Cybersecurity: Fact vs. Fiction
Dispelling FUD

John LaCour
June 21, 2013

Cybercrime: Fact vs. Fiction

- About PhishLabs
- Fear, Uncertainty, and Doubt
- Cybersecurity MythBusters
- Evolution of Cybercrime
- Real World Threats
- Understanding Risks
- Top Threats and Countermeasures

What we do: PhishLabs is the leading provider of cybercrime protection and intelligence services that fight back against online threats and reduce the risk posed by phishing, malware, distributed denial of service (DDoS) and other cyber-attacks.

Where: HQ in Charleston, SC with staff in 4 countries

How: 24x7x365 Security Operations Center investigates and mitigates ~50,000 incidents / year
FUD
FUD

Oh please, oh please...

CAT FUD

CAT FUD

CAT FUD
Fear, Uncertainty, and Doubt

COMPUTER VIRUS SPREADS TO HUMANS!
Eight charged in US over cyber crime ring

EIGHT alleged members of an international cybercrime ring have been accused of hacking into the computers of more than a dozen leading financial institutions and the US army’s payroll service.

US prosecutors said the scheme to steal millions from customer accounts was led by Oleksiy Sharapka, 33, of Kiev, Ukraine, who remains at large along with a second Ukrainian citizen.

The conspiracy is alleged to have begun about the same time Sharapka was deported from the US in 2012 after serving time in federal prison in Massachusetts.
Fear, Uncertainty, and Doubt

3.6 million Social Security numbers hacked in S.C.

Published: October 26, 2012

Tax returns, personal data compromised in ‘massive’ breach

By NOELLE PHILLIPS — nophillips@thestate.com

The U.S. Secret Service detected a security breach at the S.C. Department of Revenue on Oct. 10, but it took state officials 10 days to close the attacker's access and another six days to inform the public that 3.6 million Social Security numbers had been compromised.
Fear, Uncertainty, and Doubt
Fear, Uncertainty, and Doubt

Fast-Talking Computer Hacker Just Has To Break Through Encryption Shield Before Uploading Nano-Virus

NEWS • Science & Technology • Internet • ISSUE 49•15 • Apr 9, 2013

Cipher, moments before cracking into the mainframe and declaring, “I’m in.”
MythBusters

Myth: You’re responsible for fraud on your ATM / debit card

Reality: Consumers are not responsible for unauthorized ATM transactions under Regulation E (Electronic Fund Transfer Act)
MythBusters

Myth: You’re responsible for fraud on your credit card

Reality: Your not responsible for credit card fraud as long as it is promptly reported
Myth: Most hackers target their victims

Reality: Most hackers are opportunistic. They don’t care who their victim is in most cases.
Myth: Macs are more secure than PCs (Windows)

Reality: Macs are not inherently more secure than PCs. Windows PC are targeted by malware more often since they’re more ubiquitous. As Macs and smartphones have become increasingly popular, the prevalence of malware and attack code for these platforms has increased.
Myth: If I keep my AntiVirus software up-to-date, I won’t get infected.

Reality: Thousands of new pieces of malware are released every day. AntiVirus software provides some protection, but most infection happens because your other software isn’t up to date or you decide to run an unknown program.
The Evolution of Cybercrime

1970

1980

1986 – Brain Virus

1988 – Morris Worm

1990

Theft of Services / Spamming

1994 – Green Card Lottery Spam

2000
The Evolution of Cybercrime

- **2000** – Bank Web Site ‘Phishing’
- **2005** – Cybercrime for Profit
  - 2007 Zeus Banking Trojan
- **2010** – ‘Anonymous’ denial of service attacks
  - ‘Hacktivism’
The Evolution of Cybercrime

- **2009**: Operation Aurora – China
- **2010**: Operation StuxNet – US / Israel
- **2012**: Operation Ababil - Bank DDOS Attacks – Iran?
The Evolution of Cybercrime

Cybersecurity incidents by type of target:

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft of Services</td>
<td>ISPs, Telcos, Email Providers, Web sites</td>
</tr>
<tr>
<td>Money / e-theft</td>
<td><strong>Individuals and businesses</strong></td>
</tr>
<tr>
<td>Hacktivism / Political Activism</td>
<td>Government, NGOs, companies targeted by activists</td>
</tr>
<tr>
<td>Financial Espionage</td>
<td>Large corporations</td>
</tr>
<tr>
<td>Nation State Aggression</td>
<td>Critical infrastructure</td>
</tr>
<tr>
<td>Intelligence Gathering</td>
<td>Defense Contractors, Government, Other vendors to Government</td>
</tr>
</tbody>
</table>
Phishing by Target

Target Bank Account Credentials

Phishing by Target

Target
Online Games

Phishing by Target

Phishing by Target

Target
Student
Financial Aid

Phishing by Target

Enabling Target Money Laundering

Phishing by Target

Enabling Target Proxy Services

Phishing by Target

Enabling Target Webmail Account

Phishing by Target

Enabling Target Facebook

Phishing by Target

Enabling Target Shipping Companies

Phishing by Target

Enabling Target Online Dating Sites

Phishing by Victim

Dear Sir,

Our records indicate that you are a non-resident alien. As a result, you are exempted from United States of America Tax reporting and withholdings, on interest paid you on your account and other financial dealings to protect your exemption from tax on your account and other financial benefit in rectifying your exemption status.

Therefore, you are to authenticate the following by completing form W-4018, and return to us as soon as possible through the fax number: +1 (646) 527-8772.

If you are a USA Citizen, a resident, legal or illegal immigrant, this form W-4018 is also meant for you, please indicate “USA Citizen/Resident/legal or illegal immigrant” on the form and return it to us. We shall then send you a form W9095.

When completing form W-4018, please follow the steps below:

1. We need you to provide your permanent address if different from the current mailing address on your Form W-4018, you must indicate if a non-USA resident, legal or illegal immigrant, your country of origin to support your non-resident status (if your bank account or other financial dealing has a USA address for mailing purpose).

2. If any joint account holder are now USA residents or Citizen, or in any way subject to USA tax reporting laws, Please check the box in this section.
Advanced Persistent Threats

IT Security & Network Security News

DOE Lab Shuts Down Email, Web Access After Sophisticated Cyber-Attack

By: Fahmida Y. Rashid
2011-07-06
Article Rating:★★★★☆ / 4

Cyber-attackers hit another Department of Energy research lab, managers to shut down all of the facility's computer links to contain the damage.

The Energy Department's Pacific Northwest National Laboratory in Washington shut down internet access and email services following a sophisticated cyber-attack, according to a July 5 post on the facility's Twitter account. Officials became aware of the cyber-attack on July 1, Greg Koller, the lab's spokesperson, told the Associated Press.

The Definitive Story About the Most Sophisticated Cyberattack in History

By: Alexis Madrigal

The worm, called Stuxnet, targeted an Iranian nuclear facility, is about 2.5 megabytes of code that the worm is able to detect and count down in a way that it makes it very difficult as figuring them out in the first place.

While the worm is such a triumph. She got access to the worm, read about how to tell the most technically skilled what's up, and contained any bombshell revelations about how the worm works and how we figured that out.


Hacker Spies Hit Security Firm RSA

By: Kim Zetter
March 17, 2011 | 6:40 pm | Categories: Breaches, Hacks and Cracks, RSA Conference
Follow @KimZetter 2,512 followers

Top security firm RSA Security revealed on Thursday that it’s been the victim of an “extremely sophisticated” hack.
Malware Attacks

Lure Example

# Malware Attacks

## Exploit Kits:

Collection of web pages, scripts, and control panel used to infect website visitors without requiring user interaction

<table>
<thead>
<tr>
<th>Bomba</th>
<th>Bleeding Life</th>
<th>Siberia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Papka</td>
<td>CRIMEPACK</td>
<td>JustExploit</td>
</tr>
<tr>
<td>Open Source</td>
<td>Phoenix</td>
<td>Zopack</td>
</tr>
<tr>
<td>MetaPack</td>
<td>T-Iframer</td>
<td>iPack</td>
</tr>
<tr>
<td>mushroom</td>
<td>Tornado</td>
<td>EL Fiiesta</td>
</tr>
<tr>
<td>Robopak</td>
<td>SEO Sploit</td>
<td>Icepack</td>
</tr>
<tr>
<td>nuclear</td>
<td>Zombie</td>
<td>Mpack</td>
</tr>
<tr>
<td>Katrin</td>
<td>Unique</td>
<td>Webattack</td>
</tr>
<tr>
<td>Eleonore</td>
<td>Fragus 1</td>
<td></td>
</tr>
<tr>
<td>Incognito</td>
<td>Yes Exploit</td>
<td></td>
</tr>
<tr>
<td>Blackhole</td>
<td>Liberty</td>
<td></td>
</tr>
</tbody>
</table>

*Collectively, these packs exploits 74 browser and plug-in vulnerabilities!*

*http://contagiodump.blogspot.com/2010/06/overview-of-exploit-packs-update.html*
## Elenore Pack

### Operation Systems:

<table>
<thead>
<tr>
<th>System</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP</td>
<td>7574</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>2571</td>
</tr>
<tr>
<td>Windows 7</td>
<td>1766</td>
</tr>
<tr>
<td>Mac OS</td>
<td>708</td>
</tr>
<tr>
<td>Windows 2000</td>
<td>243</td>
</tr>
<tr>
<td>iPhone OS</td>
<td>197</td>
</tr>
<tr>
<td>Windows 2003</td>
<td>183</td>
</tr>
<tr>
<td>Linux</td>
<td>141</td>
</tr>
<tr>
<td>Power PC</td>
<td>102</td>
</tr>
<tr>
<td>Unknown OS :(</td>
<td>76</td>
</tr>
<tr>
<td>Windows 98</td>
<td>15</td>
</tr>
<tr>
<td>Windows ME</td>
<td>9</td>
</tr>
<tr>
<td>Symbian OS</td>
<td>7</td>
</tr>
<tr>
<td>Bots</td>
<td>5</td>
</tr>
<tr>
<td>Windows NT 4</td>
<td>2</td>
</tr>
</tbody>
</table>

*Eleonore exploits pack version 1.3.2 for Reseller. Fast statistic: Traffic: 13599 / Loads: 1363 / Percent: 10.02%*
What should I do?
Understanding Risk

Risk =

Impact of an Event
X
Probability of Event

Security =

Countermeasures < Risk
Often, Perceived Security Risk != Security Reality:

• People exaggerate spectacular but rare risks and downplay common risks.
• People have trouble estimating risks for anything not exactly like their normal situation.
• Personified risks are perceived to be greater than anonymous risks.
• People underestimate risks they willingly take and overestimate risks in situations they can't control.
• Last, people overestimate risks that are being talked about and remain an object of public scrutiny.

Source: Bruce Schneier, The Psychology of Security
District juggling earthquake concerns, bond referendums, and weary parents

Earthquake! (Don't panic.) Panic!
by Greg Hambrick

An earthquake in the Charleston region is far from assured in the next five years — hell, some don't expect another quake for another century or more. But the risk, regardless of the odds, has led the staff at the Charleston County School District to call for four downtown schools to be temporarily shuttered.

A well-documented 1886 earthquake wrecked the peninsula, killing dozens. And the next one isn't a matter of if, but when. As far as peninsula schools are concerned, that may well be tomorrow, and the district isn't taking any chances.
Understanding Risk

Risk = Impact of an Event × Probability of Event × Moral Outrage
Likely Cybersecurity Events

• Your PC will become infected

• Keep all of your software up-to-date
  – Secunia PSI
Likely Cybersecurity Events

• Your hard drive will crash
• Your laptop will be stolen or lost

• Back-up your computer
  – CrashPlan, Carbonite, Mozy
Likely Cybersecurity Events

• You will get emails that try to defraud or infect you

• Never open emails you’re not expecting.

• Use a Mac or dedicated PC for online banking
Likely Cybersecurity Events

- Your online services will be hacked
- Never re-use the same password on multiple systems
- Always use long passwords or passphrases
Summary

• Cybersecurity incidents rarely as bad as the media would have you believe
• But the Internet is overwhelmingly out to get you
• Most end-user threats are social engineering based and not purely technical
• Try to avoid the 5 security psychology traps, unless outrage is a real risk
• Four effective tips will give you the best bang for the buck
Thank you!

Questions?

John LaCour
jal@phishlabs.com
Twitter: @phishlabs
www.phishlabs.com