WEDNESDAY, JUNE 29, 2011

Jun 22 CVE-2011-0611 PDF-SWF "Fruits of economic growth" with revoked COMODO cert and Trojan Taidoor

Message is signed by a certificate "Issued by COMODO Client Authentication and Secure Email CA" and the certificate is revoked.
The sender address is a spoofed Gmail address of SEF News sef1941@gmail.com but it was sent from a HINET server in Taiwan, not from Gmail. The exploit used is CVE-2011-0611, with the same malicious SWF as described in the previous post Jun 27 PDF - SWF CVE-2011-0611 Two Views On The South China Sea from compromised Pikes Peak BOCES account w Taidoor.
The payload is the same too **Trojan Taidoor / Rubinurd** (see more with Taidoor here) with CC server **213.42.74.85**- Dubai, UAE
Update June 29 As screenshots of the certificate show, it was not expired. The Comodo Certificate Revocation List showed that the certificate was revoked less than 12 hours before it was sent, which means it was stolen and ready to be used while it was still valid. Perhaps it was used while still val for a while before I got it.
Digitally signed messages are used to gain trust of the recipient. Contagio has examples of stolen valid and invalid certificates used to signed malicious binaries in order to bypass white-listing applications and other filters. Speaking of CRL, here are two articles related to web certificates.
Revocation doesn't work (18 Mar 2011) Imperial Violet
Detecting Certificate Authority compromises and web browser collusion (22 Mar 2011) Tor Blog by ioerror

Common Vulnerabilities and Exposures (CVE)number

CVE-2011-0611

Adobe Flash Player before 10.2.154.27 on Windows, Mac OS X, Linux, and Solaris and 10.2.156.12 and earlier on Android; Adobe AIR before 2.6.19140; and Authplay.dll (aka AuthPlayLib.bundle) in Adobe Reader 9.x before 9.4.4 and 10.x through 10.0.1 on Windows, Adobe Reader 9.x before 9.4.4 and 10.x before 10.0.3 on Mac OS X, and Adobe Acrobat 9.x before 9.4.4 and 10.x before 10.0.3 on Windows and Mac OS X allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via crafted Flash content; a demonstrated by a Microsoft Office document with an embedded .swf file that has a size inconsistency in a "group of included constants," object type confusion, ActionScript that adds custom functions to prototypes, and Date objects; and as exploited in the wild in April 2011.

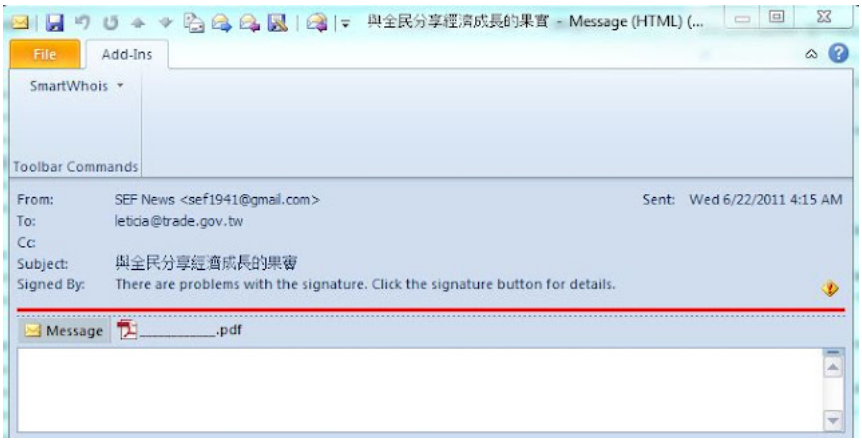
General File Information

File Name: _____.pdf
MD5: 8E3D7FCFA89307C0D3B7951BD36B3513
File Size: 249913 bytes
Distribution: Email attachment

File Download

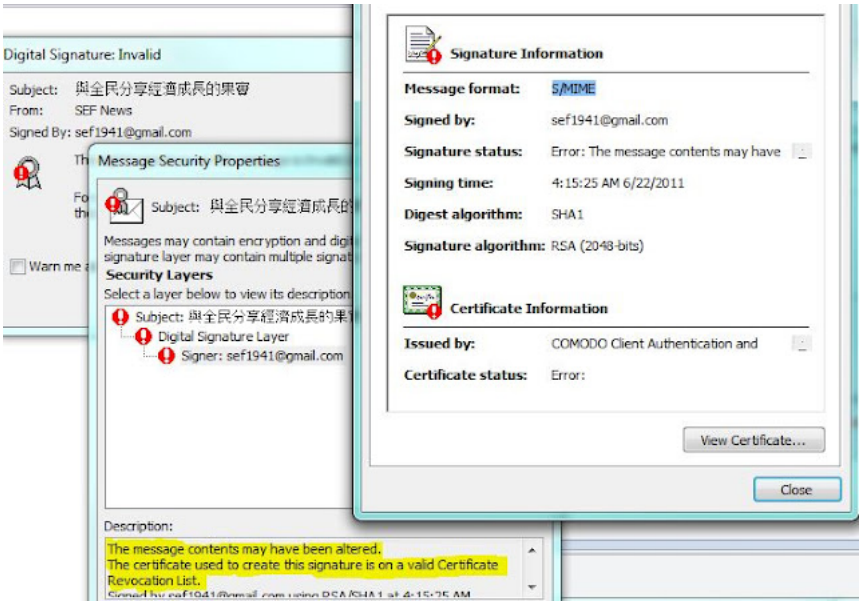
Download the original document as a password protected archive (contact me if you need the password)

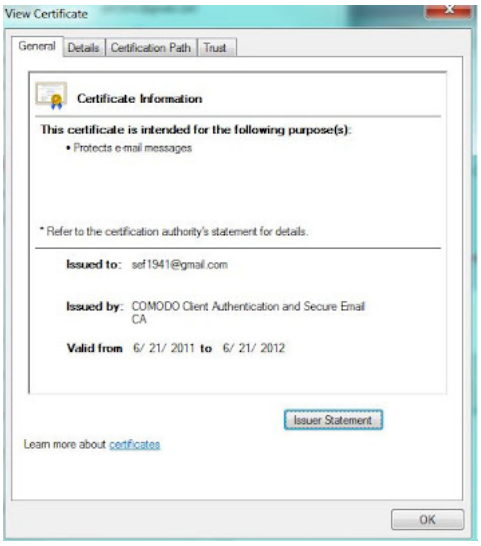
Original Message



From: SEF News [mailto:sef1941@gmail.com]
Sent: Wednesday, June 22, 2011 4:15 AM
To: leticia@trade.gov.tw
Subject: 與全民分享經濟成長的果實

與全民分享經濟成長的果實 (Google translate: All the people sharing the fruits of economic growth)
Invalid Comodo certificate: Certificate Issued by COMODO Client Authentication and Secure Email CA
Error:
The message contents may have been altered.
The certificate used to create this signature is on a valid Certificate Revocation List.
Signed by sef1941@gmail.com using RSA/SHA1 at 4:15:25 AM 6/22/2011.

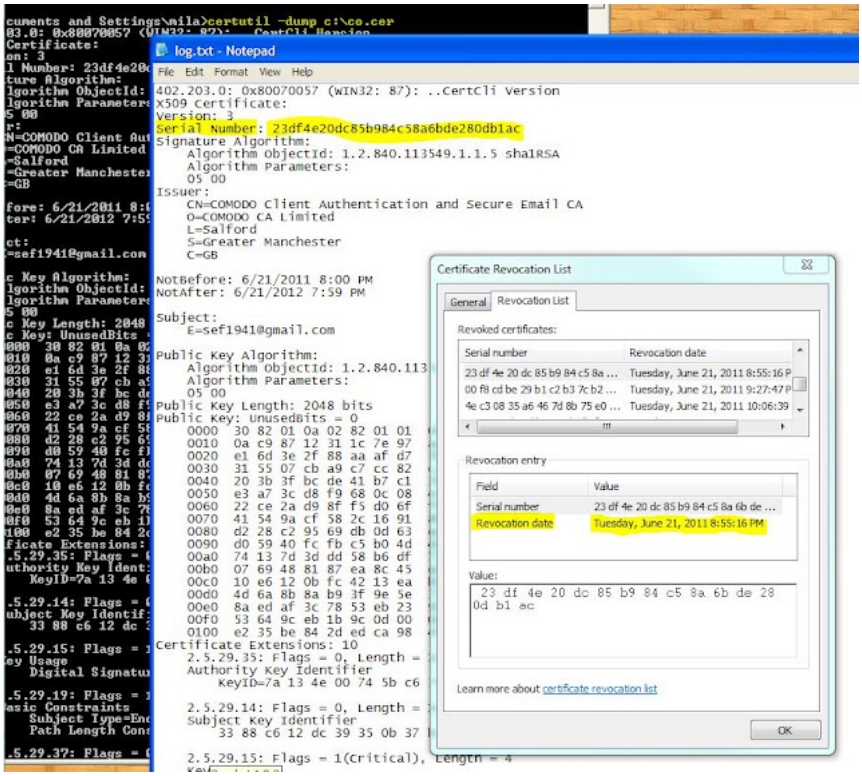




CN = COMODO Client Authentication and Secure Email CA

O = COMODO CA Limited
L = Salford
S = Greater Manchester
C = GB
KeyID=7a 13 4e 00 74 5b c6 78 63 64 27 c1 2f e2 a0 5b bc 79 c5 7b
RFC822 Name=sef1941@gmail.com
Update June 29
Revocation List showed that the certificate was revoked less that 12 hours before it was sent, which means it was stolen and ready to be used while it was still valid. Perhaps it was used while still valid for a while before I got it.
Wed, 22 Jun 2011 16:15:25 +0800 - Message sent
Tue, 21, Jun 2011 20:55:16 - Certificate revoked (I assume it is UTC +0000)

Here is all the info about the certificate (For Windows, download Server 2003 Admin pack and run **certutil.exe** to dump all the info including Certificate Revocation List URL)
current list is here http://crl.comodoca.com/COMODOClientAuthenticationandSecureEmailCA.crl
or you can download it from here, as it will change later.



402.203.0: 0x80070057 (WIN32: 87): ..CertCli Version
X509 Certificate:
Version: 3
Serial Number: 23df4e20dc85b984c58a6bde280db1ac
Signature Algorithm:
Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
Algorithm Parameters:
05 00
Issuer:
CN=COMODO Client Authentication and Secure Email CA
O=COMODO CA Limited
L=Salford
S=Greater Manchester
C=GB
NotBefore: 6/21/2011 8:00 PM
NotAfter: 6/21/2012 7:59 PM

==========

Headers

Received: (qmail 1844 invoked from network); 22 Jun 2011 08:15:30 -0000
Received: from msr6.hinet.net (HELO msr6.hinet.net) (168.95.4.106)
by XXXXXXXXXXXX with SMTP; 22 Jun 2011 08:15:30 -0000
Received: from FuckYouMan (61-221-34-242.HINET-IP.hinet.net [61.221.34.242])
by msr6.hinet.net (8.14.2/8.14.2) with SMTP id p5M8F0St022693; Wed, 22 Jun 2011 16:15:01 +0800 (CST)

Message-ID: <010601cc30b4$90aaa210$5c00a8c0@FuckYouMan>

From: "SEF News"

To: xxxxxxxxxxxxxxxxxxxx

Subject: =?big5?B?u1Cl/qXBpMCoybhnwNmmqKr4qrqqR7nq?=

Date: Wed, 22 Jun 2011 16:15:25 +0800

MIME-Version: 1.0

Content-Type: multipart/signed; protocol="application/x-pkcs7-signature";

micalg=SHA1; boundary="----=_NextPart_000_00FF_01CC30F7.9854C750"

X-Priority: 3

X-MSMail-Priority: Normal

X-Mailer: Microsoft Outlook Express 6.00.2900.3138

X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.3138

Sender

61.221.34.242

61-221-34-242.hinet-ip.hinet.net

Host reachable, 283 ms. average

61.221.34.240 - 61.221.34.247

O Lien Co., Ltd.

Taipei Taiwan

TW

PDF Information

Exploit used is CVE-2011-0611. The malicious SWF action script is identical to the one found in the previous message I posted. See analysis here: Jun 27 PDF - SWF CVE-2011-0611 Two Views On The South China Sea from compromised Pikes Peak BOCES account w Taidoor

Just like in the file discussed in the post above, the file checks for Reader versions and offers to upgrade if it is below version 9

```
if (typeof(ADBE.Reader_Value_Asked) == "undefined")
ADBE.Reader_Value_Asked = false;
if (typeof(ADBE.Viewer_Value_Asked) == "undefined")
ADBE.Viewer_Value_Asked = false;
if (typeof(ADBE.Reader_Need_Version) == "undefined" || ADBE.Reader_Need_Version < 9.0)
{
ADBE.Reader_Need_Version = 9.0;
ADBE.Reader_Value_New_Version_URL = "http://cgi.adobe.com/special/acrobat/update";
ADBE.SYSINFO = "?p=" + app.platform + "&v=" + app.viewerVersion + "&l=" + app.language + "&c=" + app.viewerType + "&r=" +

ADBE.Reader_Need_Version;
}
if (typeof(ADBE.Viewer_Need_Version) == "undefined" || ADBE.Viewer_Need_Version < 9.0)
{
ADBE.Viewer_Need_Version = 9.0;
ADBE.Viewer_Value_New_Version_URL = "http://cgi.adobe.com/special/acrobat/update";
ADBE.SYSINFO = "?p=" + app.platform + "&v=" + app.viewerVersion + "&l=" + app.language + "&c=" + app.viewerType + "&r=" +

ADBE.Viewer_Need_Version;
}

---
if (typeof(this.ADBE) == "undefined")
this.ADBE = new Object();
ADBE.LANGUAGE = "ENU";
ADBE.Viewer_string_Title = "Adobe Acrobat";
ADBE.Viewer_string_Update_Desc = "Adobe Interactive Forms Update";
ADBE.Reader_string_Need_New_Version_Msg = "This PDF file requires a newer version of Adobe Reader. Press OK to download the latest

version or see your system administrator.";
ADBE.Viewer_string_Need_New_Version_Msg_Old = "This PDF requires a newer version of Acrobat. Copy this URL and paste into your

browser or see your sys admin.";
ADBE.Viewer_string_Need_New_Version_Msg = "This PDF form requires a newer version of Adobe Acrobat. Without a newer version, the form

may display, but may not work properly. Some form elements might not be visible at all. Click OK for more information on obtaining the
latest

version of Adobe Reader.";
ADBE.Viewer_string_Need_New_Version_Msg_Updater = "This PDF form requires a newer version of Adobe Acrobat. Without a newer version,

the form may display, but may not work properly. Some form elements might not be visible at all. If an internet connection is
available, clicking

OK will download and install the latest version.";
```

Payload and Traffic

As expected, the payload is also identical to the message described above - see more details here

- Jun 27 PDF - SWF CVE-2011-0611 Two Views On The South China Sea from compromised Pikes Peak BOCES account w Taidoor
- May-June 2011 Trojan Taidoor "Louisvilleheartsurgery.com" phishing campaign
- Feb 25 CVE-2010-3333 DOC China's Military Build-up from a compromised IBEW-NECA Joint Trust Funds account

%userprofile%\Local Settings\%Name from the list below%

List of possible names:

Alerter.exe

AppMgmt.exe

CiSvc.exe

ClipSrv.exe

COMSysApp.exe

dmadmin.exe

Dot3svc.exe
EapHost.exe
HidServ.exe
hkmsvc.exe
ImapiService.exe
Messenger.exe
mnmsrvc.exe
MSDTC.exe
MSIServer.exe
napagent.exe
NetDDE.exe
NetDDEdsdm.exe
Netlogon.exe
NtLmSsp.exe
NtmsSvc.exe
ose.exe
RasAuto.exe
RDSessMgr.exe
RemoteAccess.exe
rpcapd.exe
RpcLocator.exe
RSVP.exe
SwPrv.exe
SysmonLog.exe
TlntSvr.exe
upnphost.exe
UPS.exe
VSS.exe
WmdmPmSN.exe
Wmi.exe
WmiApSrv.exe
wuauserv.exe
xmlprov.exe

23/42 - Virustotal on June 29, 2011 http://www.virustotal.com/file-scan/report.html?id=54003bd1025a8cadce96dea30fda16dac75e898beac10c13794204200dc3f153-1309203930 12/ 42 Virustotal on June 24, 2011 http://www.virustotal.com/file-scan/report.html?id=54003bd1025a8cadce96dea30fda16dac75e898beac10c13794204200dc3f153-1308889375

- o http://213.42.74.85/ywjfr.php?id=007164111D3048C607
- o http://213.42.74.85/cipaa.php?id=006655111D3048C607
- o http://213.42.74.85/zeits.php?id=012376111D3048C607
- o http://213.42.74.85/qqjnl.php?id=030576111D3048C607

213.42.74.85
Host reachable, 318 ms. average

213.42.74.80 - 213.42.74.95
Complease Trading LLC
P.O. Box 23351, Dubai, UAE

Wolfgang Vondracek
Complease Trading LLC
wvondrac@emirates.net.ae
phone: +971 4 3511616
fax: +971 4 3525720

COMPLEASE-EMIRNET
Updated: 12-Jun-2002
Source: whois.ripe.net

Clean PDF contents

%temp%\11.pdf

與全民分享經濟成長的果實
根據行政院主計處統計資料顯示，去（2010）年台灣經濟成長達
兩位數 10.88%，創下 24 年來的新高。另根據瑞士洛桑國際管理學院
see the rest here Yahoo News http://tw.news.yahoo.com/article/url/d/a/110629/53/2u5bp.html or with Google Translation.

Posted by Mila at 8:06 AM Tags: certificate, CVE-2011-0611, taidoor

No comments:

Post a Comment

Enter Comment

Newer Post Home Older Pos

Subscribe to: Post Comments (Atom)

Home