How Are They Doing That? – “What’s Old is New Again”

Phill Shade (Forensic Engineer – Merlion’s Keep Consulting)
Phillip D. Shade is the founder of Merlion’s Keep Consulting, a professional services company specializing in Network and Forensics Analysis.

Internationally recognized Network Security and Forensics expert, with over 30 years of experience.

Member of FBI InfraGard, Computer Security Institute, the IEEE and Volunteer at the Cyber Warfare Forum Initiative.

Numerous certifications including CNX-Ethernet (Certified Network Expert), Cisco CCNA, CWNA (Certified Wireless Network Administrator), WildPackets PasTech and WNAX (WildPackets Certified Network Forensics Analysis Expert).

Certified instructor for a number of advanced Network Training academies including Wireshark University, Global Knowledge, Sniffer University, and Planet-3 Wireless Academy.
So What is a Hacker?*

*Competing definitions:

- **Computer Programming** - A software designer and programmer who builds elegant, beautiful programs and systems. A hacker can also be a programmer who hacks or reaches a goal by employing a series of modifications to exploit or extend existing code or resources.

- **Computer Security** - A person who specializes in work with the security mechanisms for computer and network systems. It more often is used to refer to those who seek access despite them.

- **Other Technical Fields** - A person who makes things work beyond perceived limits through their own technical skill, such as a hardware or reality hacker.

Classic Hacker Profile

- >80% a former employee or student
  - Between 18 – 35 years old
  - Intelligent / Creative / Loner

- Highly motivated
  - Economic gain
  - Bragging rights
  - Revenge
  - Curiosity / Pride

- >60% from 5 major locations:
  - China / North Korea
  - Russia / Eastern Europe
  - South America

The number 1 reason
Rouges Gallery - Faces of The Enemy

1. 

2. 

3. 

4. 

5. 

6. 

7. 

SHARKFEST '12
Some Sobering Statistics…

**DIGITAL SECURITY REMAINS A MAJOR THREAT TO CONSUMERS**

- **725,000 cases of reported fraud**
  - In 2010, the FTC reports that there were over 725,000 cases of reported fraud. This is up 12.7% since 2008.
  - **2008**: 643,195 cases, 63% conducted digitally
  - **2009**: 721,418 cases, 60% conducted digitally
  - **2010**: 725,087 cases, 56% conducted digitally

- **$594**
  - The median amount fraud cost individual consumers in 2010.

Despite increased awareness of online security threats, the majority of fraud is still committed via digital contact.

**HOW VICTIMS ARE CONTACTED:**

- **45%** E-MAIL
- **19%** PHONE
- **14%** OTHER
- **11%** WEBSITES
- **10%** MAIL
ID Theft – The #1 Threat to Consumers

Identity Theft Stays On Top

19% Identity Theft

- 11% Debt Collection
- 5% Internet Services
- 5% Prizes, Sweepstakes, and Lotteries
- 4% Shop-at-Home and Catalog Sales
- 4% Impostor Scams
- 4% Internet Auction
- 3% Foreign Money Offers and Counterfeit Check Scams
- 2% Credit Cards
- 3% Telephone and Mobile Services

The most common fraud committed is identity theft, accounting for nearly 20% of all reported 2010 cases.

Although it remains a significant problem, identity theft incidence is down from 2009, when it accounted for 21% of all fraud reports.
A Major Source of Information...

BIGGEST DATA BREACHES OF ALL TIME:

Consumer fraud is a big problem, but the biggest security threats typically target companies.

- 1984 TRW
- 2005 CardSystems, Visa, MasterCard, and American Express
- 2007 T.J.X Companies Inc
- 2009 Heartland Payment Systems
- 2011 Sony Corporation

Estimated cost of the breach
Records lost

$5,400 million
$2,400 million
$5,640 Million
$7,800 million
$4,620 million
$1,476 million
What is The Government Doing About It?

What is Being Done?

Cybercrime perpetrators are not without pursuit. The Secret Service works to find and prosecute these criminals.

1,200 Suspects

$7 Billion

Is it enough?

The Secret Service arrested more than 1,200 suspects for cybercrime in 2010.

These investigations involved over $500 million in fraud loss.

They prevented approximately $7 billion in additional losses.

Sources: WTTW.FTC.GOV, DATALOSSDB.ORG, SECRETSERVICE.GOV
Case Study 1 – Spear-Phishing – A Twist to A Classic…
**Phishing** is a way of attempting to acquire information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic Communication.…. (Wikipedia)

**Spear-Phishing** is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. (Whatis.com)
Is it Legitimate?

Google AdWords

Update Billing Preferences

Primary Card Information

Type of card: Visa
Credit card number: 
The 3 or 4 digit Security Code: 
Card holder's name: 

Unlock your account at PayPal

Account has been temporarily limited
We are hereby notifying you that, after a recent review of your account activity, it has been determined that you are in violation of PayPal’s Acceptable Use Policy. Therefore, your account has been temporarily limited for 60 days to prevent further misuse of our system.

Tips to unlock your PayPal account - it’s easy
Here’s how to get started:
1. Log in to your PayPal account.
2. Follow the steps to update your personal records and you will not be allowed to use the service.
3. Once you have completed these steps, you will be sent an email notifying you that your account is available.
4. Please allow 3 to 5 business days for processing.

Note: Please do not reply to this email. This email is not monitored. If you have any questions, please log in to your PayPal account and choose the help menu.

Raise money for Steve Jobs Charity Fund!

Good afternoon,

Steve Jobs Charitable Foundation ask people about help for young webcoders. Majority of young gifted people do not have opportunity to study and bring their ideas into the life. As most known innovators in IT we support the individuals who dare to be different and work hard to change our living quality for better.

You are the one who can join us. Even a small amount will work for us and for good.

We will keep in touch sending the reports of our activities.

Thank you very much.
Real World Event – China Gmail Hack

- Google executives received an Email containing a PDF with an embedded link saying "Corporate Information – Google Management"
  - Site purports to list Google's executives, including Eric Schmidt, Sergey Brin and Larry Page

- The site executed a “Drive-by” exploit that installed Trojan spyware on the victims computers
  - Compromised information included Identities of numerous Human-Rights activists using Gmail to evade Chinese security agencies

- Cost – not publically released, but numerous dissidents have reportedly “disappeared”
What They Saw...
Case Study 2 –
Application Based Attacks / Exploits...
Example – Fake Login Screen

Fake Gmail login page
(ServiceLoginAuthen.htm)

- Blue ribbon
- Icons & text
- Some links are en_KR (Google in English for Korea)
- 2010 and text
- Wrong password alert (JS pop up)

Real Gmail login page
(ServiceLoginAuth.htm)

- Icons & text
- All links are for Google USA
- 2011 and text
Web-Based Hijack Exploit (1)
Web-Based Hijack Exploit (2)

Malicious Code Encoded:

How it Works:

1. Client visits the landing site
2. Redirect to get the exploit
3. Redirect to get the exploit
4. Download the Malware executable

Landing Site

Victim

Hop Point

Malware Distribution Site

Kaspersky Lab
New Terms For the 21st Century

- **Malware** – Malicious software designed to install remote control, password stealing or Trojan scripts onto the target machine
  - Often used to create networks or “Bot-nets” of infected machines
- **Crimeware** – Malicious software designed to install password stealing or Trojan scripts onto the target machine
  - Used to create networks or “Bot-nets” of infected machines
  - Also used to facilitate criminal activities such as monetary theft “Money Mules” or to trick user into purchasing fake or unwanted products
- **Ransomware** - Malicious software designed to install remote control, encryption or Trojan scripts onto the target machine
  - Used to extort money from victims by holding encrypted data hostage or threatening Denial of Service attacks (DoS) or data deletion
- **Hacktivist** – Hackers that publicly claim to be working to resolve perceived public or social injustice
A Classic Tale – How It Began

- Organized crime “Protection / Insurance” representatives would visit the small business offering “insurance”
  - Often targeted various ethnic communities
  - Typically for a weekly % of the sales

- Customers were protected against unfortunate business “accidents”
  - If something happened, they were usually reimbursed

- Non-Customers suffered “accidents” to their businesses

Unfortunately, organized crime has adapted to the 21st century….
"Hello. If you want to continue having your site operational, you must pay us 10 000 rubles monthly. Attention! Starting as of DATE your site will be a subject to a DDoS attack. Your site will remain unavailable until you pay us.

The first attack will involve 2,000 bots. If you contact the companies involved in the protection of DDoS-attacks and they begin to block our bots, we will increase the number of bots to 50 000, and the protection of 50 000 bots is very, very expensive.

1-st payment (10 000 rubles) Must be made no later than DATE. All subsequent payments (10 000 rubles) Must be committed no later than 31 (30) day of each month starting from August 31. Late payment penalties will be charged 100% for each day of delay.

For example, if you do not have time to make payment on the last day of the month, then 1 day of you will have to pay a fine 100%, for instance 20 000 rubles. If you pay only the 2nd date of the month, it will be for 30 000 rubles etc. Please pay on time, and then the initial 10 000 rubles offer will not change. Penalty fees apply to your first payment - no later than DATE"

You will also receive several bonuses...
1. 30% discount if you request DDoS attack on your competitors/enemies. Fair market value DDoS attacks a simple site is about $ 100 per night, for you it will cost only 70 $ per day.
2. If we turn to your competitors / enemies, to make an attack on your site, then we deny them.

Payment must be done on our purse Yandex-money number 41001474323733. Every month the number will be a new purse, be careful. About how to use Yandex-money read on www.money.yandex.ru. If you want to apply to law enforcement agencies, we will not discourage you. We even give you their contacts: www.fsb.ru, www.mvd.ru"
Just How Difficult is it to Start?
“Kits” For Sale….

Hi everyone,
I am selling Zeus 1.3.0.0

TRUSTED MEMBERS ONLY

[Version 1.3.0.0, 20.11.2009]
[+] Interception WinApi by splicing.
[+] Be fully operational in Windows Vista / 7.
[+] Temporarily disable hidden files Trojan.
[*] Removed TAN-grabber.
[-] Fixed duplicate records in nspr4.dll.
[*] Grabbed certificates are now written with the name grabbed_dd_mm_yyy.pfx, and password in UTF-8.
[*] Team gets, obtained certificates only from MY-store, and not from all. Since obtaining certificates from all hranilsh not make sense.
[*] Changed behavior grabber certificates.
[*] Rewrote FTP/POP3 sniffer, ulucheshno detection logins, made support for IPv6-addresses.
[*] Rewrote the interception of keyboard input, fixed method of working with international characters to.
[-] Corrected a bug in HTTP-fake, which could lead to deadlock.

Prices: $700 USD
Payment Methods:
Paypal (3-5 day wait)
Liberty Reserve (2 day wait)
Western Union (No wait)
Real World Event – A Zeus Bot Network

• Zeus is a do-it-yourself kit for bad guys to make computer viruses and other malware with a point and click interface

• In October 2010, a Zeus-bot network owned by “Kristina Svechinskaya (part of the Zbot Group) struck numerous major financial institutions

• The millions of compromised account experienced a transaction “fee” of $0.99 (USD) during a 30-minute period

• Cost is estimated to be in excess of $14 million (USD)
This example contains a copy of the “Ribbon Worm” designed to install a remote back-door access point into the client machine.
Case Study 3 –
Attacking From Within – The Man-in-The-Middle…
Anatomy of a Man-in-the-Middle Attack

- Attacker attempts to “insert” itself into a key location within the network
  - Favorite of industrial espionage and banking attackers
  - Originated within the early Ethernet community, returned with the advent of wide-spread Wi-Fi networking

- It will then launch a diversionary attack such as the classic “ARP-poison” to trick the targeted systems into accepting it as the “true” Server / Gateway / Router / Client / etc..

- The targeted devices will now send their traffic to the intruder
  - Intruder can copy / reinsert / manipulate the traffic
A major network analysis vendor had been working on a key project for 2 years…
- One (1) week prior to product launch, a competitor suddenly trademarked the primary name for the product as well as all of the secondary's
- Company was forced to research, develop and produce an entirely new marketing campaign, literature and product documentation

A forensics investigation revealed that the software company had been “Man-in-the-Middle” victimized
- Cost to company was in excess of two million (USD)
The device AmbitMic_aa:af:80 is attempting to trick the internet gateway (Runtop_d9:0d:db) into thinking it is the client while making the client (AmbitMic_aa:af:01) think it is the internet gateway.

### ARP Poison in Progress

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Time</th>
<th>DeltaTime</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>AmbitMic_aa:af:80</td>
<td>Runtop_d9:0d:db</td>
<td>1.134550</td>
<td>0.001270</td>
<td>ARP</td>
<td>64</td>
<td>192.168.1.103 is at 00:d0:59:aa:af:80</td>
</tr>
<tr>
<td>7</td>
<td>AmbitMic_aa:af:80</td>
<td>AmbitMic_12:9b:01</td>
<td>1.136550</td>
<td>0.002000</td>
<td>ARP</td>
<td>64</td>
<td>192.168.1.1 is at 00:d0:59:aa:af:80</td>
</tr>
<tr>
<td>10</td>
<td>Runtop_d9:0d:db</td>
<td>AmbitMic_aa:af:80</td>
<td>3.137851</td>
<td>0.000729</td>
<td>ARP</td>
<td>64</td>
<td>192.168.1.1 is at 00:20:78:d9:0d:db</td>
</tr>
<tr>
<td>11</td>
<td>AmbitMic_aa:af:80</td>
<td>AmbitMic_12:9b:01</td>
<td>3.138933</td>
<td>0.001082</td>
<td>ARP</td>
<td>64</td>
<td>Who has 192.168.1.103? Tell 192.168.1.1</td>
</tr>
<tr>
<td>12</td>
<td>AmbitMic_12:9b:01</td>
<td>AmbitMic_aa:af:80</td>
<td>3.139347</td>
<td>0.000414</td>
<td>ARP</td>
<td>64</td>
<td>192.168.1.103 is at 00:d0:59:12:9b:01</td>
</tr>
<tr>
<td>13</td>
<td>AmbitMic_aa:af:80</td>
<td>Runtop_d9:0d:db</td>
<td>5.139359</td>
<td>2.000012</td>
<td>ARP</td>
<td>64</td>
<td>192.168.1.103 is at 00:d0:59:aa:af:80</td>
</tr>
<tr>
<td>14</td>
<td>AmbitMic_aa:af:80</td>
<td>AmbitMic_12:9b:01</td>
<td>5.141324</td>
<td>0.001965</td>
<td>ARP</td>
<td>64</td>
<td>192.168.1.1 is at 00:d0:59:aa:af:80</td>
</tr>
<tr>
<td>16</td>
<td>Runtop_d9:0d:db</td>
<td>AmbitMic_aa:af:80</td>
<td>7.142461</td>
<td>0.000713</td>
<td>ARP</td>
<td>64</td>
<td>192.168.1.1 is at 00:20:78:d9:0d:db</td>
</tr>
<tr>
<td>17</td>
<td>AmbitMic_aa:af:80</td>
<td>AmbitMic_12:9b:01</td>
<td>7.143711</td>
<td>0.001250</td>
<td>ARP</td>
<td>64</td>
<td>Who has 192.168.1.103? Tell 192.168.1.1</td>
</tr>
<tr>
<td>18</td>
<td>AmbitMic_12:9b:01</td>
<td>AmbitMic_aa:af:80</td>
<td>7.143913</td>
<td>0.000202</td>
<td>ARP</td>
<td>64</td>
<td>192.168.1.103 is at 00:d0:59:12:9b:01</td>
</tr>
<tr>
<td>20</td>
<td>AmbitMic_aa:af:80</td>
<td>AmbitMic_12:9b:01</td>
<td>9.146104</td>
<td>0.001965</td>
<td>ARP</td>
<td>64</td>
<td>192.168.1.1 is at 00:d0:59:aa:af:80</td>
</tr>
</tbody>
</table>
Case Study 4 –

A Fly on The Wall - Call Interception…
Security Issue - Bluebug

- Software exploit developed by a German researcher (Hefurt)

- Exploit that allows the attacker to use the phone to initiate calls to premium rate numbers, send sms messages, read sms messages, connect to data services such as the Internet, and even eavesdrop on conversations in the vicinity
  - Done via a voice call over the GSM network
    - Allows the listening post to be anywhere in the world.
    - Bluetooth access is only required for a few seconds in order to set up the call

- Creates a serial profile connection to the device, giving full access to the AT command set, which is then exploited using standard off the shelf tools
  - PPP for networking or gnokii for messaging,
Security Issue – BlueSnarfing

- BlueSnarfing is the unauthorized accessing of features on Bluetooth-enabled devices
  - Phones
  - PDA’s
  - WLAN network devices

- Typically employed in long-range attacks
  - Favorite industrial espionage attack

“…BlueSniper rifle, a yagi-antenna and scope affixed to a gun-like stock that this week broke a distance record for BlueSnarfing… by slurping data from a Nokia 6310i from 1.1 away (2 Km) away…” Wired News Aug2004
This example contains four (4) calls and is from a VoIP network using Cisco phones and SIP signaling with G.711 audio codec.
Questions and Answers / Discussion
Thank You!