Sep 28 CVE-2010-3333 Manuscript with Taidoor (Trojan.Matryoshka by CyberESI)

contagiodump.blogspot.com/2011/10/sep-28-cve-2010-3333-manuscript-with.html

CyberESI

Jared Myers from CyberESI posted a fantastic detailed analysis of Taidoor trojan variant he called Trojan. Matryoshka for being just a container/carrier for another malicious file "Trojan.Einstein". See Trojan.Matryoshka and Trojan.Einstein The trojan arrived in a malicious RTF attachment CVE-2010-3333 from a a spoofed address of the National Chengchi University / NCCU of Taiwan. The actual sending host was a server **IBM111**, which is used by a particular group of attackers and is seen quite frequently. This sample was donated by a reader but I have a lot of IBM111-produced attachments if you are after them.

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 Name: 過程論的觀點分析六方會談 審查意見.doc
File Size: 61455 bytes
MD5: 8406c1ae494add6e4f0e78b476fb4db0

Download

 Download -8406c1ae494add6e4f0e78b476fb4db0 - as a password protected archive (contact me if you need the password)

Message + Headers

> From: 戰略學刊 [mailto:95273503@nccu.edu.tw]
> Sent: Wednesday, September 28, 2011 5:22 AM
> Subject: 稿件
> 如附檔，請收悉。
>
> From: Strategy Journal [mailto: 95273503@nccu.edu.tw]
> Sent: Wednesday, September 28, 2011 5:22 AM
> Subject: manuscript
>
> Such as the attached file, please acknowledge receipt.
>
> The viewpoint of the process of six-party talks on the review comments

Received: from IBM111 (60-249-219-82.HINET-IP.hinet.net [60.249.219.82])
xxxxxxxxxxxxxx; Wed,
28 Sep 2011 17:22:14 +0800 (CST)
Date: Wed, 28 Sep 2011 17:21:43 +0800
From: =?big5?B?vtSypL7HpVo=?= <95273503@nccu.edu.tw>
Subject: =?big5?B?vVql8w==?=
xxxxxxxxxxxxxxxxxxxx
Message-id: <051c01cc7dc0$15472a40$c900a8c0@IBM111>
MIME-version: 1.0
X-MIMEOLE: Produced By Microsoft MimeOLE V6.00.2900.2180
X-Mailer: Microsoft Outlook Express 6.00.2900.2180
Content-type: multipart/mixed; boundary="Boundary_(ID_6HJcv7WYiwyCKpqySxUA2g)"

X-Priority: 3
X-MSMail-priority: Normal

Sender

60.249.219.82
60-249-219-82.HINET-IP.hinet.net
Da Shi Yung Co., Ltd
Tainan County County Taiwan
Taiwan

Automated Scans

doc
http://www.virustotal.com/file-scan/report.html?id=ca3744ae693409b2f8addd3de99c1ccae0bc8c709678ea357898bd02e8fb362a-1317347501
Submission date:2011-09-30 01:51:41 (UTC)
AntiVir 7.11.15.74 2011.09.29 EXP/CVE-2010-3333
Antiy-AVL 2.0.3.7 2011.09.29 Exploit/MSWord.CVE-2010-3333
Avast 6.0.1289.0 2011.09.30 RTF:CVE-2010-3333 [Expl]
AVG 10.0.0.1190 2011.09.30 Suspicion: unknown virus
BitDefender 7.2 2011.09.30 Exploit.RTF.Gen
ClamAV 0.97.0.0 2011.09.30 PUA.RFT.EmbeddedOLE
Commtouch 5.3.2.6 2011.09.30 CVE-2010-3333!Camelot
DrWeb 5.0.2.03300 2011.09.30 Exploit.Rtf.based
F-Secure 9.0.16440.0 2011.09.30 Exploit.RTF.Gen
Fortinet 4.3.370.0 2011.09.30 Data/CVE20103333.A!exploit
GData 22 2011.09.30 Exploit.RTF.Gen
Kaspersky 9.0.0.837 2011.09.30 Exploit.MSWord.CVE-2010-3333.r
Microsoft 1.7702 2011.09.29 Exploit:Win32/CVE-2010-3333
nProtect 2011-09-29.01 2011.09.29 Exploit.RTF.Gen
PCTools 8.0.0.5 2011.09.30 HeurEngine.MaliciousExploit
Sophos 4.69.0 2011.09.30 Troj/RTFDrp-C
Symantec 20111.2.0.82 2011.09.30 Bloodhound.Exploit.366
TrendMicro 9.500.0.1008 2011.09.29 Possible_ARTIEF
TrendMicro-HouseCall 9.500.0.1008 2011.09.30 Possible_ARTIEF
VIPRE 10616 2011.09.30 Exploit.RTF.CVE-2010-3333 (v)
MD5 : 8406c1ae494add6e4f0e78b476fb4db0

Payload

File name:payload.exe
Submission date:2011-10-06 12:39:32 (UTC)
Result:17 /42 (40.5%)
http://www.virustotal.com/file-scan/report.html?id=53d03f3db44d40de762ca445b85011a93e6b549788c5713862e42eed173eefa3-1317904772
AhnLab-V3 2011.10.05.00 2011.10.05 Backdoor/Win32.CSon
AntiVir 7.11.15.137 2011.10.06 TR/Hijacker.Gen
AVG 10.0.0.1190 2011.10.06 BackDoor.Generic14.AJZQ
BitDefender 7.2 2011.10.06 Trojan.CryptRedol.Gen.3
DrWeb 5.0.2.03300 2011.10.06 Trojan.Taidoor
Emsisoft 5.1.0.11 2011.10.06 Backdoor.Win32.Simbot!IK
eTrust-Vet 36.1.8602 2011.10.06 -
F-Secure 9.0.16440.0 2011.10.06 Trojan.CryptRedol.Gen.3
GData 22 2011.10.06 Trojan.CryptRedol.Gen.3
Ikarus T3.1.1.107.0 2011.10.06 Backdoor.Win32.Simbot
Kaspersky 9.0.0.837 2011.10.06 HEUR:Trojan.Win32.Generic
Microsoft 1.7702 2011.10.06 Backdoor:Win32/Simbot.gen
NOD32 6521 2011.10.06 a variant of Win32/Injector.JQA
nProtect 2011-10-06.01 2011.10.06 Trojan.CryptRedol.Gen.3
Panda 10.0.3.5 2011.10.05 Suspicious file
Rising 23.77.04.01 2011.09.30 Suspicious
Symantec 20111.2.0.82 2011.10.06 Suspicious.Cloud.5
VBA32 3.12.16.4 2011.10.06 TrojanDownloader.Rubinurd.f
MD5 : d24a5c27628327da1cea545be2f99756