Altro

contagio

malware dump

Home

Mobile and print friendly view |

MONDAY, JUNE 13, 2011

Jun 1 CVE-2010-3333 DOC You are my King from compromised louisvilleheartsurgery.com w Trojan Taidoor

Common Vulnerabilities and Exposures (CVE) number

CVE-2010-3333 Stack-based buffer overflow in Microsoft Office XP SP3, Office 2003 SP3, Office 2007 SP2, Office 2010, Office 2004 and 2008 for Mac, Office for Mac 2011, and Open XML File Format Converter for Mac allows remote attackers to execute arbitrary code via crafted RTF data, aka "RTF Stack Buffer Overflow Vulnerability

General File Information

File You are my king.doc
File Size 58531 bytes
MD5 09D68EF693AC6B7D3ACF0DDFF0585543
Distribution Email attachment

CLICK HERE SEE ALL OTHERS 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.(I have other examples of phish mail sent via that server and I will post them as soon as I can)

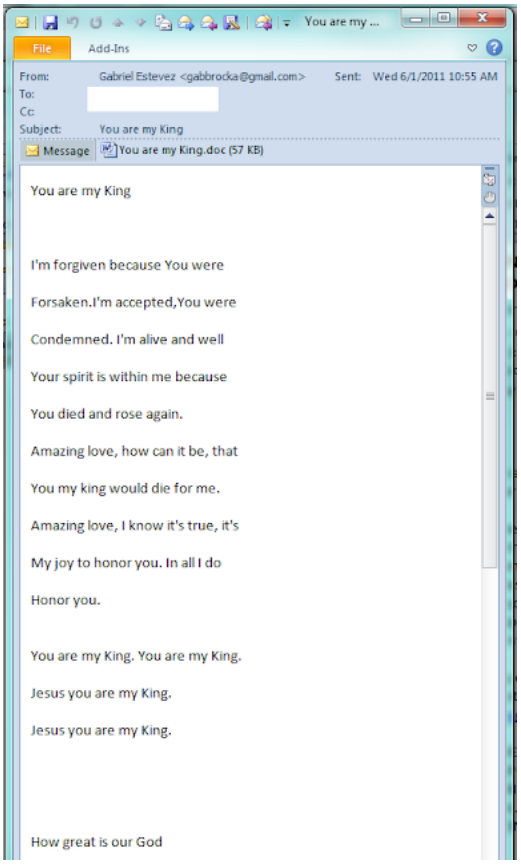
Download

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: Gabriel Estevez [mailto:gabbrocka@gmail.com]
Sent: Wednesday, June 01, 2011 10:55 AM
To: xxxxxxxxxxx
Subject: You are my King

You are my King
I'm forgiven because You were
Forsaken.I'm accepted,You were
Condemned. I'm alive and well
Your spirit is within me because
You died and rose again.
Amazing love, how can it be, that



You my king would die for me.
Amazing love, I know it's true, it's
My joy to honor you. In all I do
Honor you.
You are my King. You are my King.
Jesus you are my King.
Jesus you are my King.

How great is our God
The splender of the King clothed in
Majesty, let all the earth rejoice.
All the earth rejoice.He wraps
Himself in light and darkness tries
To hide and trembles at His voice.
And trembles at His voice.
How great is our God.Sing with
Me,how great is our God.And all
Will seehow great, how great is
Our God.
And age to age He stands, and
Time is in His hands,beginning
And the end.Begining and the
End.The Godhead three in one
Father Spirit Son, the lion and
The Lamb, the Lion and the Lamb.
Name above all names, worthy of
All praise.My heart will sing, how
Great is our God.

Message Headers

```
Received: (qmail 23009 invoked from network); 1 Jun 2011 14:55:10 -0000
Received: from mail.louisvilleheartsurgery.com (HELO ucsamd.com) (66.147.51.202)
  by xxxxxxxxxxxx
Received: from UCSADC1 ([192.168.20.2]) by ucsamd.com with Microsoft SMTPSVC(6.0.3790.4675);
     Wed, 1 Jun 2011 10:55:09 -0400
Subject: You are my King
Date: Wed, 1 Jun 2011 10:55:09 -0400
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="----=_NextPart_000_0009_01CC2047.803733D0"
X-Priority: 3
X-MSMail-Priority: Normal
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.4721
From: "Gabriel Estevez"
To: xxxxxxxx
X-Mailer: Microsoft Outlook, Build 10.0.2627
Return-Path: gabbrocka@gmail.com
Message-ID:
X-OriginalArrivalTime: 01 Jun 2011 14:55:09.0496 (UTC) FILETIME=[E6EFB380:01CC206B]
```

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: You are my King.doc
Submission date: 2011-06-03 17:20:34 (UTC)
Result: 15 /42 (35.7%)
http://www.virustotal.com/file-scan/report.html?id=41aac004dcadbdb87eac1df7f82d2fb70eb65a43c8bc6a65129c7bffed859c32-1307121634
Compact Print results Antivirus Version Last Update Result
AhnLab-V3 2011.06.03.01 2011.06.03 Dropper/Cve-2010-3333
AntiVir 7.11.9.3 2011.06.03 EXP/CVE-2010-3333
Antiy-AVL 2.0.3.7 2011.06.03 Exploit/MSWord.CVE-2010-3333
ClamAV 0.97.0.0 2011.06.03 PUA.RFT.EmbeddedOLE
Commtouch 5.3.2.6 2011.06.03 CVE-2010-3333!Camelot
DrWeb 5.0.2.03300 2011.06.03 Exploit.Rtf.based
Fortinet 4.2.257.0 2011.06.03 Data/CVE20103333.A!exploit
Ikarus T3.1.1.104.0 2011.06.03 Exploit.Win32.CVE-2010
Kaspersky 9.0.0.837 2011.06.03 Exploit.MSWord.CVE-2010-3333.p
Microsoft 1.6903 2011.06.03 Exploit:Win32/CVE-2010-3333
PCTools 7.0.3.5 2011.06.03 HeurEngine.MaliciousExploit
SUPERAntiSpyware 4.40.0.1006 2011.06.03 -
Symantec 20111.1.0.186 2011.06.03 Bloodhound.Exploit.366
TrendMicro 9.200.0.1012 2011.06.03 Possible_ARTIEF
TrendMicro-HouseCall 9.200.0.1012 2011.06.03 Possible_ARTIEF
VIPRE 9473 2011.06.03 Exploit.MSWord.CVE-2010-3333.c (v)
Additional informationShow all
MD5 : 09d68ef693ac6b7d3acf0ddff0585543

Created files

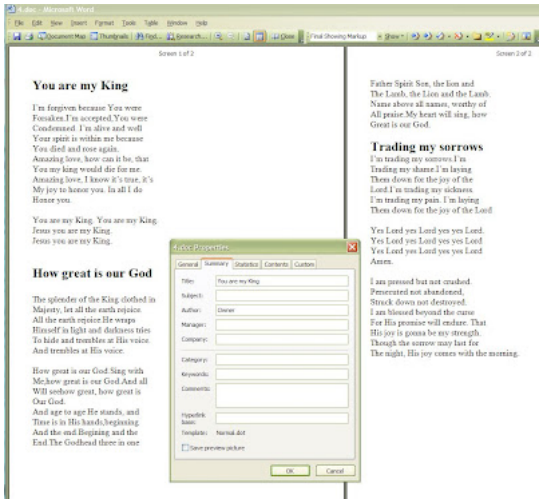
This trojan is characterized by the traffic it generates -

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\Temp\4.doc
Local Settings\UPS.exe 5EA58C5F12405A4E959234134123380D

(same file as %Temp%\~Svchost.exe 5EA58C5F12405A4E959234134123380D from May 31 CVE-2010-3333 DOC Q and A.doc compromised louisvilleheartsurgery.com w Trojan Taidoor)
created and deleted
Local Settings\Temp\\~dfds3.reg

4.doc - decoy clean file



~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]
"VSS"="C:\\Documents and Settings\\mila\\Local Settings\\VSS.exe"

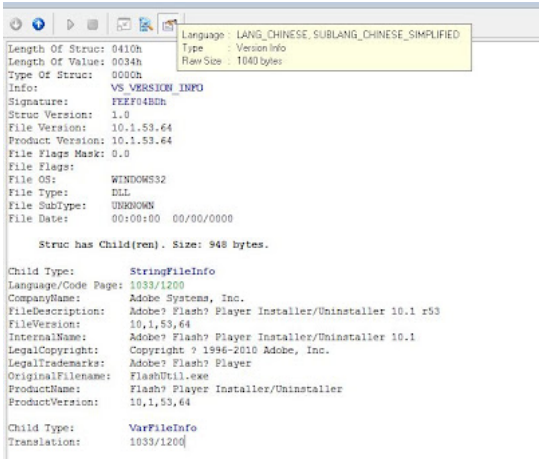
VSS.exe 5EA58C5F12405A4E9592341341233 80D

VSS.exe

Submission date: 2011-06-13 21:48:47 (UTC)
Result: 22/ 42 (52.4%)
http://www.virustotal.com/file-scan/report.html?id=bb40b1e17e37e0fba0f40d42d2064e97d32cb20f1fc3ea49f33781c570182196-1308001727
AhnLab-V3 2011.06.14.00 2011.06.13 Win-Trojan/Injector.17925.E
AntiVir 7.11.9.167 2011.06.13 TR/Crypt.ZPACK.Gen
Avast 4.8.1351.0 2011.06.13 Win32:Malware-gen
Avast5 5.0.677.0 2011.06.13 Win32:Malware-gen
AVG 10.0.0.1190 2011.06.13 Generic22.BYWE
BitDefender 7.2 2011.06.13 Trojan.CryptRedol.Gen.3
DrWeb 5.0.2.03300 2011.06.13 Trojan.Taidoor
F-Secure 9.0.16440.0 2011.06.13 Trojan.CryptRedol.Gen.3
Fortinet 4.2.257.0 2011.06.13 W32/Sasfis.BKXQ!tr
GData 22 2011.06.13 Trojan.CryptRedol.Gen.3
Ikarus T3.1.1.104.0 2011.06.13 Trojan.SuspectCRC
Kaspersky 9.0.0.837 2011.06.13 Trojan.Win32.Sasfis.bkxq
Microsoft 1.6903 2011.06.13 VirTool:Win32/Injector.gen!BJ
NOD32 6204 2011.06.13 Win32/TrojanDownloader.Agent.PTT
Norman 6.07.10 2011.06.13 W32/Malware.TJAQ
nProtect 2011-06-13.02 2011.06.13 Trojan.CryptRedol.Gen.3
Panda 10.0.3.5 2011.06.13 Trj/CI.A
PCTools 7.0.3.5 2011.06.10 Trojan.Gen
Rising 23.62.00.03 2011.06.13 Suspicious
Sophos 4.66.0 2011.06.13 Troj/Mdrop-DMI
Symantec 20111.1.0.186 2011.06.13 Suspicious.Cloud.5
VBA32 3.12.16.1 2011.06.13 TrojanDownloader.Rubinurd.f
MD5 : 5ea58c5f12405a4e959234134123380d
Strings excerpt

V/_z
>d/R(
ntdll.dll
NtUnmapViewOfSection
%s "%s"
exe.secivres
abcde

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

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 /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

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 /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 **http://www.threatexpert.com/report.aspx?md5=5ea58c5f12405a4e959234134123380d**
File System Modifications
The following file was created in the system:

#	Filename(s)	File Size	File Hash
1	[file and pathname of the sample #1]	17,925 bytes	MD5: 0x5EA58C5F12405A4E959234134123380D SHA-1: 0xB5C466CB36FEA327DA8B3DAF13E3CAE5EBB05DF6

China

- The data identified by the following URLs was then requested from the remote web server:
  - http://99.1.23.71:443/iiohf.php?id=029590121212121212
  - http://65.87.199.102:443/iiohf.php?id=024326121212121212
  - http://99.1.23.71:443/figuq.php?id=025431121212121212
  - http://65.87.199.102:443/figuq.php?id=017975121212121212
  - http://99.1.23.71:443/heisp.php?id=014218121212121212
  - http://65.87.199.102:443/heisp.php?id=013836121212121212
  - http://99.1.23.71:443/qtcbv.php?id=022665121212121212

- http://65.87.199.102:443/qtcbv.php?id=003529121212121212
- http://99.1.23.71:443/hlobe.php?id=004518121212121212
- http://65.87.199.102:443/hlobe.php?id=009835121212121212
- http://99.1.23.71:443/epzkq.php?id=018399121212121212
- http://65.87.199.102:443/epzkq.php?id=012316121212121212
- http://99.1.23.71:443/tlhdt.php?id=015598121212121212
- http://65.87.199.102:443/tlhdt.php?id=026804121212121212
- http://99.1.23.71:443/vyqld.php?id=024007121212121212
- http://65.87.199.102:443/vyqld.php?id=008414121212121212
- http://99.1.23.71:443/ttlvm.php?id=013126121212121212
- http://65.87.199.102:443/ttlvm.php?id=022955121212121212
- http://99.1.23.71:443/vocpb.php?id=011307121212121212
- http://65.87.199.102:443/vocpb.php?id=006291121212121212
- http://99.1.23.71:443/ixoga.php?id=008375121212121212
- http://65.87.199.102:443/ixoga.php?id=019758121212121212
- http://99.1.23.71:443/mrhfu.php?id=029330121212121212
- http://65.87.199.102:443/mrhfu.php?id=010690121212121212
- http://99.1.23.71:443/uklxd.php?id=002815121212121212
- http://65.87.199.102:443/uklxd.php?id=008982121212121212
- http://99.1.23.71:443/mwmco.php?id=031260121212121212
- http://65.87.199.102:443/mwmco.php?id=028267121212121212
- http://99.1.23.71:443/mnopi.php?id=028612121212121212
- http://65.87.199.102:443/mnopi.php?id=023566121212121212
- http://99.1.23.71:443/janim.php?id=006088121212121212
- http://65.87.199.102:443/janim.php?id=030408121212121212
- http://99.1.23.71:443/vkreb.php?id=017322121212121212
- http://65.87.199.102:443/vkreb.php?id=020437121212121212
- http://99.1.23.71:443/ashlg.php?id=002182121212121212
- http://65.87.199.102:443/ashlg.php?id=016018121212121212
- http://99.1.23.71:443/ygzad.php?id=011976121212121212
- http://65.87.199.102:443/ygzad.php?id=020329121212121212
- http://99.1.23.71:443/bpomm.php?id=020982121212121212
- http://65.87.199.102:443/bpomm.php?id=002109121212121212
- http://99.1.23.71:443/rjjoe.php?id=008994121212121212
- http://65.87.199.102:443/rjjoe.php?id=015622121212121212
- http://99.1.23.71:443/cslvv.php?id=028657121212121212
- http://65.87.199.102:443/cslvv.php?id=009700121212121212
- http://99.1.23.71:443/vghtg.php?id=002106121212121212
- http://65.87.199.102:443/vghtg.php?id=018698121212121212
- http://99.1.23.71:443/kbyny.php?id=010796121212121212
- http://65.87.199.102:443/kbyny.php?id=032222121212121212
- http://99.1.23.71:443/ypanf.php?id=017108121212121212
- http://65.87.199.102:443/ypanf.php?id=024083121212121212
- http://99.1.23.71:443/gmvrl.php?id=018065121212121212
- http://65.87.199.102:443/gmvrl.php?id=003381121212121212
- http://99.1.23.71:443/xtjan.php?id=027263121212121212
- http://65.87.199.102:443/xtjan.php?id=010227121212121212
- http://99.1.23.71:443/ofypv.php?id=015393121212121212
- http://65.87.199.102:443/ofypv.php?id=023673121212121212
- http://99.1.23.71:443/luiae.php?id=005768121212121212
- http://65.87.199.102:443/luiae.php?id=022611121212121212
- http://99.1.23.71:443/ksycs.php?id=024451121212121212
- http://65.87.199.102:443/ksycs.php?id=023453121212121212
- http://99.1.23.71:443/ydtff.php?id=025174121212121212
- http://65.87.199.102:443/ydtff.php?id=010519121212121212
- http://99.1.23.71:443/vskti.php?id=003464121212121212
- http://65.87.199.102:443/vskti.php?id=030690121212121212
- http://99.1.23.71:443/tzdhx.php?id=011630121212121212
- http://65.87.199.102:443/tzdhx.php?id=028644121212121212
- http://99.1.23.71:443/qgzrs.php?id=026953121212121212
- http://65.87.199.102:443/qgzrs.php?id=002819121212121212
- http://99.1.23.71:443/gjyxf.php?id=015749121212121212
- http://65.87.199.102:443/gjyxf.php?id=012118121212121212
- http://99.1.23.71:443/nhfwt.php?id=010929121212121212
- http://65.87.199.102:443/nhfwt.php?id=003353121212121212

- http://99.1.23.71:443/uokpr.php?id=022892121212121212
- http://65.87.199.102:443/uokpr.php?id=016839121212121212
- http://99.1.23.71:443/tfbop.php?id=001928121212121212
- http://65.87.199.102:443/tfbop.php?id=019181121212121212
- http://99.1.23.71:443/mctvb.php?id=016834121212121212
- http://65.87.199.102:443/mctvb.php?id=020153121212121212
- http://99.1.23.71:443/qkyqc.php?id=017507121212121212
- http://65.87.199.102:443/qkyqc.php?id=022713121212121212
- http://99.1.23.71:443/balzi.php?id=010407121212121212
- http://65.87.199.102:443/balzi.php?id=001853121212121212
- http://99.1.23.71:443/nacey.php?id=017409121212121212
- http://65.87.199.102:443/nacey.php?id=007558121212121212
- http://99.1.23.71:443/udgnd.php?id=000997121212121212
- http://65.87.199.102:443/udgnd.php?id=030448121212121212
- http://99.1.23.71:443/lwcnf.php?id=019193121212121212
- http://65.87.199.102:443/lwcnf.php?id=013732121212121212
- http://99.1.23.71:443/zlkqq.php?id=023888121212121212
- http://65.87.199.102:443/zlkqq.php?id=024162121212121212
- http://99.1.23.71:443/goydj.php?id=029390121212121212
- http://65.87.199.102:443/goydj.php?id=006897121212121212
- http://99.1.23.71:443/adljt.php?id=011083121212121212
- http://65.87.199.102:443/adljt.php?id=022793121212121212
- http://99.1.23.71:443/bzymc.php?id=017084121212121212
- http://65.87.199.102:443/bzymc.php?id=004077121212121212
- http://99.1.23.71:443/otcvx.php?id=020400121212121212
- http://65.87.199.102:443/otcvx.php?id=021512121212121212
- http://99.1.23.71:443/yjzbo.php?id=026078121212121212
- http://65.87.199.102:443/yjzbo.php?id=018125121212121212

Posted by Mila at 11:12 PM Tags: cve-2010-3333, louisvilleheartsurgery.com, taidoor

No comments:

Post a Comment

Enter Comment

Newer Post Home Older Pos

Subscribe to: Post Comments (Atom)

Home