The Three Lost Battles
*Winning the War on Cybercrime*

George Tubin
Sr. Security Strategist
Meet vorVzakone
# About Trusteer

<table>
<thead>
<tr>
<th>Global</th>
<th>Hundreds of Customers</th>
<th>Leading Global Organizations Put Their TRUST In Us</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>100,000,000 Endpoints</td>
<td>7/10 Top US Banks</td>
</tr>
<tr>
<td>Solutions</td>
<td>Financial Fraud Prevention</td>
<td>9/10 Top UK Banks</td>
</tr>
<tr>
<td>Leader</td>
<td>Advanced Threat Protection</td>
<td>5/6 Top Canadian Banks</td>
</tr>
<tr>
<td></td>
<td>Intelligence Technology Expertise</td>
<td>Major European Banks</td>
</tr>
</tbody>
</table>
Agenda

- The State of Cybercrime
- Cybercrime & Malware Trends
- Latest Bank-Specific Threats
The State of Cyber-Crime
Three Lost Battles
Users Cannot Be Educated

From: linkedin.com <message-wk881425ffjm55@linkedin.com>
Subject: Mark Andronas at Payroll Processing wants to connect on LinkedIn
Date: June 2, 2011 12:55:01 PM GMT+03:00
To: Mickey Boordaei
Reply-To: message-wk881425ffjm@linkedin.com

LinkedIn
I’d like to add you to my professional network on LinkedIn.

Neal Collins
Vice President, Strategy & Corporate Development at Payroll Processing
Greater Chicago Area

Confirm that you know Neal

© 2011, LinkedIn Corporation

Blackhole

Zeus
Vulnerabilities Cannot Be Avoided

Vulnerabilities


<table>
<thead>
<tr>
<th>Platform</th>
<th>Cost Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADOBE READER</td>
<td>$5,000–$30,000</td>
</tr>
<tr>
<td>MAC OSX</td>
<td>$20,000–$50,000</td>
</tr>
<tr>
<td>ANDROID</td>
<td>$30,000–$60,000</td>
</tr>
<tr>
<td>FLASH OR JAVA BROWSER PLUG-INS</td>
<td>$40,000–$100,000</td>
</tr>
<tr>
<td>MICROSOFT WORD</td>
<td>$50,000–$100,000</td>
</tr>
<tr>
<td>WINDOWS</td>
<td>$60,000–$120,000</td>
</tr>
<tr>
<td>FIREFOX OR SAFARI</td>
<td>$60,000–$150,000</td>
</tr>
<tr>
<td>CHROME OR INTERNET EXPLORER</td>
<td>$80,000–$200,000</td>
</tr>
<tr>
<td>IOS</td>
<td>$100,000–$250,000</td>
</tr>
</tbody>
</table>

Source: Forbes, March 2012

Photo credit: Ryan Naraine
Computers Cannot Be Kept Clean

SHA256: 869579adb68399f2cadc684e49dfed0b149ee250c58f9e989f17a8a6e2
File name: file-2324493_swat
Detection ratio: 2 / 42
Analysis date: 2011-06-01 23:02:18 UTC (1 year, 2 months ago)
Result: Endpoints Cannot be Trusted
Anatomy of a Cyber-Attack

User Target
Spear-Phishing, Weaponized document

System Exploit
Zero-day or Unpatched Application Vulnerability

Malware Infection
Dropper
C&C comm, Payload, Dwell, Exfiltrate

Data Exfiltration
Advanced Malware: RSA Case Study

Data Exfiltration

Endpoint Controls

Exploit

RAT

Perimeter Controls

Data Center Controls

WWW
MitB Malware: Anything Is Possible

PII Theft

Credentials Theft

Social Engineering
Most Malware Use Form-Grabbers
Cybercrime & Malware Trends
Cybercriminals: The Perfect Storm

- **Nation-State Cyberwarfare**
  - Intensive training programs
  - Meager pensions

- **Organized Crime**
  - Highly advanced underground economy
  - Programmers “forced” to collaborate
Vulnerabilities Are NOT Going Away

- **2013 0-days (critical)**
  - Java – 1/10, 1/16, 2/13, 4/13, 6/13
  - Adobe – 2/7, 2/13, 4/13, 5/13, 6/13, 7/11
  - Microsoft – 2/13, 4/13, 5/6, 5/13, 7/11
  - Google Chrome – 3/11
  - Chrome OS – 4/13

- **And, Breaches on the Rise**
  - Operation Red October
  - NYT, WSJ, Washington Post
  - Federal Reserve
  - Twitter, Facebook, Microsoft, Evernote, LivingSocial
  - Bit9!

**Weekly Calendar:**
- **Wednesday:**
  - 1:30 - Java (James Forshaw) **PWNED**
  - 2:30 - Java (Joshua Drake) **PWNED**
  - 3:30 - IE 10 (VUPEN Security) **PWNED**
  - 4:30 - Chrome (Nils & Jon) **PWNED**
  - 5:30 - Firefox (VUPEN Security) **PWNED**
  - 5:31 - Java (VUPEN Security) **PWNED**

- **Thursday:**
  - 12pm - Flash (VUPEN Security) **PWNED**
  - 1pm - Adobe Reader (George Hotz) **PWNED**
  - 2pm - Java (Ben Murphy via proxy) **PWNED**
June 5, 2013
University of Massachusetts - Amherst
Amherst, Massachusetts
EDU HACK 1,700

The information of almost 1,700 clients of the Center for Language, Speech, and Hearing may have been exposed. A computer workstation was found to be infected by a malicious software program. Client Social Security numbers, addresses, names of health insurers, and primary health care or referring doctors may have been accessible because the computer was compromised.

March 16, 2013
Salem State University
Salem, Massachusetts
EDU HACK 25,000

A server was found to be infected with a virus. The University computer contained information related to paychecks distributed by the University. Current and former employees who may have been students or staff may have been affected.

February 13, 2013
University of North Carolina
Chapel Hill, North Carolina
EDU HACK 3,500

A cyber attack on two servers resulted in the exposure of employee information. The servers were at the UNC Lineberger Comprehensive Cancer Center. Employees, contractors, and visiting lecturers at the Lineberger Center may have had their Social Security numbers or passport numbers exposed. The breach was discovered in May of 2012 and notifications were sent in December of 2012. Fewer than 15 people who were subjects in research studies were also affected by the breach.
Malvertising: Surf the Web, Get Infected

• “Malicious Advertising” – to spread malware.
  ▪ Inserted into high-profile reputable websites
  ▪ Can "push" exploits to web users

• Recent Campaign
  ▪ Several ad networks hosting campaigns, including: Clicksor, linkbucks.com, Hooqy Media Advertiser, and traff.co
  ▪ Blackhole Exploit Kit targeting Java 0-day vulnerability
You Can’t Even Trust Twitter

Twitter Malware: Spreading More Than Just Tweets

```javascript
function _PostTweet()
{
    var a = $('input[name="authenticity_token"]').val();
    a.length > 0 && $.post("/i/tweet/create", {
        authenticity_token: a,
        place_id: "",
        status: _GetRndMsg()
    }).always(function() {
        ar[0].msgsent = 1, SetO(), window.location.href = window.location.href
    })
}
```

![Twitter Malware Image]

![Associated Press Tweet]

Breaking: Two Explosions in the White House and Barack Obama is injured

12:07 PM - 23 Apr 13
Evasion Techniques Just Keep Getting Better

- **Tilon Discovered by Trusteer – Aug 12**
  - Avoids virtual machines
  - Injects code into native Windows processes
  - Watchdog thread

- **Shylock’s New Evasion Trick – Nov 12**
  - Detects Remote Desktop Protocol
  - Hooks into shutdown process

- **Tinba and Tilon “Downgrade” – Feb 13**
  - Shift to credential theft
  - Includes:
    - Fake login page
    - Login blocking with error message
    - Captures all authentication
    - Avoids backend risk engines
Employee Endpoints Are Infected

Advanced Malware Infection Distribution on Employee Endpoints (large US bank)

- Gozi: 17%
- Hiloti: 13%
- Zeus2: 23%
- Other: 13%
- Torpig: 7%
- eBlaster: 7%
- Bugat: 4%
- Nugg: 4%
- SpyEye: 4%
- Zeus1: 4%
- Seus: 2%
- Tatanga: 2%
Latest Bank-Specific Threats
Fraud as a Service
An Identity is Born

ZAPILI.CC

Scan service

Utility bill (UK)

Atlantic Electric and Gas

Dear John Smith,

Thank you for paying by Direct Debit. You have received our maximum discount by paying this way.

This is your electricity statement for 15 March 2013 until 15 June 2013.

As you are spreading your electricity costs throughout the year, we will carry forward the balance you owe of £86.22.

www.atlanticag.co.uk

28179320116

0845 073 3030

Your electricity account

new threats, new thinking
Fraud as a Service
An Identity is Born

Scan service
Hello, Yamato!

Support: support@zapili.cc
Account Take Over
Bank Accounts

Selling EU and US bank accounts that include:

- Online banking user name
- Online banking password
- Any data needed for secret questions or authentication
- The victim’s IP and SOCKS proxy on the victim’s device
Legal Implications:
What Do These Cases Have In Common?

$560,000 loss
97 Wire Transfers

$345,000 loss
6 ACH Transfers

$440,000 loss
1 Wire Transfer

$336,600 loss
1 Wire Transfer
DDoS Is Not Just About DDoS!

“Twas the night before Christmas…”
Key Takeaways

Despite the industry’s best efforts
- Software vulnerabilities will continue
- User devices will become compromised

Advanced malware will remain difficult to prevent and detect
- Sophisticated malware can only be beaten with equally sophisticated prevention technologies
- Silver bullets do not exist, but a well constructed layered security approach does work

Fraud prevention is a shared responsibility
- Institutions must provide education, tools, support
- Users must know their responsibilities and take advantage of provided tools
Thank YOU

cnew threats, new thinking