« Ten Impossible Things You Can Do with Metadata, Part 2 | Main | Vawtrak DGA Round 2 »

Wednesday, November 09, 2016

Commodity Remote Access Trojans (RATs) -- which are designed, productized and sold to the casual and experienced hacker alike -- put powerful remote access capabilities into the hands of criminals. RATs, such as H-W0rm, njRAT, KilerRAT, DarkComet, Netwire, XtremeRAT, JSocket/AlienSpy/Adwind and others, hold special interest for the Threat Research Team at Fidelis Cybersecurity. We're constantly following, detecting and monitoring the lifecycle of these RATs as they appear, disappear and often reappear under a new moniker.

There have been recent reports [1], [2] about a new version of one such commodity RAT, H-W0rm (Hworm), and the various campaigns it is being used in. Our telemetry shows that H-W0rm is one of the most active RATs we've seen, with infections observed across virtually all enterprise verticals and geographies in which Fidelis Cybersecurity products are deployed.

In this blog post, the Threat Research Team at Fidelis Cybersecurity is supplementing these recent reports by providing the security community with the following:

- Technical descriptions of the payload behavior when installed on the victim machine.
- Domains observed in active infections over the past six months. We also make a larger mined dataset available through Fidelis Barncat, a malware configuration intelligence database shared at no cost with trusted third parties.
- Artifacts correlating Hworm C2 domains with njRAT, XtremeRAT and DarkComet.
- Yara rules that can be used to detect the VBS and PE versions of H-W0rm.

The following is a screenshot of the Hworm v.1.3 panel and the builder tab:

Hworm 1.3 builder panel

Hworm 1.3 server builder window

A Worm That's Really a RAT

It is worth clarifying that even though the malware is known as H-W0rm/Hworm, this version is not a typical worm. Specifically, it features classic Remote Access Trojan capabilities that allow the adversary to fully control the infected system. Here is rundown of some of these capabilities:

- Collect system information: hardware ID, client name/campaign code, computer name, operating system, worm/RAT version, information about AV installed, webcam presence, etc.
- File Manager: download, rename, delete, execute
- Remote Desktop capture/screenshot
- Keylogger
- Collect password filled in forms from web browsers, such as Mozilla Firefox, Google Chrome, and Opera
- Webcam
- Microphone
- Run remote application or script from disk or internet, or load it in memory via RunPE
- Update RAT from disk or internet
- Close connection
- Uninstall RAT

Let's Go to the Videotape

A YouTube video shows an Hworm version that is referred to as version 2. The following is a screenshot from one of the windows presented in the video:

The Exploit panel, under the Builder tab, looks interesting. At the moment, it is unclear how this feature works, but its mere presence suggests the potential for creating and integrating future exploits into the malware. The following is a screenshot of the panel:

Our analysis found that one of the samples saved keystroke data into the %TEMP% directory using the filename [*malware_name*.**dat**]. In this instance, the malware was configured from the builder to be installed in the %TEMP% directory, but based on the builder settings, it can be installed in the following directories:

- %APPDATA%

Search

Archives

November 2016
October 2016
August 2016
July 2016
June 2016
May 2016
March 2016
February 2016
January 2016
December 2015

Blogroll

Dark Reading
Didier Stevens
Krebs on Security
Malware Tracker
Naked Security
Schneier on Security
Tech Dirt
The Forrester Blog
Threat Level
Threat Post

- %USERPROFILE%
- %PROGRAMDATA% (Windows 7)
- %TEMP%

The malware also created the following hidden folder in the attached USB drive: $RECYCLE.BIN.

The Link to Houdini

There has been speculation in the research community[3], [4], [5] that "Houdini" (aka 'Mohamed Benabdellah') is believed to have connection with "njq8" (aka 'Naser Al Mutairi'), the initial developer of "njRAT" and "njw0rm". It has further been speculated that "Houdini" is based in Algeria and "njq8" in Kuwait. It is also said that "njq8" has a connection with "Black Mafia" on the development on "Black Worm", indicating potential collaboration between these RAT developers.

AV Information in the Network Traffic

The network traffic of some versions of the Hworm malware contain information about the antivirus tool installed in the victim system. This data indicates that some of the infected systems appeared to have been running antivirus tools like:

- Microsoft Security Essentials
- Symantec Endpoint Protection
- McAfee VirusScan Enterprise
- ESET Smart Security
- Windows Defender

Normally, those tools will detected the malware, but for some unknown reason it looks like the AV tools didn't remove those versions of the Hworm malware running in memory. Without a copy of the specific Hworm version in the victim system and a Forensics investigation, it is difficult to confirm why those AV tools didn't remove the sample from those victim system.

Protect Yourself

These findings are another validation of how a layered approach to secure the network enterprise is needed to protect your endpoints from these cyber threats.

In order to aid the security community with indicators of the Hworm RAT, the following is a list of C2 domains we have seen in the past six months:

1cowsound.mooo[dot]com	hbooob.no-ip[dot]biz	p-dark.zapto[dot]org
3bod-x.no-ip[dot]biz	hell222.no-ip[dot]biz	pilo-raouf.no-ip[dot]biz
43r0m4x.publicvm[dot]com	herohero.no-ip[dot]org	qalsdahxjnm.no-ip[dot]biz
9amoo.zapto[dot]org	hussamhack.no-ip[dot]biz	qwwq.no-ip[dot]biz
a.servecounterstrike[dot]com	ines0049.ddns[dot]net	qwwq.servehttp[dot]com
aaaazzzz9999000.no-ip[dot]biz	j2w2d.no-ip[dot]biz	righi.linkpc[dot]net
aabod8.no-ip[dot]biz	jeflex.no-ip[dot]org	ronaldo-123.no-ip[dot]biz
adolf2013.sytes[dot]net	jn.redirectme[dot]net	sara-tabuk.no-ip[dot]biz
ah99.no-ip[dot]info	justprogamers.ddns[dot]net	servecounterstrike.servecounterstr
ahmad212.no-ip[dot]biz	khdt1.zapto[dot]org	smoker21.hopto[dot]org
aktam04.no-ip[dot]info	king0780.no-ip[dot]biz	strangler89.no-ip[dot]org
ali252612.zapto[dot]org	king999.ddns[dot]net	support.microsoft.linkpc[dot]net
amran-pc.no-ip[dot]biz	kingofus.myq-see[dot]com	swanox.no-ip[dot]org
anarqe77.no-ip[dot]biz	klonkino.no-ip[dot]org	syses.sytes[dot]net
anonymous-0.no-ip[dot]biz	kohen.no-ip[dot]org	systim.publicvm[dot]com
asdfghj123.ddns[dot]net	ksa2013.no-ip[dot]biz	universal2010.no-ip[dot]org

azo8oz.no-ip[dot]biz	mastlg.no-ip[dot]biz	updlate.serveminecraft[dot]net
bifrost-jordan.zapto[dot]org	max-ps.sytes[dot]net	vipvip3.dyndns[dot]org
cyberspy.zapto[dot]org	maxy.no-ip[dot]info	vipx.zapto[dot]org
dmar123.no-ip[dot]biz	mi0.bounceme[dot]net	wormaa.zapto[dot]org
doda.redirectme[dot]net	microsoft8.publicvm[dot]com	wvvw.sytes[dot]net
douda.linkpc[dot]net	microsoftntdll.sytes[dot]net	x.dvr-ddns[dot]com
douda.no-ip[dot]info	microsoftsystem.sytes[dot]net	xdz.no-ip[dot]org
dz47.linkpc[dot]net	mohamedmmk.zapto[dot]org	xxtataxx.no-ip[dot]biz
elaspany.ddns[dot]net	mouradel.no-ip[dot]org	yahia17.no-ip[dot]org
epohme.no-ip[dot]org	nemlacom.no-ip[dot]iz	
fecabook.redirectme[dot]net	njrat2012.no-ip[dot]biz	
g00gle.sytes[dot]net	noooot.no-ip[dot]biz	
googlechrome.servequake[dot]com	ody.no-ip[dot]biz	
hacker0021.no-ip[dot]biz	org.publicvm[dot]com	

From the above domains, the following one quickly stands out: "**njrat**2012.no-ip[dot]biz". The last Hworm activity observed at a client site with this domain was on Oct 2016. pDNS data shows that in June 2016 this domain was associated with Xtreme RAT activity. We also found samples of njRAT v.0.7d and v.0.4.1a beaconing to this domain. The following table shows some of the C2 correlations:

Malware	**MD5**	**C2**
XtremeRAT	6b3ef140a6062d7fa295c8fedde7d689	njrat2012.no-ip[dot]biz:22
njRAT v.0.7d	0de41aef336f40a07ed6984db61b52ab	njrat2012.no-ip[dot]biz:2020
njRAT v.0.4.1a	e081a42d6e09a3fcf049a33b2ecf0412	njrat2012.no-ip[dot]biz:1177
DarkComet	06e125132b458321f97b6409a4db9ac4	vipvip3.dyndns[dot]org:1604
njRAT	361c9d44809f788b92023b762e363449	vipvip3.dyndns[dot]org:8817

To aid the security community, we're constantly enriching Fidelis Barncat with newer Hworm configurations using our mining techniques.

The following Yara rules can also be used to detect this threat:

```
rule win_vbs_rat_hworm
{
   strings:
            $sa1 = "CONFIG"
      $sa2 = "MYCODE"
      $sa3 = "SHELLOBJ.EXPANDENVIRONMENTSTRINGS"
      $sa4 = "BASE64TOHEX"
      $sa5 = "DCOM.VIRTUALALLOC"
      $sa6 = "LOADER_"
      $sa7 = "PE_PTR"
```

```
        $sa8 = "OBJWMISERVICE.EXECQUERY"
        $sa9 = "WSCRIPT.EXE" nocase
        $sa10 = "FUNCTION"
        $sa11 = "DIM"
        $sa12 = "END SUB"
                $sb1 = "HOST_FILE"
        $sb2 = "FILE_NAME"
        $sb3 = "INSTALL_DIR"
        $sb4 = "START_UP_REG"
        $sb5 = "START_UP_TASK"
        $sb6 = "START_UP_FOLDER"
        $sc1 = "DCOM_DATA"
        $sc2 = "LOADER_DATA"
        $sc3 = "FILE_DATA"
        $sc4 = "(1)"
        $sc5 = "(2)"
        $sc6 = "(3)"
        $sc7 = "FILE_SIZE"
    condition:
                (all of ($sa*)) and ( (all of ($sb*)) or (all of ($sc*)) )
}
rule win_exe_rat_hworm
{
    strings:
                $sa1 = "connection_host" wide ascii
                $sa2 = "connection_port" wide ascii
                $sa3 = "install_folder" wide ascii
                $sa4 = "install_name" wide ascii
                $sa5 = "nickname_id" wide ascii
                $sa6 = "password" wide ascii
                $sa7 = "injection" wide ascii
                $sa8 = "startup_registry" wide ascii
                $sa9 = "startup_folder" wide ascii
                $sa10 = "startup_task" wide ascii
                $sa11 = "process_name" wide ascii
                $sa12 = "fkeylogger_host" wide ascii
                $sa13 = "fkeylogger_port" wide ascii
                $sa14 = "keylogger_init" wide ascii
                $sa15 = "keylogger_offline" wide ascii
                $sa16 = "file_manager" wide ascii
                $sa17 = "usb" wide ascii
                $sa18 = "password" wide ascii
                $sa19 = "filemanager" wide ascii
                $sa20 = "keylogger" wide ascii
                $sa21 = "screenshot" wide ascii
                $sa22 = "show" nocase wide ascii
                $sa23 = "open" wide ascii
                $sa25 = "create" wide ascii
                $sa26 = "Self" wide ascii
                $sa27 = "createsuspended" wide ascii
    condition:
```

```
                (uint16(0) == 0x5A4D) and (all of them)

}
```

Posted by ThreatGeek at 08:47 AM | Permalink

Tweet Like 19