

# Emissary Panda – A potential new malicious tool

18 May 2018

By [Nikolaos Pantazopoulos](#)



◆ Research   ◆ Reverse Engineering   ◆ Vulnerability   ◆ Threat Intelligence

## Introduction

Hacking groups linked to the Chinese state are not a new threat. In fact, for the last couple years they have tended to be the most active along with Russian state affiliated hacking groups. One of these groups is the 'Emissary Panda' group, also known as TG-3390, APT 27 and Bronze Union. This is a hacking group with Chinese origins which targets selected organisations related with education, energy and technology.

In the past, Emissary Panda has used many ways to target their victims, with the most notable being the exploits from the Hacking Team leak. Usually, the delivered payload is either the well-known 'PlugX' or 'HttpBrowser' RAT, a tool which is believed to have Chinese origins and to be used only by certain Chinese hacking groups.

Recent research showed that a new tool is in development from this group, which is still active, and is being found in recent compromised machines. The purpose of this blog post is to briefly describe this new tool we found which has possible ties with the same people who developed 'HttpBrowser'.

## Attribution

While attribution is always hard, we assessed that the Emissary Panda group is highly likely behind the development of this tool based on the following information:



- Several code similarities with previous samples (see examples in Figure 1 and 2).
- Tools were found on compromised machines which have been used in the past by this group. These tools are:
  - ChinaChopper, a web shell which allows the attacker to execute commands on the victim's machine. A password is required in order to interact with the web shell. In our case the password was: "123!@ZA".
  - The publicly available nbtscan and netview enumeration tools.
  - A modifier
  - The Hunt
  - Use of DI past.

This website makes use of cookies.



n the

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

Accept all cookies

Reject all cookies

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

essBuffer

Analytical Cookies

Off

Analytical cookies help us to improve our website by collecting and reporting information on

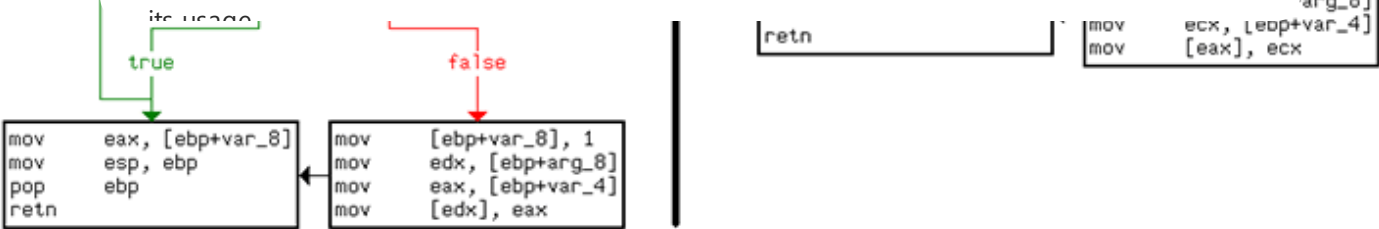


Figure 1: Old sample on the left side, our sample on the right side

mov [ebp+var\_2E], cx  
pop ecx  
push 44h ; 'D'  
mov [ebp+var\_2C], cx  
pop ecx  
push 56h ; 'V'  
mov [ebp+var\_2A], cx  
pop ecx  
push 50h ; 'P'  
mov [ebp+var\_28], cx  
pop ecx  
push 4  
mov [ebp+var\_26], cx  
pop ecx  
push 5  
mov [ebp+var\_24], cx  
pop ecx  
push 7  
mov [ebp+var\_22], cx  
pop ecx  
push 7  
mov [ebp+var\_20], cx  
pop ecx  
push 6  
mov [ebp+var\_1E], cx  
pop ecx  
mov [ebp+var\_1C], cx  
xor [ebp+var\_1A], cx  
mov [ebp+var\_18], cx  
push 1  
lea [ebp+var\_16], ecx  
xor [ebp+var\_14], ecx  
push [ebp+var\_12]  
push [ebp+var\_10]  
mov [ebp+var\_0E], cx  
mov [ebp+var\_0C], cx  
call [ebp+var\_0A]

push 2Eh ; '.'  
mov [ebp+var\_2C], ax  
pop eax  
push 5Ch ; '\\'  
mov ecx, eax  
mov [ebp+var\_2A], cx  
mov [ebp+var\_28], cx  
pop ecx  
push 73h ; 's'  
mov [ebp+var\_26], cx

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Off

amev

Analytical cookies help us to improve our website by collecting and reporting information on

Figure 2: Old sample on the left side, our sample on the right side

Page 3 of 12

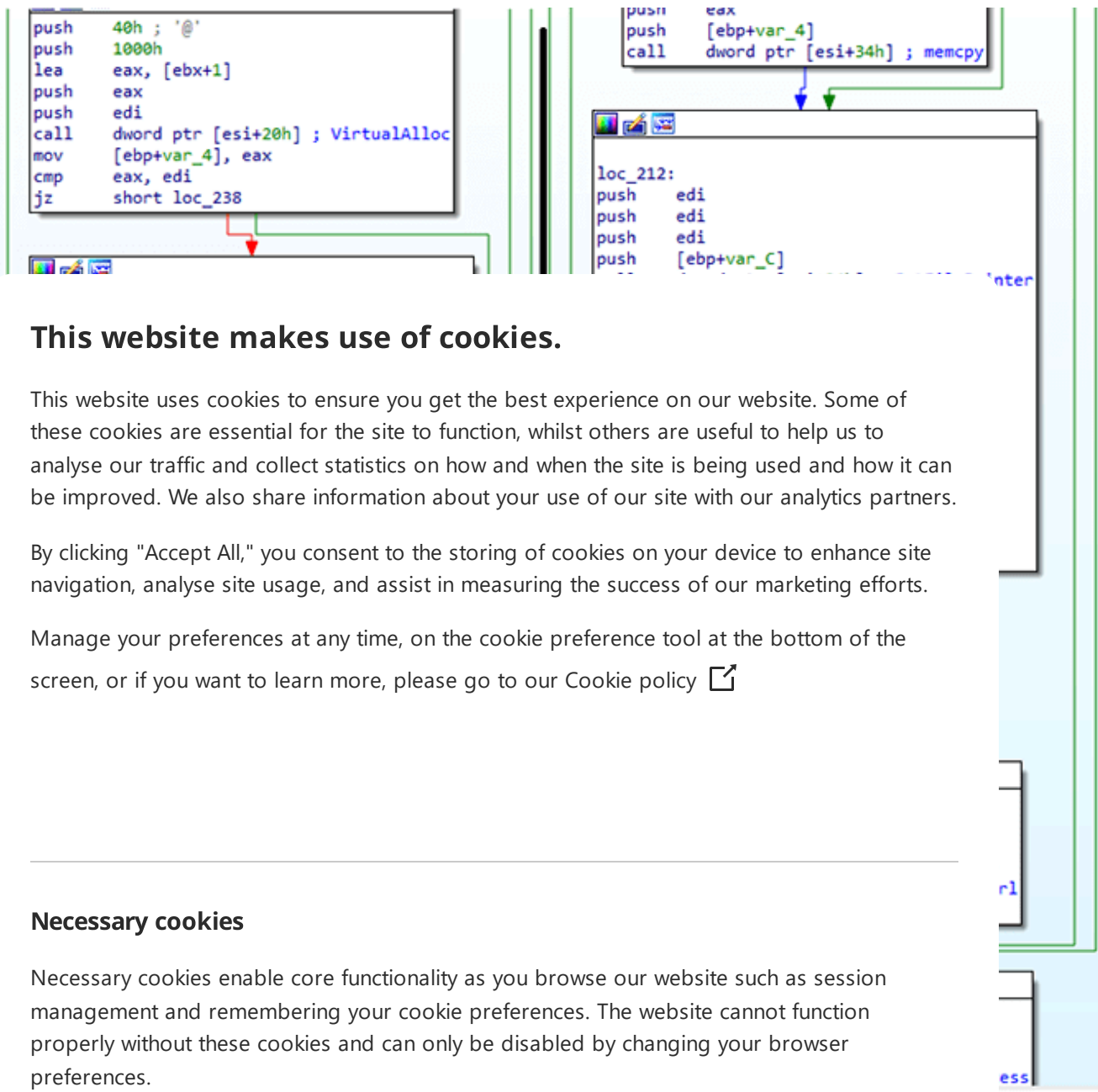


Figure 3:

## Tech

### Analytical Cookies

Based on its usage Analytical cookies help us to improve our website by collecting and reporting information on find two samples which seem to be in development and contain code from some old HttpBrowser samples. Both samples share a lot of code but one of them has more functionality.

The execution starts when a malicious SFX file is executed. The following files are included in the executable:

- INISafeWebSSO.exe – Legitimate file which will load the malicious DLL

- inicore\_v2.3.30.dll – Malicious DLL
- sys.bin.url – The name of both malicious payloads we found

In order to execute the payload, the attackers take advantage of a technique called DLL Search Order Hijacking. Once the malicious DLL is loaded, it will decrypt a part of its own code using a XOR loop (see Figure 4), patch the entry point of the legitimate executable and jump again, back to the malicious DLL (see Figure 5).

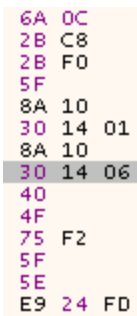


Figure 4:

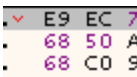


Figure 5:

After jumping to the address dynamically

Lastly, it will XOR decrypt

## Payload

We will focus on the strings within the reason

### This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

#### Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

#### Analytical Cookies

Analytical cookies help us to improve our website by collecting and reporting information on its usage.



```
L"mydebug"
L"Failed"
L"mydebug"
L"Failed"
L"mydebug"
```

The action  
following

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

No. of pages	

- It will check if it runs from the %TEMP% folder, if it does, it will attempt to kill its own process.
- If it runs from the %APPDATA% folder it will spawn a new svchost process with -k as a parameter and it will inject the sys.bin.url to it.
- Otherwise, it will create a new directory with the name systemconfig under %APPDATA%, move all the three files (executable, DLL, sys.bin.url) into it, and will execute the binary from the created

directory using WMI.

## Option one – Svchost injection

Where the number of passed parameters is one, the payload will read the sys.bin.url file from %appdata%\systemconfig. It will then spawns a new svchost process as C:\windows\system32\svchost.exe -k update in suspended state and injects the payload. Finally, it patches the entry point of svchost.exe so it can execute the malicious payload after the ResumeT

## Option two – This website makes use of cookies.

The method  
a user will  
config, in  
service. T

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

ing from  
from the  
the  
meter.

Otherwise  
key with  
it will inje

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

on\Run  
all, then

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

## Option three

This is de

## Option four

An already  
will work  
developm

### Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

ethod  
in

## Core functionality

Currently  
commun  
or downl

### Analytical Cookies



loading

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

## Configuration

Each value of the config is written to the registry after encrypting them using the DES algorithm. A new registry key is created under HKEY\_CURRENT\_USER\Software\Classes using either the SystemProductName value from the HARDWARE\DESCRIPTION\System\BIOS key or the hardcoded string "68A-D3H-B1111 as a name. Additionally, a hardcoded string - HjDWr6vsJqfYb89mxxxx is appended to the name. For example:

- VMware Virtual Service-HjDWr6vsJqfYb89mxxxx or
- Z68A-D3H-B1111-HjDWr6vsJqfYb89mxxxx

The key and the IV used in the encryption are based on the first eight bytes of this registry key's name, for example, VMware V.

The encrypted sub-keys are described below. The majority of these sub-keys will not be read from the payload once they have been written. This might suggest that there are plans to expand the functionality of the tool to include more sub-keys.

registry key found in

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our Cookie policy

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Off

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

Associated Files

Legitimate executable which will

INISafeWebSSO.exe

INISafeWebSSO.exe



	load the DLL file.		
Periodic	N/A	0:1	0:1
Process	Process to inject	svchost.exe	svchost.exe

Serv

ServDi

### This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

3

## Diffe

As menti  
between

- Each sam
- The samp  
to comm  
the binar  
A summa

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

5

1 order  
ded in

Function			
Persiste			
UAC byp			
C&C Cor			
Write co			
Read reg			
Inject to			
x64 Injection			✓
Debug strings	✓		✓
Execution based on params	✓		✓
WMI execution	✓		

# Conclusion

Emissary Panda is still active and continues to target selected organisations. Even though the discovered samples do not have any malicious functionality, we assess that they are still in development and will be used in future attacks.

# References

[1] [https://www.nccgroup.com/us/research-blog/missary-panda-a-potential-new-malicious-tool/](#) [gistry](#)

**Previous** [https://www.cyberesp](#) This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

[https://www](#) By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

**IOCs** Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our Cookie policy [↗](#)

C C IP

103.59

159.65

Registr

HjDWr

Z68A-D

C:Prog

system

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

Systemconfig

Check for this service with description: "for systemconfig"

File Name	SHA-256
INISafeWebSSO.exe	C501203FF3335FBFC258B2729A72E82638719F60F7E6361FC1CA3C856036
inicare_v2.3.30.dll	4D65D371A789AABE1BEADCC10B38DA1F998CD3EC87D4CC1CFBF0AF01

sys.bin.url	2B2BB4C132D808572F180FE4DB3A0A3143A37FDECE667F8E78778EE1E9
sys.bin.url	3E718F39DFB2F6B8FBA366FEFA8B7C127DB1E6795F3CAAD2D4A9F3753E

Published date: 18 May 2018

Written by: Nikolaos Pantazopoulos and Thomas Henry

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our Cookie policy

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Off

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

Terms and Conditions

Privacy Policy

Contact Us

Managed Services

Incident Response

Threat Intelligence

24/7 Incident Response Hotline  
+1-(855)-684-1212  
or cirt@nccgroup.com




© NCC Group 2024. All rights reserved.

## This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#) 

---

### Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

---

### Analytical Cookies

Off

Analytical cookies help us to improve our website by collecting and reporting information on its usage.