Now You See Me – H-worm by Houdini

Blog

Now You See Me – H-worm by Houdini

September 24, 2013 | by Thousque Haq and Ned Moran | Threat Intelligence

H-worm is a VBS (Visual Basic Script) based RAT written by an individual going by the name Houdini. We believe the author is based in Algeria and has connections to njO, the author of njw0rm [1] and njRAT/LV [2] through means of a shared or common code base. We have seen the H-worm RAT being employed in targeted attacks against the international energy industry; however, we also see it being employed in a wider context as run of the mill attacks through spammed email attachments and malicious links.

The Payload

The H-worm payload is simply a VBS file, which is often wrapped in a PE executable dropper. The H-worm VBS file is also packed with multiple layers of obfuscation in some cases. While analyzing such samples (81c1f3256e5d91614689f5f7d70136c and 4543daa69836d544da8782b3d95c4f1), we discovered that they were obfuscated with custom [Base64 encoding, multiple levels of standard [Base64 encoring [Safe Crypter], and character substitutions. The obfuscation techniques used have been described here [3] already and are summarized in Figure 1 below. There is also an Autoit version of H-worm called the “underworld version” floating around which has the same functionality as the VBS version.

http://www.fireeye.com/blog/technical/threat-intelligence/2013/09/now-you-see-me-h-wor...  5/28/2014
**Dissecting Command and Control (CnC) Behavior**

Upon successful compromise, the worm generates network telemetry (beacon), as shown below:

**POST ls-ready HTTP/1.1**

Accept: */*
Accept-Language: en-us
User-Agent: (DiskVolumeSerial)>(Hostname)>({Username})>({OS})>({platform})>({AVProductInstalled or n/a}-{})
(USBSpread: true or false) -- (CurrentSystemDate)

http://www.fireeye.com/blog/technical/threat-intelligence/2013/09/now-you-see-me-h-wor... 5/28/2014
As seen in the beacon, it sends out various pieces of sensitive identification information in the User-Agent field. We have also observed versions where the URI was modified to use other strings such as "POST /AM_WEB/READY". The keyword "<param1>="" is constant in the beacon but we have seen versions where this was modified as well. We saw instances where "<param2>="" was used instead. It expects a response of the form:

(command)<--(param1)<--(param2)

The worm supports the following remote commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Communication Request generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>execute</td>
<td>Executes param value using 'execute'</td>
<td>-</td>
</tr>
<tr>
<td>update</td>
<td>Replaces the payload and restarts with the wscript engine</td>
<td>-</td>
</tr>
<tr>
<td>uninstall</td>
<td>Deletes startup entries and payload</td>
<td>-</td>
</tr>
<tr>
<td>send</td>
<td>Downloads file from CnC server</td>
<td>POST (command)&lt;--(param1)&lt;--(param2)</td>
</tr>
<tr>
<td>site-send</td>
<td>Downloads file from URL</td>
<td>GET (command)&lt;--(param1)&lt;--(param2)</td>
</tr>
<tr>
<td>recv</td>
<td>Uploads file to CnC server</td>
<td>POST (command)&lt;--(param1)&lt;--(param2)</td>
</tr>
<tr>
<td>enum-driver</td>
<td>Sends all drive information to the CnC</td>
<td>POST (command)&lt;--(param1)&lt;--(param2)</td>
</tr>
<tr>
<td>enum-taf</td>
<td>Sends all file and folder attributes in a specified directory</td>
<td>POST (command)&lt;--(param1)&lt;--(param2)</td>
</tr>
<tr>
<td>enum-process</td>
<td>Sends all running processes</td>
<td>POST (command)&lt;--(param1)&lt;--(param2)</td>
</tr>
<tr>
<td>cmd-shell</td>
<td>Executes param value with 'cmd.exe /c ' and returns result</td>
<td>POST (command)&lt;--(param1)&lt;--(param2)</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes file or folder specified in param</td>
<td>-</td>
</tr>
<tr>
<td>exit-process</td>
<td>Kills process specified in param</td>
<td>-</td>
</tr>
<tr>
<td>sleep</td>
<td>Sleep call in param is passed to eval()</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 1 – Remote commands available in H-worm

**Behind The Curtains**

The control panel for H-worm has a builder and a controller interface to interact with the infected machine. The control panel is written in Delphi. Some of the features such as password grabber and USB spreading were not functional in the versions we analyzed. These features could be operational in newer versions of H-worm.

http://www.fireeye.com/blog/technical/threat-intelligence/2013/09/now-you-see-me-h-wor... 5/28/2014
Now You See Me – H-worm by Houdini | FireEye Blog

Figure 2 – Control panel of H-worm

The author, Houdini, has a portal to show off his wares, which hosts a demonstration video of H-worm. The contents of the portal indicate that he is proficient in both French and Arabic. Based on this and various other identifiable clues in the video, it is likely that the author of H-worm is from Algeria. We also believe the thumbnail images briefly seen in the video may be of the author himself. For the keen eyed observers, it is also evident that the author likes to play “Beetle Bug 2” and “Chicken invaders 4.”

Figure 3 – Snippets from Houdini’s demo of H-worm

CnC Intel Analysis

http://www.fireeye.com/blog/technical/threat-intelligence/2013/09/now-you-see-me-h-wor... 5/28/2014
Now You See Me – H-worm by Houdini | FireEye Blog

On further analysis of the command and control infrastructure, we discovered that the CnC infrastructure used by some of the H-worm variants were shared by others RATs such as NJ0rm, njRAT/LV, XtremeRAT, and Poisonivy. The attackers behind these instances appear to have an arsenal of RATs at their disposal, in order to perform various attack campaigns.

<table>
<thead>
<tr>
<th>CnC Domain</th>
<th>Other associated RATs</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:silent@zapto.org">silent@zapto.org</a></td>
<td>Nj0rm</td>
</tr>
<tr>
<td>adolf2013.sysnet.net</td>
<td>XtremeRAT</td>
</tr>
<tr>
<td>balligogo.no-ip.biz</td>
<td>XtremeRAT</td>
</tr>
<tr>
<td>pass-12.zapto.org</td>
<td>DarkComet</td>
</tr>
<tr>
<td>sidisilms.myvnc.com</td>
<td>LV</td>
</tr>
<tr>
<td>xkiller.no-ip.info</td>
<td>LV</td>
</tr>
<tr>
<td>karimstar.zapto.org</td>
<td>LV</td>
</tr>
<tr>
<td>securityfocus.bounceme.net</td>
<td>LV</td>
</tr>
<tr>
<td>kiyoma260.no-ip.biz</td>
<td>LV</td>
</tr>
<tr>
<td></td>
<td>Poisonivy</td>
</tr>
</tbody>
</table>

Table 2 – Direct over-laps on command and control infrastructure

Possible Connections to the nj08 Enterprise

We recently talked about nj0rm [1] and the author behind it, nj08. We found strong connections indicating that nj0rm and njRAT/LV [2] were written by the same author. We believe H-worm is also linked to nj08, through a shared code base. An earlier version of H-worm was analyzed here [4], by another researcher. It is evident from this older version, that the client side module was originally coded by nj08. The older version beacons with “POST/ready” instead of “POST is-ready”, as seen in the newer versions. This blog was re-tweeted on the nj08 twitter page. Our earlier nj0rm blog was also promptly re-tweeted on the nj08 twitter page. It is unclear how connected Houdini and nj08 are, but it is likely that nj08 is a group of individuals collaborating on the development of RATs, or alternatively, there are development forks on the same code base by multiple authors.

Figure 4 – Common code base and nj08 connections

H-worm Hashes

00df326eeb1f8f7eae2b8dd36f84ac1546
1483dc5c5c687b4a05f22b23116f1024
4543d3ea929d3de54d8c87286290f9d5a1f
80b169041b217313c14e6f0de683d6c275d
9f3633b345a227727a073648b69db4ef72d
9e273220e71f490ee99b023bcf1ae3

http://www.fireeye.com/blog/technical/threat-intelligence/2013/09/now-you-see-me-h-wor... 5/28/2014
H-worm Command and Control (CnC) Infrastructure

adamalem.zapto.org:1973
adolf2013.zapto.net:1183
adolf2013.systes.net:1184
ahmad212.no-ip.biz:86
all007.zapto.org:288
all007.zapto.org:6611
am1.no-ip.info:1888
ballgogo.no-ip.biz:8088
basss.no-ip.info:2026
basss.no-ip.info:82
bg1337.zapto.org:1155
bg05151.zapto.org:991
dataday3.no-ip.org:83
dodeur13.no-ip.org:444
doba.redirectme.net:777
dzha1003.no-ip.org:82
g00gle.systes.net:4448
gerssy.zapto.org:6000
googledrury.zapto.org:15990
hackedienq.no-ip.biz:85
hackerbabara.nip-biz:8888
hattrouni2.no-ip.biz:88
hmode123.no-ip.biz:9609
karimstar.zapto.org:85
kiyoma200.no-ip.biz:1117
koko.myftp.org:9990
ldea.no-ip.org:88
medallion.no-ip.biz:1247
microsoftsystem.systes.net:4442
moo011.no-ip.org:81
msgboz.zapto.org:5246
new-hostnet.no-ip.org:91
nijn.redirectme.net:123
no99.zapto.org:81
nocoot.no-ip.biz:443
pessa-123.zapto.org:1604
pessa-12.zapto.org:81
portipav.redirectme.net:1991
ronaldo-123.no-ip.biz:2011
ronaldo-123.no-ip.biz:2013
sawztt.no-ip.biz:333
securityfoous.bouicicme.net:1166
shagapyy1.no-ip.biz:1605
sidisalim.myync.com:1888
silentit.zapto.org:7995
terminater1.zapto.org:1991
vpn-hacker.no-ip.biz:9000
xbox720.zapto.org:1991
xkiller.no-ip.info:1
yathir17.no-ip.org:1177
zeusback.no-ip.org:223
zoa.no-ip.org:448

References:

http://www.fireeye.com/blog/technical/threat-intelligence/2013/09/now-you-see-me-h-wor...