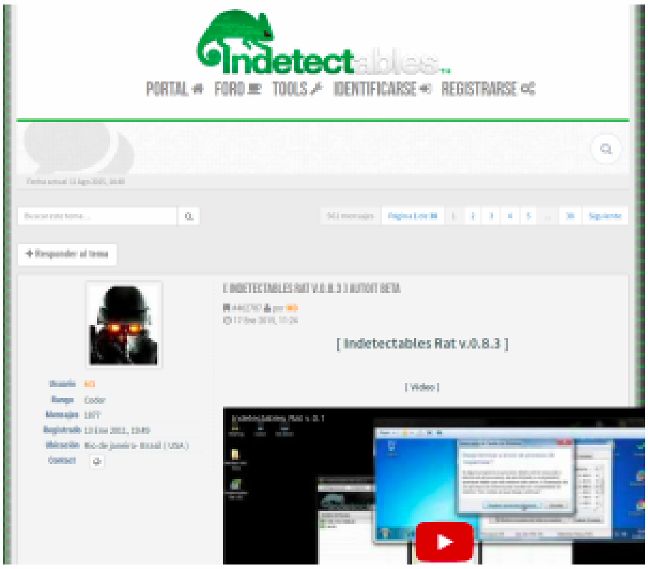
WHEN A BRAZILIAN STRING SME

Posted On 01 Oct 2015

Indetectables… did you say *indetectables*…

INDETECTABLES RAT

The experts of SEKOIA’s CERT discovered by chance a not yet famous RAT called *Indetectables RAT*. This RAT (Remote Administration Tool) is a malware freely available on the *Indetectables* forum here: http://www.indetectables.net/viewtopic.php?f=7&t=52263. This forum is a spanish security/hacking forum. In Spanish, *Indetectables* means undetectable. Here is a screenshot of the forum:



[INDETECTABLES RAT V.0.8.3] AUTOIT BETA

[Indetectables Rat v.0.8.3]

[Video]

The RAT and the administration panel are developed in AutoIt and has common features such as:

- Command execution;
- File upload;
- File download

- Passwords stealer;
- Keylogger;
- Webcam spying;
- …

The latest version of the RAT is 0.8.3.

The malware is developed by **M3**, a coder located in Rio de Janeiro in Brazil. We will speak about him later in the article.

REMOTE CODE EXECUTION

As the malicious software is developed in AutoIt, we can easily have access to the source code of the application with Exe2Aut. After a few minutes of analysis, we identified several vulnerabilities on the administration panel (the C&C part). One of these vulnerabilities was particularly interesting because it allows Remote Code Execution on the C&C when the operator tries to switch on the webcam remotely. When this task is launched, the following vulnerable code is executed:

```
17325    $swebcamclientex = BinaryToString($swebcamcliente)
17326    $swebcamclientebuilder = StringReplace($swebcamclientex, "@IPAddress1", '"' & $sreceivedataaddress & '"')
17327    $swebcamclientebuilderx = StringReplace($swebcamclientebuilder, '"[ WebCam Remota ]"', '"[ WebCam Remota ]"' & " & " & '" [ ' & $sgetuserpc & ' ]"')
17328    If FileExists($swebcamlisten) Then FileDelete($swebcamlisten)
17329    FileWrite($swebcamlisten, $swebcamclientebuilderx)
17330    Local $sfileexe = FileGetShortName(@AutoItExe & ' /AutoIt3ExecuteScript "' & $swebcamlisten & '"')
17331    Sleep(1000)
17332    $ipid = Run($sfileexe)
```

This part of the code is used to generate, compile and execute an AutoIt script on the fly. Line 17325 decodes the script contained in the variable $swebcliente. The lines 17326 and 17327 replace 2 values in the code. Finally the generated code is stored in a file on the line 17329. The file is compiled at line 17330 and finally executed at line 17332.

The weakness in this code is the fact that $sgetuserpc is controlled by the infected user. This variable contains the username and the computer name of the infected system. By manipulating this value, we can update the code with an arbitrary string. Here is the replaced line:

```
$ZPOLNXGRSJSUHCT = GUICreate("[ WebCam Remota ]",330,180, -1, -1, -1)
```

Here is the line where the hostname is set on the RAT:

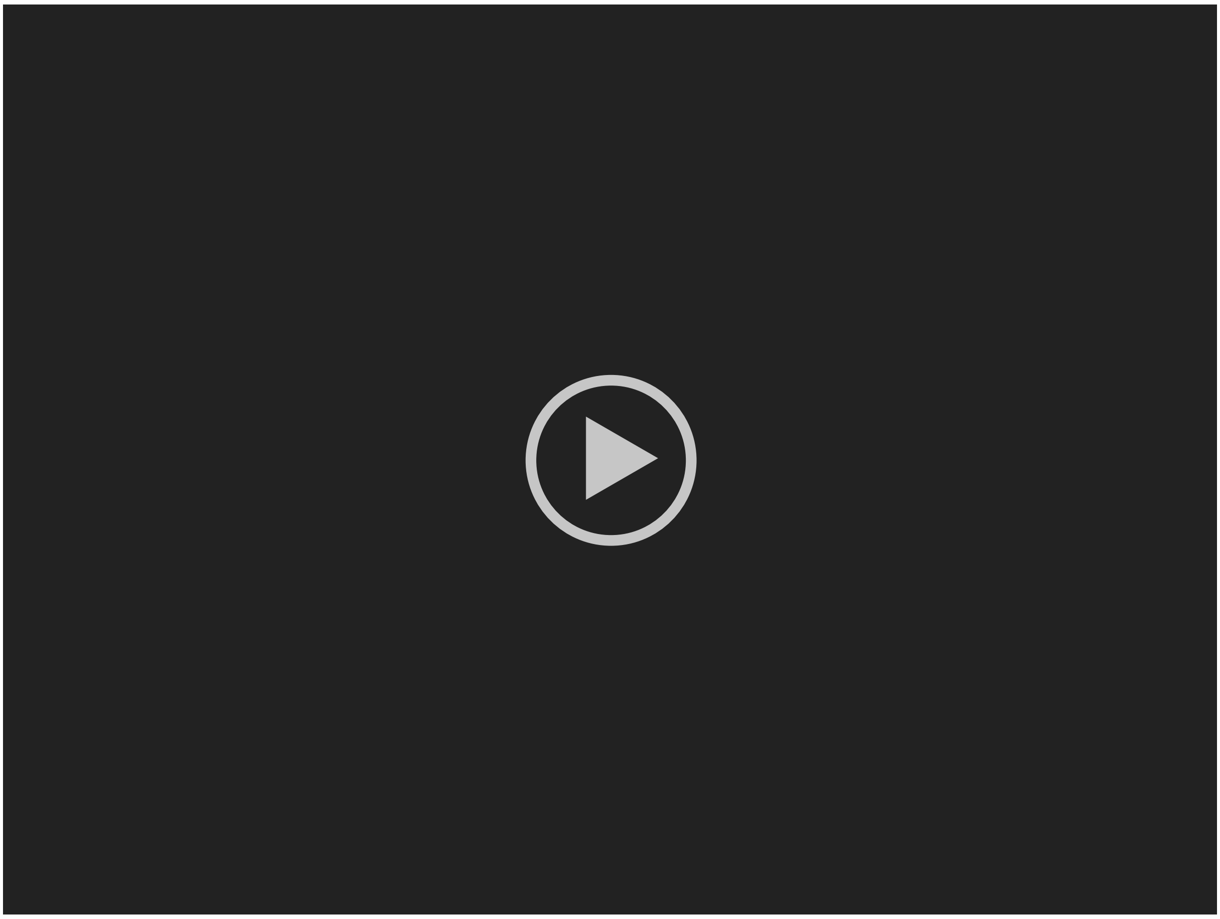
```
$sServerInfo = $sKeyBuffer & @ComputerName & $sKeyBuffer & $sAvInstalled & _
```

So we can simply modify the RAT source code in order to change our hostname:

```
$sServerInfo = $sKeyBuffer & "paul - ABC1234                     ]"", 330, 1
80, -1, -1, -1) & Run(""c:\Windows\System32\calc.exe"") ;#" & $sKeyBuffer &
$sAvInstalled & _
```

Thanks to this new hostname, we are able to execute the calc.exe on the C&C.

Here is a video on the exploitation:



1. “Exploit POC” **3:02**

Exactly the same kind of vulnerability can be found on other features of the malware.

AUTHOR’S BACKGROUND

BINARIES

We saw in the forum that the author is located in Rio de Janeiro in Brazil and his username is **M3**. We found a lot of samples on VirusTotal with the same username, developed in

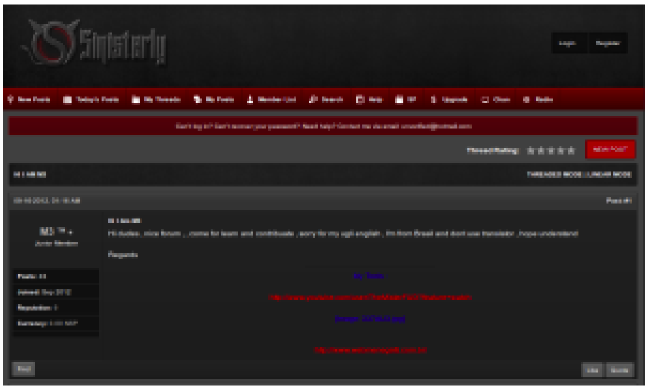
AutoIt and with the same pattern of window title naming (usage a [] or [[ ]]).

Some example of strings available on several samples:

- 081905074c19d5e32fd41a24b4c512d8fd9d2c3a8b7382009e3ab920728c7105:
  [[__M3_F_U_D_M3__]]$
- 66306c2a55a3c17b350afaba76db7e91bfc835c0e90a42aa4cf59e4179b80229:
  Coded By M3
  Stub Undetector M3
  M3 Softwares

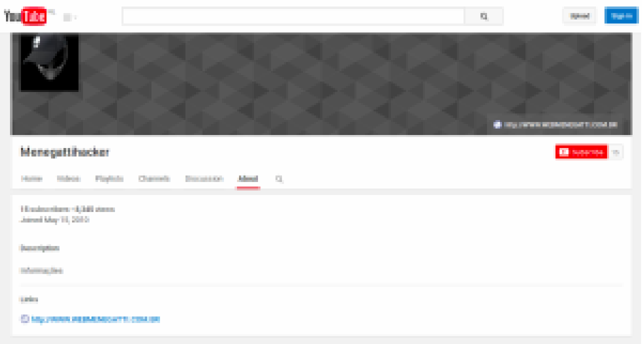
The majority of the tools developed by this coder contain his username. The last sample mentioned previously is interesting because it also contains an URL: http://www.webmenegatti.com.br/. This URL was associated to another username available on a hacking forum called Sinister.ly.

Here is a screenshot of the post:



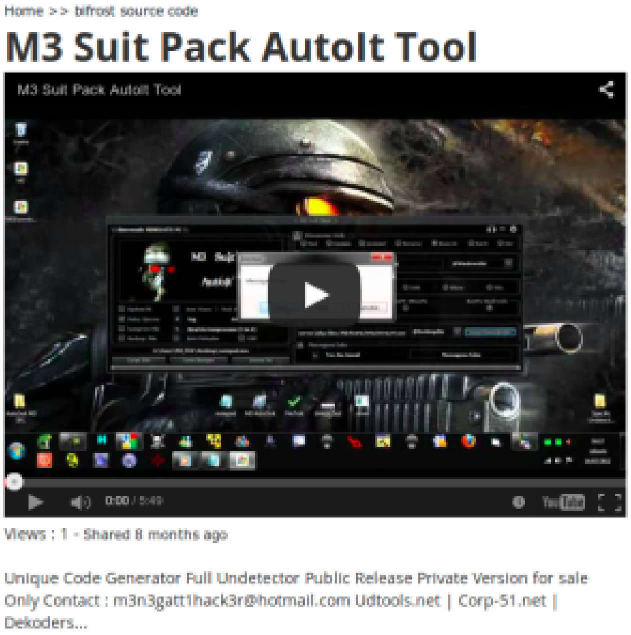
We can see in the user signature a YouTube link (called “My Tools”) and the link to the Brazilian website. The YouTube user is **TheMisterFUD** and the logo of the user is the same than the logo used by **M3** on the *Indetectables* forum.

The Brazilian website is mentioned in a third account: **Menegattihacker** on YouTube: https://www.youtube.com/user/Menegattihacker/about



Menegattihacker

This third pseudonym is interesting. After some research we found another way to write it: **M3n3gatt1hack3r,** with a lot of references to FUD and hacking products for sale:



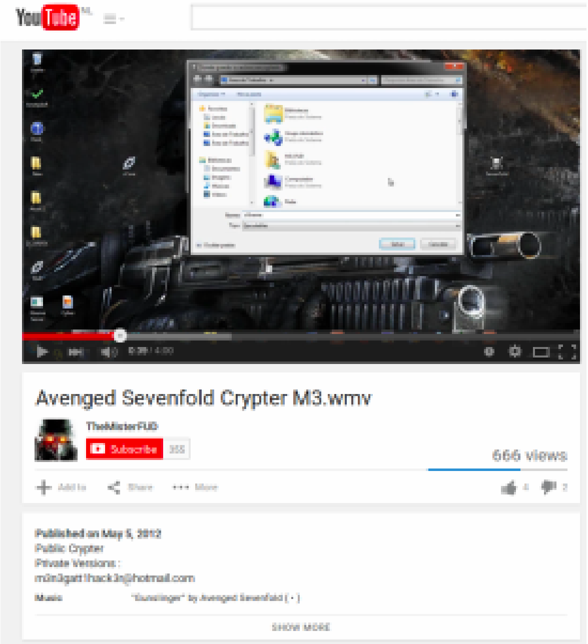
Home >> bifrost source code

M3 Suit Pack AutoIt Tool

Views : 1 - Shared 8 months ago

Unique Code Generator Full Undetector Public Release Private Version for sale Only Contact : m3n3gatt1hack3r@hotmail.com Udtools.net | Corp-51.net | Dekoders...

Moreover the **TheMisterFUD** YouTube account present tools developed by **M3n3gatt1hack3r**:



Avenged Sevenfold Crypter M3.wmv

TheMisterFUD

666 views

Published on May 5, 2012
Public Crypter
Private Versions :
m3n3gatt1hack3r@hotmail.com

Music "Gunslinger" by Avenged Sevenfold (•)

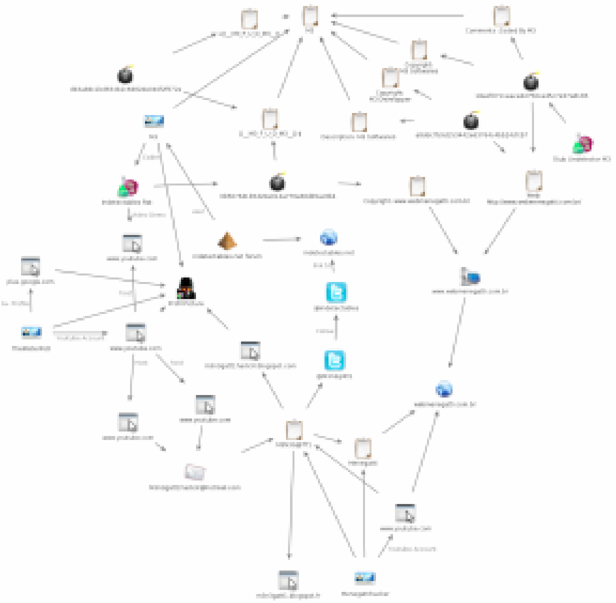
PSEUDONYMS LINKS

Thanks to the analysis of information publicly available on the Internet, we have strong suspicions that **M3** uses several pseudonyms: **Menagattihacker** and **M3n3gatt1**. In fact we think that **M3** is probably a short version of **M3n3gatt1**.

Moreover, they are strong links that may indicate that **M3** and **TheMisterFUD** are an unique person too.

We are quite confident that webmenegatti.com.br is a legitimate software company.

You can see the relations between the elements there:



Based on the hypothesis that **MisterFUD**, **M3** and **M3n3gatt1** are the same person, we have noticed a change of username during the time. Our guess is that **M3n3gatt1** is a “hacking” enthusiast since the mid-2000s. He wrote AV bypass, FUDer software and spent time in a South America hacking forum. He changed to **M3** during 2010/2012. Then we mostly see **TheMisterFUD** presence.

We have first thought that he changed from **M3n3gatt1** to **M3** then to **TheMisterFUD** in order to protect its identity and the legitimate software development activity he runs with webmenegatti.com.br (Menegatti Soluçoes Software, created in 2003). But he has kept the same avatar, still uses **M3n3gatt1**‘s email with **TheMisterFUD** account, has a **@M3n3g4tt1** twitter account following the Indetectables and finally has kept using **M3** string in its code.

We do not really know if he is trying to poorly cover his tracks, to segregate account names on various locations (and then got confused) or if he is just changing username like we are changing haircuts.

CONCLUSION

This article shows that malware developers are as all developers, they can have bugs and security holes. In this case, we were able to gain full access to the C&C.

During this investigation, we were able to link several accounts together, we are not sure at 100% but we think that these accounts are used by the same person. He probably tried to cover his tracks but we can see that this was absolutely not efficient and we were able to have a global view of this malware developer easily.

IOC

MISP event ID at CIRCL: #2286

URL:

- www.webmenegatti.com.br

SHA256:

- 66306c2a55a3c17b350afaba76db7e91bfc835c0e90a42aa4cf59e4179b80229
- 081905074c19d5e32fd41a24b4c512d8fd9d2c3a8b7382009e3ab920728c7105

SEKOIA.FR TRAINING EMERGENCY CONTACT

- 7d47f14eae6bd006454afe832afda943b03bba0c
- 2ff7a6cb6fcdb1cab3e1071f587636de37e0cfce

MD5:

- 18a1f0711eaca32750ced5c7247a6165
- 0b507641b5420e014a776e60db5ac6b4

Authors: Paul Rascagnères & Ronan Mouchoux

Paul Rascagneres

Senior threat researcher, malware analyst and IT conf speaker…

Tags: AutoIt brazil exploit indetectable malware rat

PREVIOUS POST

SEKOIA will be at Hack.lu 2015

YOU MIGHT ALSO LIKE

A not so powerful powershell ransomware…

SEPTEMBER 17, 2015

Malware and COM Object – The paradise of covert channels

SEPTEMBER 7, 2015

M

SEKOIA W
2015

The experts of
at Luxembourg
October for th

CATEGORIES

rticles (3)

onferences (4)

ews (1)

on classé (2)

TAGS

2015 APT AutoIt bitcoin brazil C&C chm COM objects conference digital forensics events exploit hack.lu honeypot incident response indetectable Luxembourg malware outlook powershell ransomware rat research security tools

RECENT POSTS

When a Brazilian string smells bad…

SEKOIA will be at Hack.lu 2015

A not so powerful powershell ransomware…

Malware and COM Object – The paradise of covert channels

Nuit Du Hack 2015 (FRANCE, JUNE 20TH – 21TH)