Overview

- Phishing Sites
- Trojans, Worms, Viruses, Drive-by-downloads
- BotNet
  - Fast Flux
  - Domain Flux
  - Infiltration of a BotNet
- Underground economy.
- APTs

Phishing Sites

- Phishers setting up fake look a like sites.
- Send spam asking user to connect.
- Redirection by other malware.
- http://www.phishtank.com

Spear Phishing / Whaling

- Mass Phishing has a very poor success rate.
- Targeting a phishing attack takes more time but works better. E.g.
  - Send fake e-mail pretending to be a boss’s secretary.
  - Send fake CVs/pdf malware to HR recruitment

Viruses & Worms

- A virus is a self replicating program that requires interaction to spread e.g.
  - autorun.inf on a USB stick.
  - opening a malware pdf
- Worms are self replicating program than can spread on their own. E.g.
  - Morris Worm, SQL Slammer, Conficker
- The term “Virus” is often miss-used.

Virus: Pentagon Attack

- Joel Brenner (ex-NSA) alleges that the Pentagon was attack via USB drives left in the car park.
- Employes found, them took them inside and plugged them in.
- autorun.inf ran malware.
- Pentagon superglued up all the USB ports. (USB drives banned until 2011)
Trojans

• Trojans are malware that need a user to download and run them.

• Often malware pretends to be keygens or anti-virus.

• Most attacks against Apple have been Trojans.

Drive-by-download

• Drive-by-downloads are malware infected webpages.

• Viewing the page with a vulnerable browser and OS will get you infected.

• Often JavaScript based on buffer overflows in browser plugins.

• Attacks often via XSS attacks.

RootKit

• Malware installed on machines.

• Typically:
  – Gives repeated, root access to machine.
  – Often installs other payloads
  – Hard to detect

• E.g. Mebroot which alters the Master Boot Record of a machine to load before the OS.

Zero Day

A zero day attack is an attack that is:
• previously unknown,
• no current defense.
• i.e. you have zero days to patch your system

Zero days are very rare, and valuable to both attacks and anti-virus companies, security contractors.

Man in the Browser Attacks

• Rootkits can be set to attack the browser.

• In this case all certificates can be faked.

• Anything that looks like a credit card no. or bank log in can be collected.

• TLS and web defense can’t stop this.
Botnets

- Most attackers are in it to make money.
- A single credit card number or spam e-mail isn’t worth very much.
- Networks of hacked computers (bots) are organised into large networks (botnets).

Denial-of-service attack

- With this many computers it’s easy to overload some web site.
- Easiest type of attack uses (rents) a botnet to perform a distributed denial-of-service attack.
- Often used to blackmail companies, or for political reasons.

Fast Flux

- Instead of using an IP address bots look for a URL.
- To stop the IPs getting blocked new IP addresses are registered every few mins.
- Makes it impossible to go after the hosts.

Zeus

- Zeus is one of the large botnets.
  - Uses Fast Flux
  - Many C&C servers
  - Spreads mainly via Trojans.
  - Man-in-the-browser (form grabbing)
  - Sends Spam, Phishing.

- Code is available for sale on black markets.
Domain Flux

- Bots continuously generates new URLs.
  - E.g. based on a hash of the date and a secret value.
- Botmasters know and register the URL in advance.
- Even if all C&C is shut down, bots will switch to a new URL in a few days.
- We can try to block all future URLs (hard)

Conflicker

- Computer Worm that installs a botnet
  - more than 10 million infections.
  - first version would not infect computers with Ukrainian keyboard layout.
  - spreads NetBIOS buffer overflows and guessing admin passwords.
  - uses Domain Flux and P2P
- Largely contained by security researchers who have blocked tens of thousands of domain names.

P2P

- More recent malware sets itself up as a P2P network.
- Malware connects to C&C and other bots.
- If the main C&C goes down botmasters can connect to any bot and update them all with a new C&C.

Torpig/Mebroot

- Mebroot is a root kit, that writes itself into the Master Boot Record.
  - Executes before OS loads
  - Very hard to detect.
- Spreads via drive by downloads.
- Downloads and installs other payloads.
- Torpig is a botnet downloaded and installed by Mebroot.

Torpig

Marco Cova and colleagues reverse engineered Torpig’s domain flux algorithm.

Looking ahead they noticed that some Torpig URLs weren’t registered.

So they decided to register the addresses themselves.

The Take Over.

- On the day of the URL switch 180000 infected computers started reporting to them.
- Torpig used simple XOR encryption of data, which was cracked.
- They had complete control of the Torpig botnet (but not Mebroot).
What they found.

It took 10 days for Mebroot to replace Torpig with a new payload.

For 10-days they had complete control of the botnet and saw all data.

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Data Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailbox account</td>
<td>54,090</td>
</tr>
<tr>
<td>Email</td>
<td>1,258,862</td>
</tr>
<tr>
<td>Form data</td>
<td>11,966,532</td>
</tr>
<tr>
<td>HTTP account</td>
<td>411,039</td>
</tr>
<tr>
<td>FTP account</td>
<td>12,307</td>
</tr>
<tr>
<td>POP account</td>
<td>415,206</td>
</tr>
<tr>
<td>SMTP account</td>
<td>100,472</td>
</tr>
<tr>
<td>Windows password</td>
<td>1,255,122</td>
</tr>
</tbody>
</table>

Form Data

- ~8000 bank/paypal account logins.
- 1660 credit card numbers & cvv
- At $0.10–$25 per card, $10–$1,000 per account this = $83K to $8.3M.
- Torpig also opened a proxy, which could be used by attackers.

Underground Markets Roles

1. Attacker that steals the data (e.g. via botnet’s, phishing etc).
2. Cashiers: take credit cards and bank accounts and removes cash.
3. Drops: people who provide a place to send goods.
5. Based on web forums and IRC

Market places

- Internet Relay Channel (IRC)
  - Anyone can connect and live chat
- Web forums, less common now.
- Tor Hidden services, growing fast
  - Although attacked by FBI in the last few months.

Bitcoin electronic current

- Based on partial SHA hash collisions:
  - If you can find a partial collision you have minted a bitcoin.
- Passed from one person to another by signing an entry in a public database.
- Only the person with the signing key can pass it on.

Payment other methods

- “Webmoney” online payment based in Russia
- Western Union money transfer
- Closed down:
  - E-Gold another digital currency: trading shut down in 2009 due to crime
  - Liberty Reserve based in Costa Rica, taken down in May.
Typical Transaction 1:
- Hacker steals 1000 fullz (credit card number, CVV, name, address, etc.)
- Sells them on forum for 10 bitcoins (£4300)
- Buyer sells them in groups of 20 to cashiers for £300 in “Webmoney”

Typical Transaction 2:
- Bot master offers network for DDoS attack at £200 a day.
- Attacker hires the botnet to attack small company, bring down their site.
- Attacker anonymously contacts the company and asks for £10,000 in bitcoins to stop.

Less Common Attacks: Advanced Persistent Threats
- APT are attackers that will put a lot of time and effort into attacking a target.
- Well funded, technically advanced.
- Common techniques include:
  - Very carefully crafted phish attacks
  - Waterholding: Drive-by-downloads on website likely to be used by public.
  - Zero days

Reading
  - what happened in cyber security last year
- Marco et al.’s paper on Torpig.
  Both linked to from the lecture website.

Conclusion
- Phishing Sites
- Trojans, Worms, Viruses, Drive-by-downloads
- BotNet
  - Fast Flux
  - Domain Flux
  - Infiltration of a BotNet
- Underground economy.
- APTs