



openHPI – Internet Security Malware: Botnets

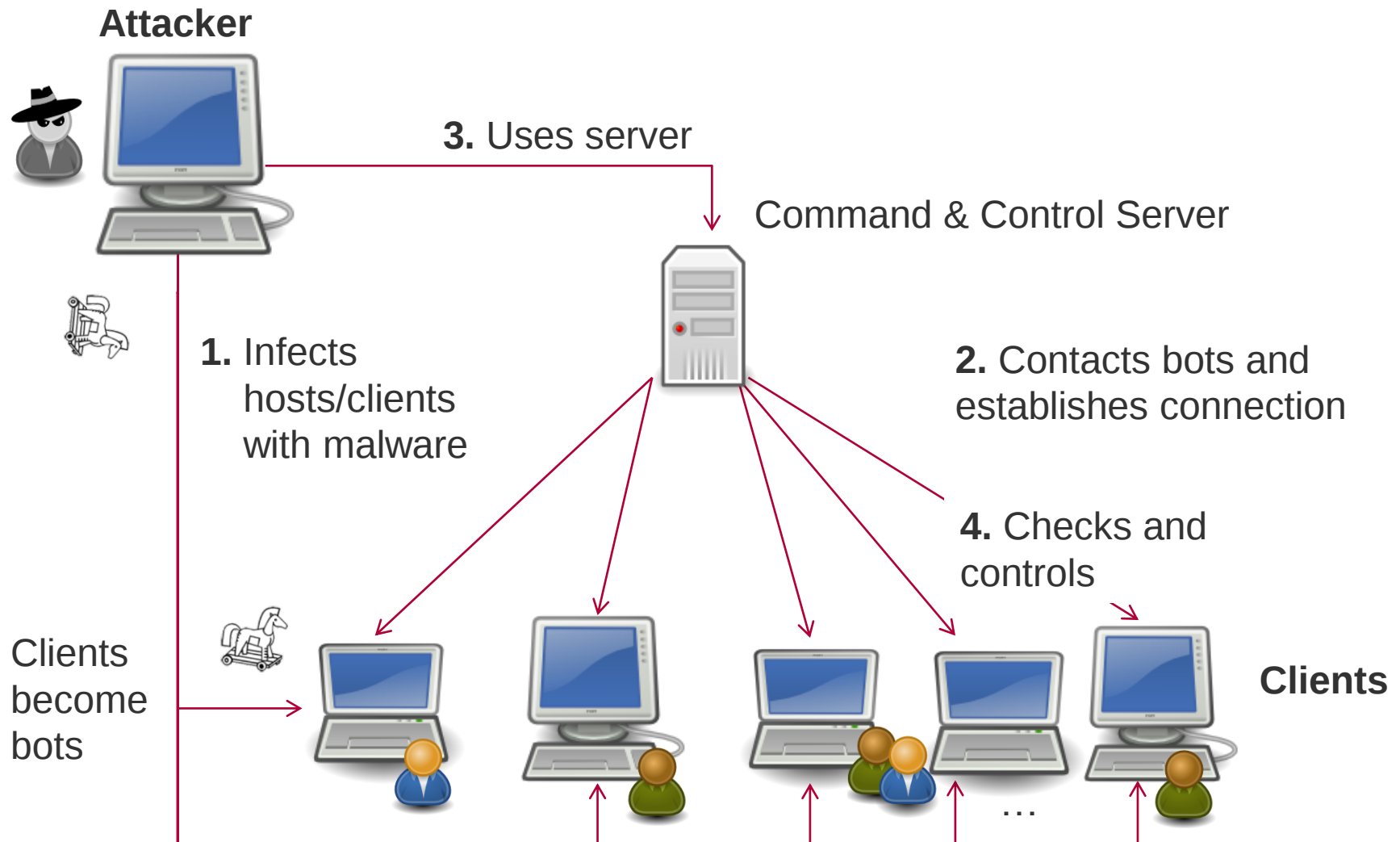
Prof. Dr. Christoph Meinel
Hasso Plattner Institute, Potsdam, Germany

Botnets

Initial description

- Remote controlled (multiple) computers - **bots** - typically produced by malware without the knowledge of the respective computer owner
- (Central) "**command and control server**" - **C&C Server** - in the hands of an attacker manages, coordinates and controls the (numerous) bots
- C&C Server takes remote control over the bots and sends operating instructions, which then run them independently
- By combining numerous bots, a large number of attacks with high computational power can occur

Botnets – Basic Principle (1/2)



Botnets – Basic Principle (2/2)

- An attacker infects many clients with malware
 - Mostly trojans are used to conceal real function
 - Worms allow fast automatic spreading as well
 - Web browser vulnerabilities also serve as an entry gate
- Malware allows communication with the C&C server
- Clients who have become "bots" can then receive and execute the commands of the C&C server
 - An attacker can send his commands to the bots via the C&C server
 - Bots then execute commands independently

Botnets – Attack Scenarios

Cybercriminals use botnets to

- Perform distributed denial of service attacks - DDoS
- Send spam e-mails
- Hide the attacker's sender address
- Perform click fraud
- Read the bot's sensitive data, e.g. passwords ...
- Provide illegal information and resources (storage medium / service provider)
- Calculate/ create crypto currency (Bitcoin mining)
- Use of ransomware, e.g. to blackmail by encrypting personal data and demand money to provide the decryption key

Botnets – Well-Known Examples

Zeus

- Estimated amount: 3,600,000 bots
- Discovered: 2007

Conficker

- Estimated amount: 9,000,000 bots
- Discovered: 2008

ZeroAccess

- Estimated amount: 9,000,000 bots
- Discovered: 2011

Mirai

- Estimated amount: 1,500,000 bots
- Discovered: 2016

Example of Botnet Attack: Bitcoin Mining

Thanks to their huge number of bots, botnets are very well suited to accomplish tasks requiring extremely high but easily distributed computing power, e.g. Bitcoin mining

- Bitcoin mining consumes a lot of computing power, but can easily be distributed
- A single PC is hardly able to do this, but when many PCs are connected, useful results can be generated
- The first "prototypes" were created in universities where students or employees used workstations to "mine"
- In December 2013, two German hackers who had modified a Trojan to "mine" and thus generate Bitcoins to the equivalent of 950,000 US \$ were arrested ...

“Storm” Botnet (1/2)

“Storm” botnet was first discovered in 2007 because of a high distribution of “Storm” worms

- Distribution via spam e-mails and subsequent infection of Windows systems
- Estimated amount: 1-50 million bot PCs
- Operators have so far remained undetected
 - Security experts / researchers underwent massive attacks as soon as investigations were made
- Antivirus programs as countermeasures were switched off remotely, but the user was led to believe they were working
- It was strong enough to disconnect whole countries from the Internet
- To an extent even more powerful than supercomputers ...

“Storm” Botnet (2/2)

- At the end of 2007 the operators of the “storm” botnet began to split their organization, possibly to sell parts of the botnet
- Data traffic for communication with the botnet was encrypted
- Architecture very complex with very different components:
 - (1) Backdoor or downloader malware
 - (2) SMTP Relay Server to send e-mails
 - (3) Attack software for stealing e-mail addresses
 - (4) Attack software to spread the malware via e-mails
 - (5) DDoS attack software to perform scattered attacks
 - (6) Updated version of malware installers

“Storm” Botnet: Stormfucker

Presented at the Chaos Communication Congress (2008, Berlin)

- Stand-alone worm that only infects systems already infected with the storm worm. Removes storm malware via update mechanism
- Allows cleanup / removal of parts of the “storm” botnet
 - Possible because identification of C&C servers was inadequate
 - Verification mechanism could be cracked by brute force attacks, this enabled the sending of commands as a “new” C&C servers (takeover of the C&C server)
 - Prompt to update the storm application
 - Replace by counterfeit application
- Bots no longer receive command from the original, but from the new C&C server

Zeus (1/3)

First discovered in 2007

- Targets Windows systems
- Trojan contains additional software for
 - Spying out personal data in the web browser, e.g. logins for social networks or online banking
 - Encryption of sensitive data and subsequent extortion for paid publication of the key
- Captured data from over 74,000 user accounts from companies like: NASA, Bank of America, Oracle, Amazon, Cisco, ...
- Very hard to identify due to concealment mechanisms
- Spread through phishing and hidden downloads
 - 3,600,000 infected systems in the US alone

Zeus (2/3)

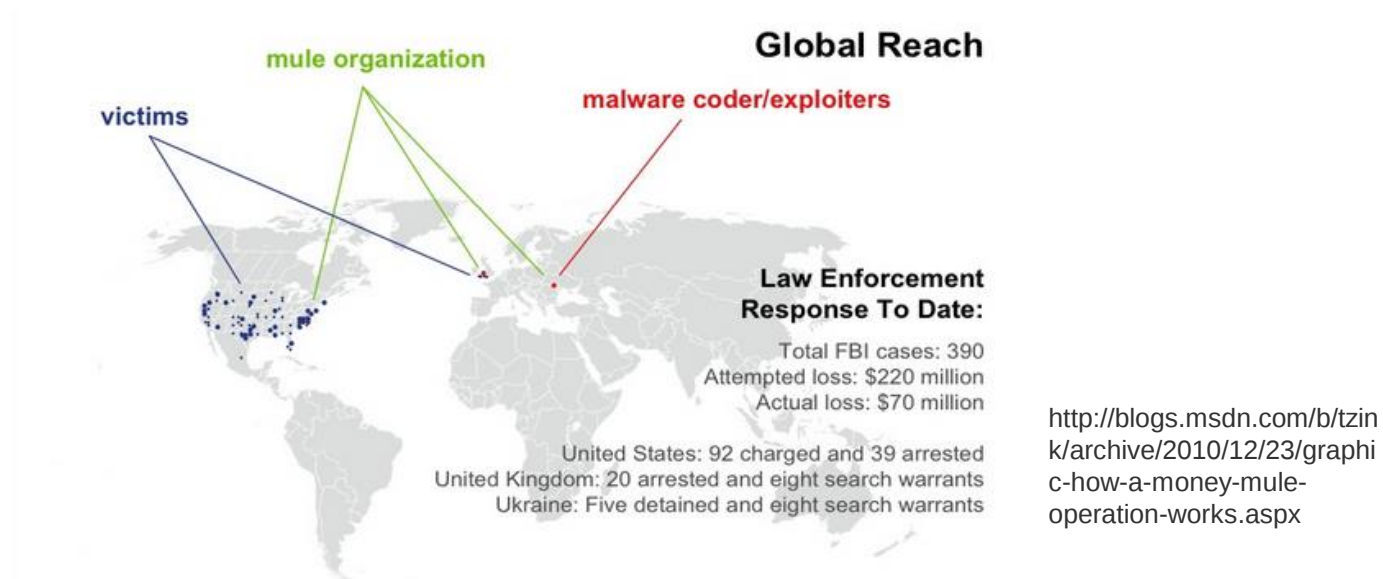
Zeus operators can finely select the information in which they are interested, e.g. Access data to specific services, social networks, online banking, ...

- In October 2010 the FBI published that Eastern European hackers had succeeded in infecting systems with Zeus malware worldwide
 - Online banking accounts were taken over and several thousand dollars were transferred to middle-men
 - Middle-men had previously opened accounts with fake identities and transferred the stolen money on or smuggled it out of the country
- Caused total damages of approximately 70 million US \$. More than 100 people were arrested

Zeus (3/3)

The global organization of criminals was phenomenal

- Cybercriminals attempted to steal in total 220 million US \$
- FBI registered 390 fraud cases
- **The hackers** came from Eastern Europe, **the middle-men** from America, Great Britain and Eastern Europe and **the victims** largely from the USA



Zeus – Gameover ZeuS

"Gameover ZeuS" was discovered at the end of 2013

- A Botnet used for bank fraud as well as criminal encryption of personal data
- Unlike older versions, the connection to the C&C server is encrypted
- Generates thousands of domain names used for communication and are valid for one day only
- One variant targets systems in Ukraine and Belarus, another computers in the US
- In June 2014 an international organization "Operation Torvar" succeeded in temporarily disconnecting the connection between the C&C server and the bots