nccgroup

Cyber Security ▸ Research Blog

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 modifie
- The Hunt
- Use of DI n the past.

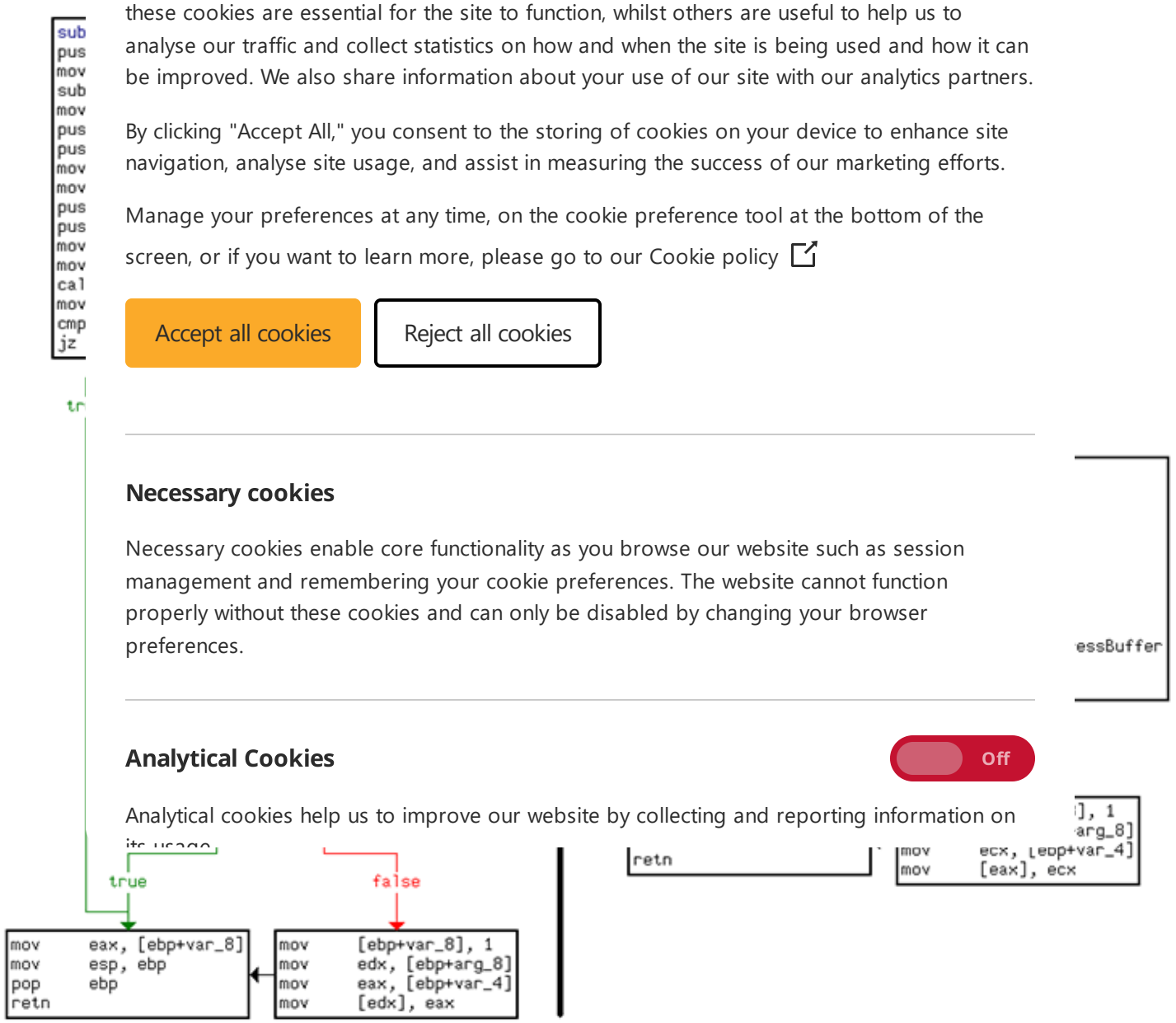

Figure 1: Old sample on the left side, our sample on the right side

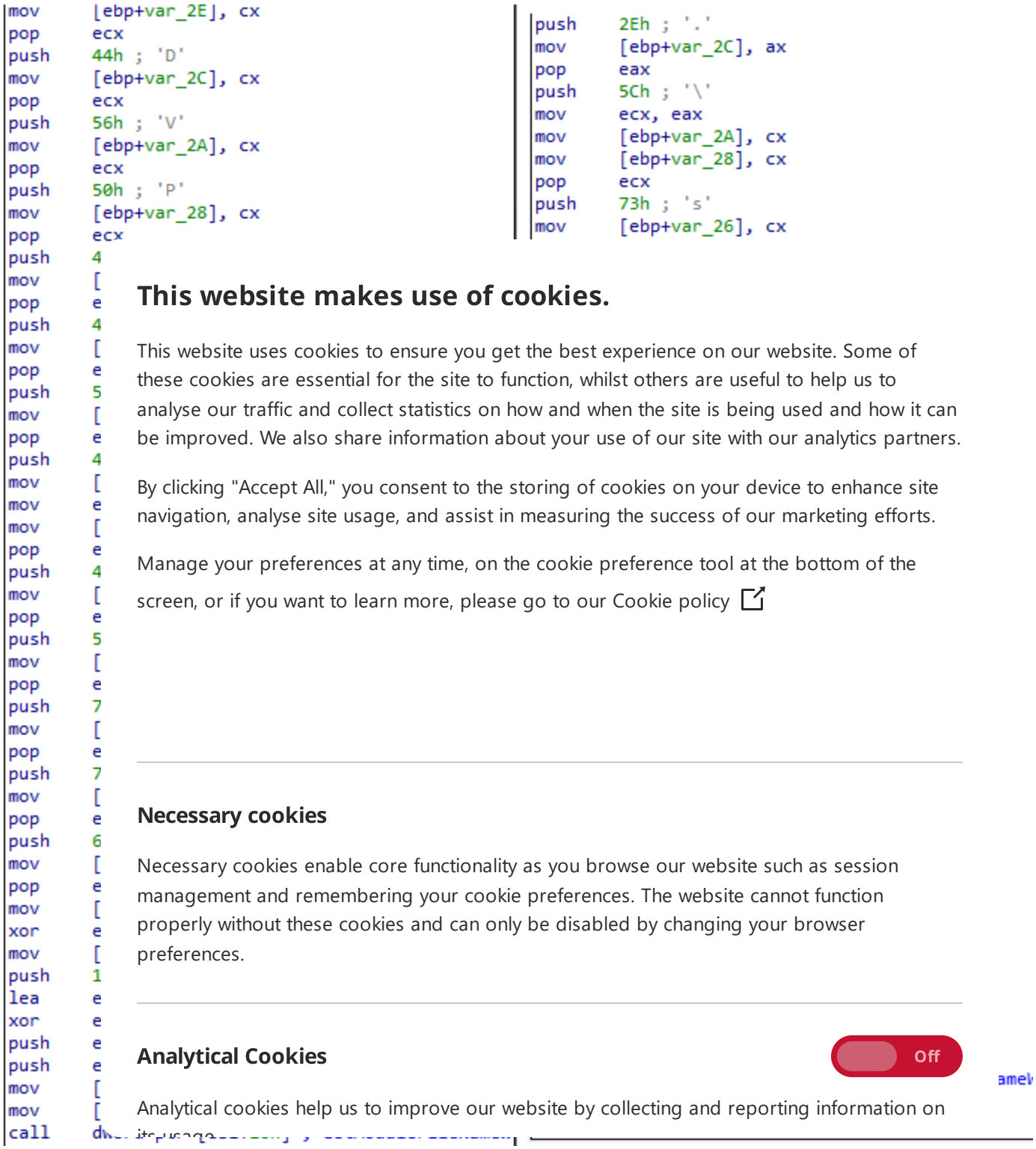

Figure 2: Old sample on the left side, our sample on the right side

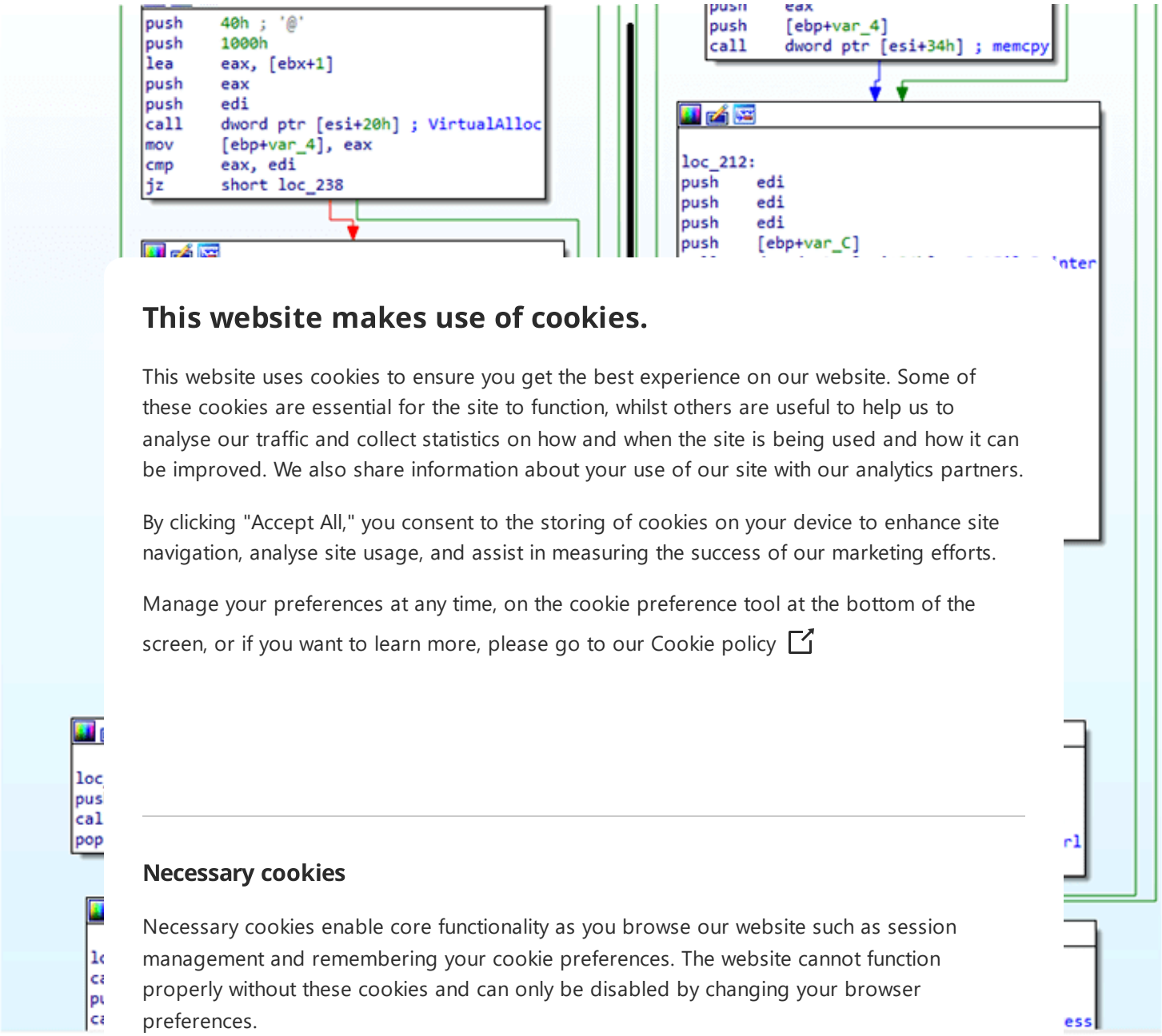

Figure 3:

Tech

Based 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).

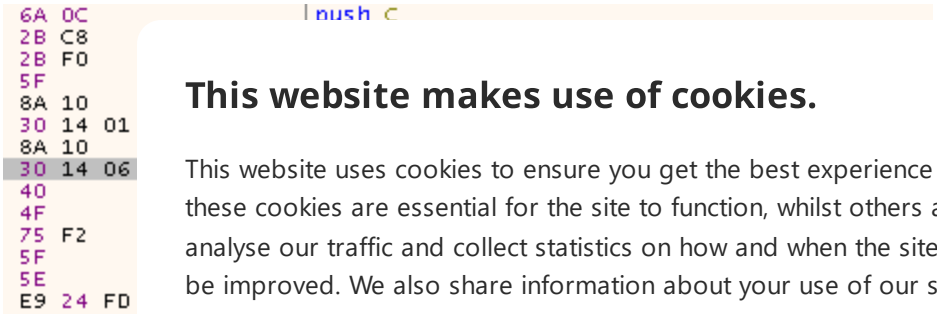

Figure 4:

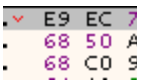

Figure 5:

After jum nd find
the addr
dynamic

Lastly, it , it will
XOR decr uffer.

Payl

We will fc nces
between ting
strings w s one of
the reasc

```
L"Setconfig"
L"[test]::Soldier %s"
L"getip"
L"[test]::Soldier %s"
L"OnlineHelp"
L"While In"
L"[test]::Soldier %s"
"8.8.8.8"
L"Console"
L"DllMain"
L"[test]::Soldier %s"
L"To Pass UAC"
L"[test]::Soldier %s"
L"Work"
L"[test]::
L"Install
L"[test]:
L"SystemS
L"[test]:
L"Double
L"[test]:
```

Figure 6:

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

Figure 7:

The actio … the following …

No. of p		
		ad to it

Optio

When the binary is executed for the first time:

- 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

Optio

The meth ıing from
a user wi rom the
config, in the
service. T neter.

Otherwis on\Run
key with all, then
it will inje

Optio

This is de

Optio

An alread ethod
will work in
developn

Core f

Currentl
commun ploading
or downl

Config

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. We want to ... the identifications of the registry k... can be found in ...

Key na...	...nple two
Bin	
Conso	
Dll	...dll
Group	
GUID	
MD5	...9mxxxx
Online	...43
Path	...\systemc

	Associated Files		
PE	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			

Diffe

As menti… between …

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

Function		
Persister		
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: gistry

Previous

https://w
cyberesp

https://w

IOCs

C C IP
103.59
159.65

Regist	
HjDWr	
Z68A-D	
C:Prog	
systen	

Systemconfig	Check for this service with description: “for systemconfig”

File Name	SHA-256
INISafeWebSSO.exe	C501203FF3335FBFC258B2729A72E82638719F60F7E6361FC1CA3C85603
inicore_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