

BOTNET

Information warfare

Theory and practices from the scene

BOTNET: Information Warfare

Theory and Practices from
“the Scene”

Authors:
Stefano Maccaglia
Alberto Passavanti
Raffaele Adesso



Virus definition

- A **computer virus** is a computer program that can copy itself and infect a computer without permission or knowledge of the user. The term "virus" is also commonly used, albeit erroneously, to refer to many different types of malware and adware programs. The original virus may modify the copies, or the copies may modify themselves, as occurs in a metamorphic virus. Viruses can spread to other computers by infecting files on a network file system or a file system that is accessed by another computer. Viruses are sometimes confused with computer worms and Trojan horses
- Commonly the term virus is often used as synonymous with malware, indicating then from time to time also categories of different , such as worms, Trojans and dialers.

From Wikipedia: http://en.wikipedia.org/wiki/Computer_virus

Worm definition

- A worm is a special category of malware able to replicate. It is similar to a virus, but unlike this does not need to bind to other executable to spread. Typically a worm that infects computers, tends to be executed each time you start the machine and it remains active until you turn off your computer or you kill the worm process accordingly.
- The most common media used by the worm to spread is by email, the malicious program search e-mail addresses stored on the host computer and sends a copy of itself as a file attachment (attachment) to all or part of addresses that could raise.
- These malicious executables can also use the circuits of file sharing to spread. In this case they copy themselves through the files shared by the victim and tend to hide as utilities or crack of very expensive programs, in order to induce others to download and run them.
- The perhaps more subtle type of worm takes advantage of bugs in some software or operating systems, to automatically spread to all vulnerable computers connected to the network.

Trojan definition

- A trojan or trojan horse, is a type of malware.
- It owes its name to the fact that its features are hidden inside a seemingly useful program, so that the user installing and running a program, unwittingly, installs and runs the trojan hidden code.
- Generally the term Trojan, refers to remote access trojan (also from RAT Remote Administration Tool), usually consisting of 2 files: **the file server**, which is installed in the machine victim, and a **client file**, used by pirate to send instructions that the server is running. In this way, like the mythical stratagem adopted by Ulysses, the victim is induced to move the program “into the city”, that means, beyond metaphor, “to run the program”.
- There are some legal software with features similar to the Trojans, but in this case the user is aware of the situation.

Trojan: Spread mechanisms and Functions

- Trojans do not spread themselves as viruses or worms, thus requiring a direct intervention by the aggressor to get the victim to the malicious executable. Often the victim, unconsciously, downloads and executes the trojan on his computer, because the crackers like to insert these "traps" for example in pirated video games, which generally are highly requested.
- A Trojan can contain any kind of evil instruction. Trojans are often used as an alternative to worms and viruses to install a keylogger or a backdoor on a target.
- Historically between 2001 and 2002, the Trojans begun to be used systematically for criminal operations, in particular to send spam and steal personal information such as credit card numbers and other documents or even emails.
- The next-generation Trojan have multiple features, such as connections via IRC bot, forming precisely Bot networks, and better options to hide in the operating system, using Rootkit's techniques .

Malware's components

- The simplest Malware is composed of two parts, sufficient to ensure its replication:
 - **a search routine**, which deals with search files suit to be infected;
 - **an infection routine**, with the task of copying the code of Malware within each file selected by the search routine.
- Many Malware are designed to run code outside the purposes of replication and thus they contain two other elements:
 - **an Activation routine**;
 - **The payload**.
- The virus can be encrypted and perhaps change algorithm and / or key each time you run, and may contain three elements:
 - **a decryption routine**;
 - **an encryption routine**;
 - **a mutation routine**, which deals with the routine change of encryption and decryption for each new copy of the virus.

AV and analysis strategies

- The antivirus actually are based on the so-called "signature" or "signatures", to identify a malicious content. Another mechanism is the comparison between a content being analyzed and the various possible malicious contents.
- In this approach if the malicious content is not recorded in the Antivirus signatures the AV cannot identify it as malware.
- Another form of analysis is the "Heuristic scanning", this technique attempts to detect known and new forms of malicious software searching for general characteristics.
- The main advantage of this technique is not based on file signatures to identify and counter malicious software.

Disadvantages: this approach is slow and the risk of false positives.

You can't stop what doesn't seem a threat!...

- Signature-based models breaks down when overloaded by variants
- New variants appear before signatures can be created for the previous variant
- Automated "malware delivery systems"
 - **Signature-based techniques (such as AV)**
- Are based on enough people being hit somewhere so that a signature is developed
- This model breaks down for targeted and zero-day attacks
- The model is reactive, not proactive

Obfuscation Techniques

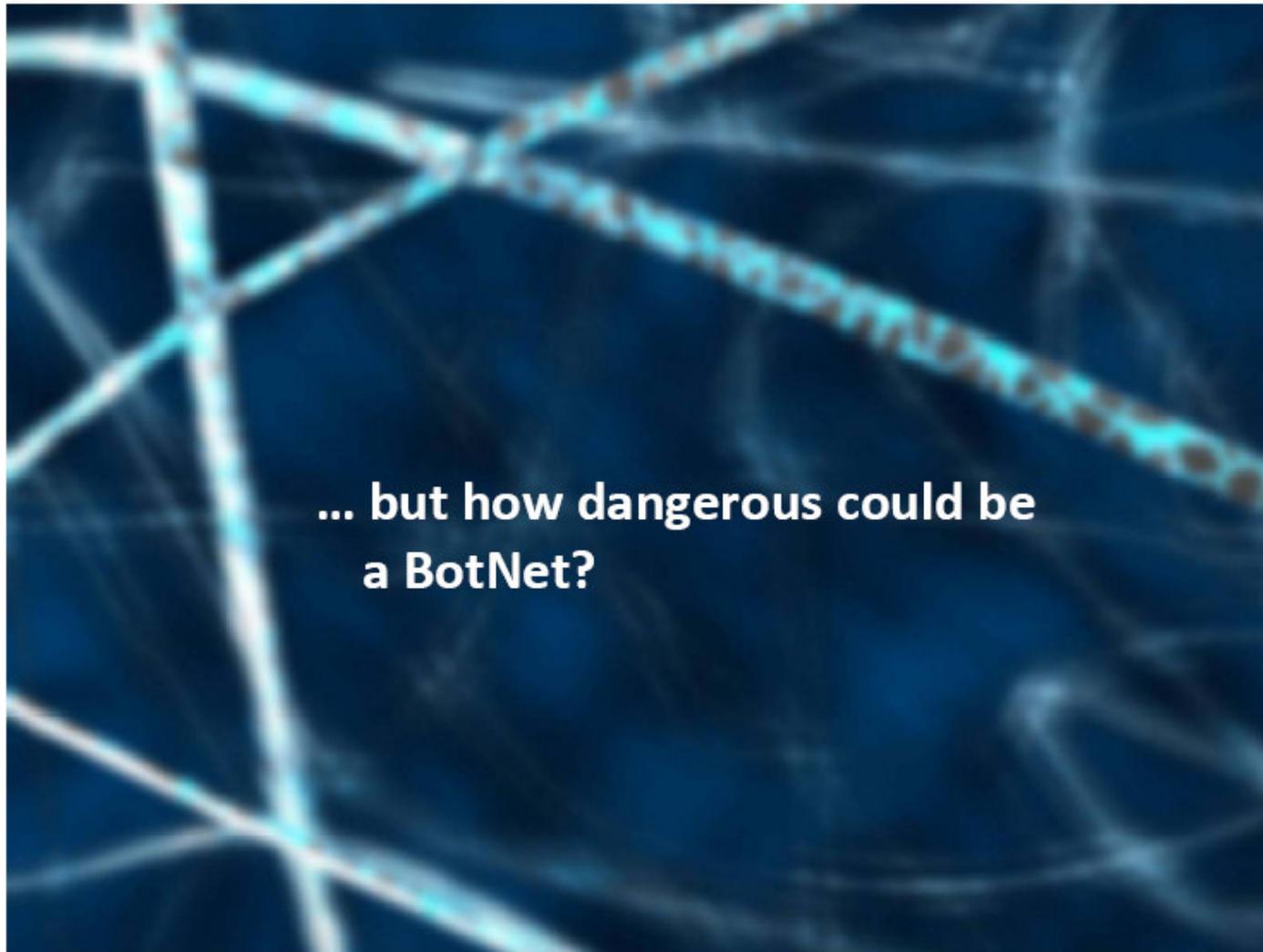
- In the past, some crackers have managed to circumvent antivirus programs using the encrypted payload to convey their attacks. For example, using UPX (The Ultimate Packer for Executables) and Morphine, a program to encrypt the data. But we have payload spread even through JPEG and GDI+ files that allow a further way to hide the Trojan horse already packed using UPX and encrypted via Morphine. With this approach the crackers can easily overcome the first defenses set by users through content filters or antivirus.

BotNet definition

- Botnet is a term used to define a set of software robots, or “bots”, working autonomously and automatically. These software bots are usually “remotely controlled”.
- Actually the Botnet word is used to define a set of compromised systems (also called “zombies” or “drones”) controlled by remote users through software as trojan or backdoor and a common infrastructure realized to support the controller.
- A botnet operator (also known as "bot herder") can control a zombie group through IRC, web server or other means (normally Instant Messaging software).

BotNet definition

- Usually the C&C (Command and Control Center) is placed inside some IRC private channels (password protected) where the zombie systems log on after the attack. A bot software works hidden ("stealth mode") and adheres to RFC 1459 (IRC) standard.
- The attack could be successful due to system weakness (exploit, buffer overflow, etc...) or to the execution of trojan horse programs.
- The first operation conducted by the bot on a newly exploited machine is the login to the C&C Channel, followed by a scan on the local network segment aiming to find more targets.



Antivirus, Firewalls, and more...

- The current scenario shows the introduction of specific technologies useful in the fight against malware and traditional methods of distribution.
- Some problems are solved, but despite this we still threat to the growth produced by Bot networks.
- The reasons are related to:
 - Bad habits of Internet users
 - Ignorance
 - Lack of implementation of basic protection mechanisms

BotNet: Facts!

guardian.co.uk

[News](#) | [Sport](#) | [Comment](#) | [Culture](#) | [Business](#) | [Money](#) | [Life & style](#)

[News](#) > [World news](#)

Russia accused of unleashing cyberwar to disable Estonia

- Parliament, ministries, banks, media targeted
- Nato experts sent in to strengthen defences



WIRED THE NEXT BIG IDEA ROLLOVER
OFTEN STARTS OFF SMALL

HOME | SUBSCRIBE » | SECTIONS » | BLOGS » | READ MAGAZINE

WIRED MAGAZINE: ISSUE 15.09

POLITICS + SECURITY

Hackers Take Down the Most Wired Country in Europe

InfoWorld [Log in](#) | [Register](#)

[HOME](#) | [NEWS](#) | [TEST CENTER](#) | [TECHNOLOGIES](#) | [BLOGS](#) | [AUDIO/VIDEO](#) | [EVENTS](#) | [AWARDS](#) | [NEWSLETTERS](#) | [C](#)

Estonia recovers from massive denial-of-service attack

Postings on Web sites indicate Russian hackers may be involved in the attacks

By Jeremy Kirk, DQ News Service
May 17, 2007

[Talkback](#) | [E-mail](#) | [Printer Friendly](#) | [Reprints](#) | [Text Size](#) **A** **A**

A spree of denial-of-service (DOS) attacks against Web sites in Estonia appears to be subsiding, as the government calls for greater response mechanisms to cyber attacks within the European Union.

Possible BotNet uses

The flexibility of botnets is shown by many malicious applications that you can achieve with them:

- Distributed Denial-of-Service attacks
- Spamming
- Spreading malware
- Traffic sniffing
- Keylogging
- Identity theft

BotNet Architecture

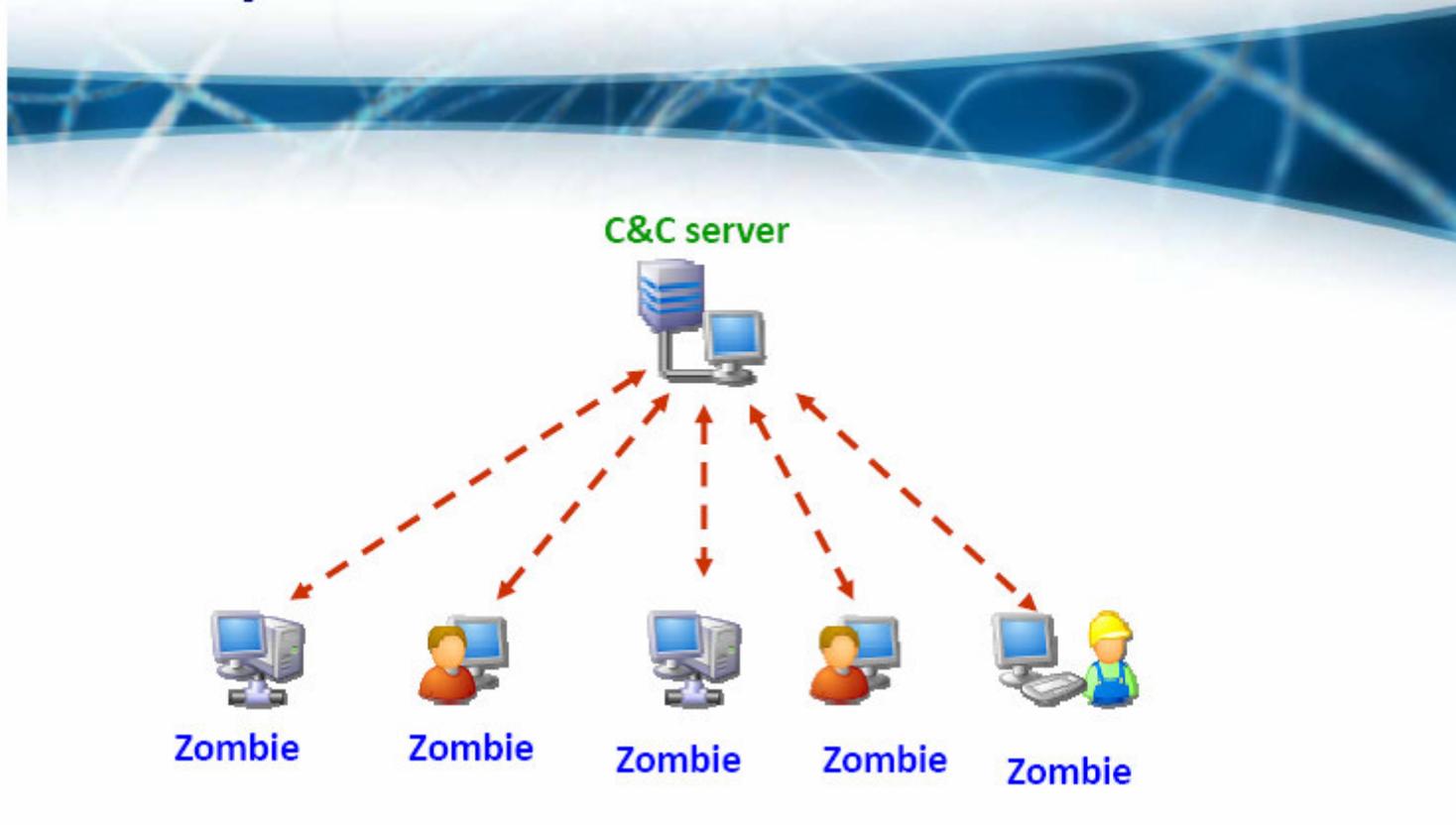
The communications in a botnet require three components:

- a sender,
- a channel,
- a receiver,

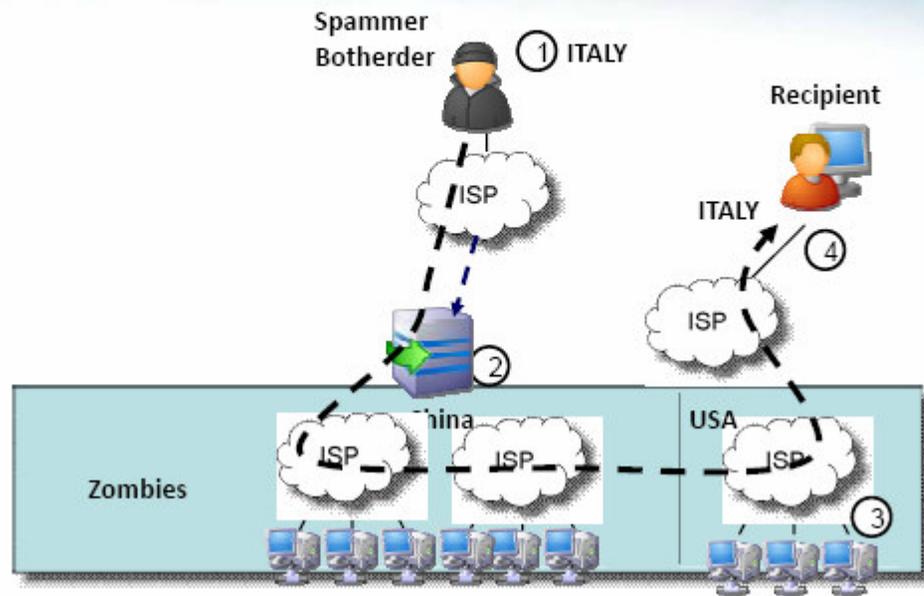
There are also several models of communication and control of a Bot networks, usually each has its advantages and its disadvantages.

We show now three of these models.

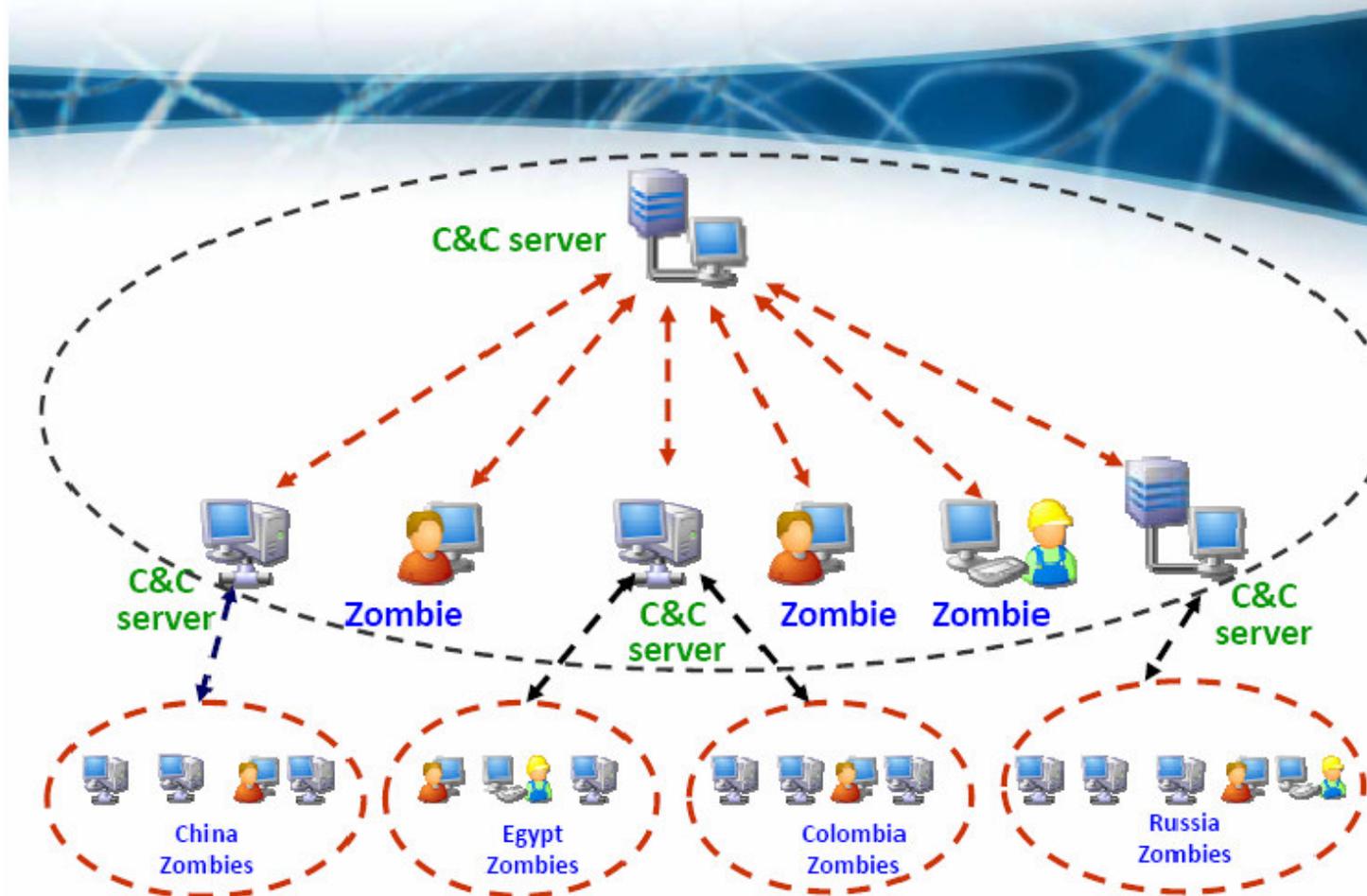
Many-to-one



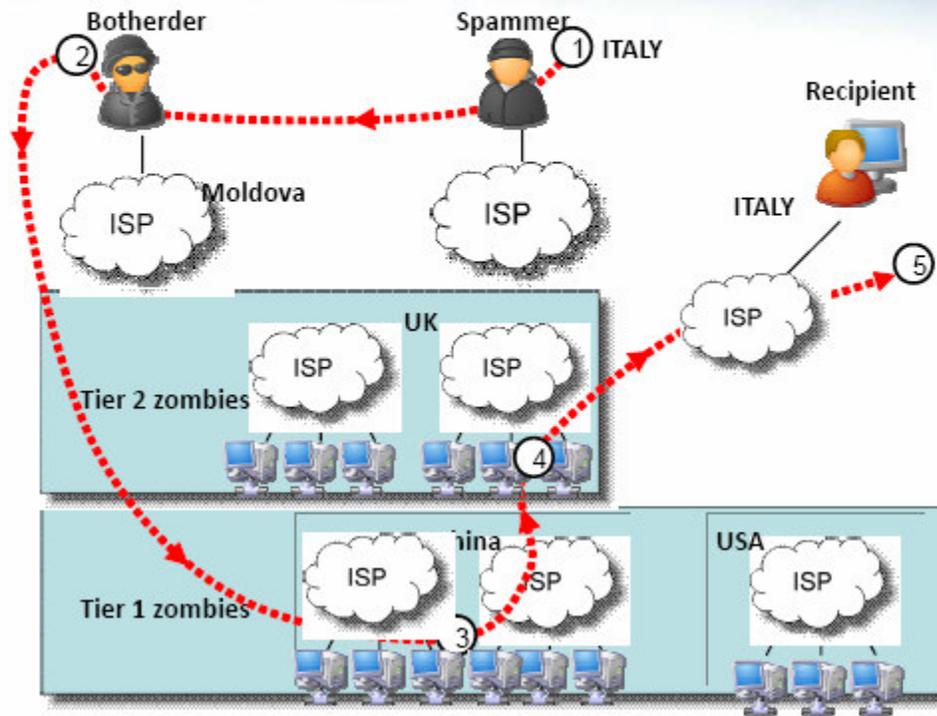
Spam method of distribution



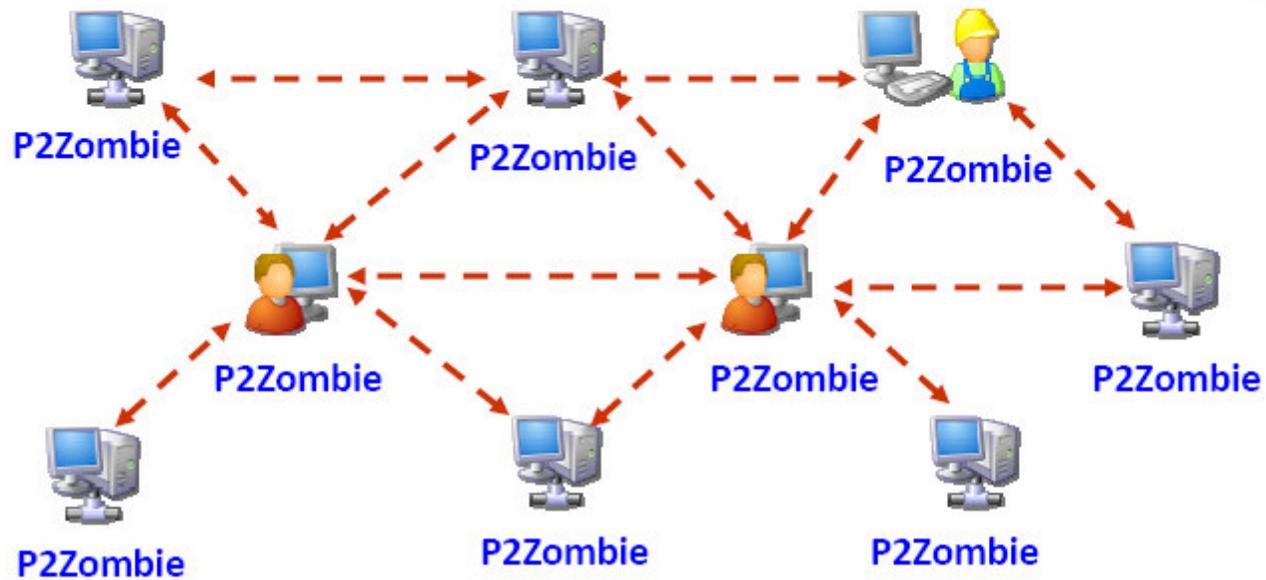
2-Tiers BotNet



Example: 2 Tiers Spam Distribution



Many-to-many



How to create a BotNet?

- Two methods are available to create a BotNet:
 - Standard, script-kiddie way
 - Creative, 31337 way

Botnet creation 4 dummies

- **All you need to do is:**
 - Find a good Trojan Console (Agobot, Rbot, ecc...)
 - Define the behavior through Gui options
 - Obfuscate the signature (automagically)
 - Compile the Trojan (better if Multistage)
 - Prepare a Channel on IRC or a Web site for Bot gathering
 - Diffuse the Trojan through P2P or Warez Sites
 - Enjoy

Botnet the 31337's way

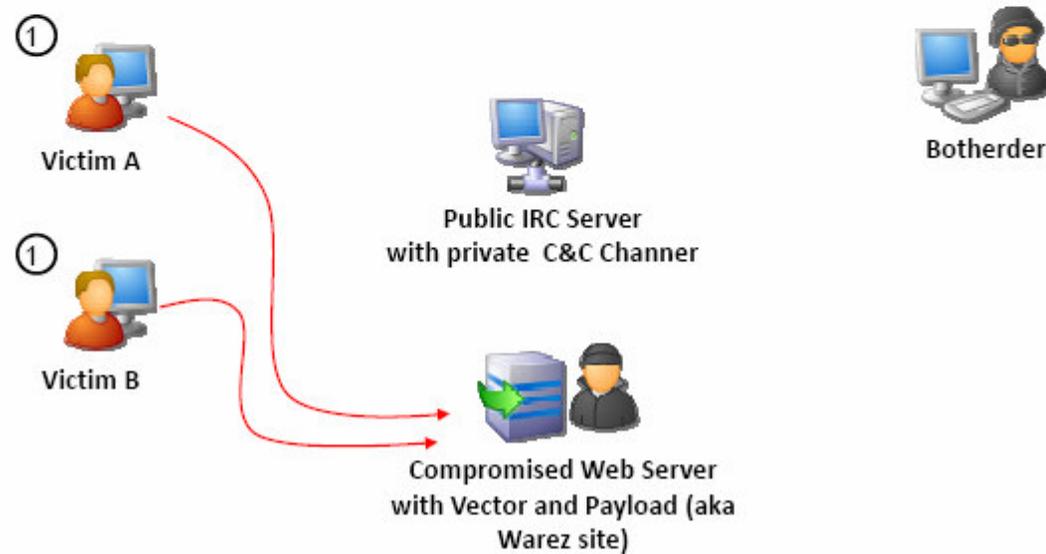
- An 31337 cr3w could do worst...
 - Develop a 0-day exploit (if needed) or modify an existing one
 - Code it into a multistage trojan
 - Compile it and pack it with Morphine or UPX
 - Diffuse it through P2P, Warez, Chat, etc...
 - Organize the Bot-gathering
 - Sell the Botnet on the market or use it for fun

The Scenario for the “practice” ...

- **And now, let's begin the scenario...**
- We use 2 newly installed computer with service packs and commercial Antiviruses.
- A C&C computer with IRC Server installed on.
- A “third party” web server with the exploit code and the bot code (taken from Gaobot family and partially rewritten by us).

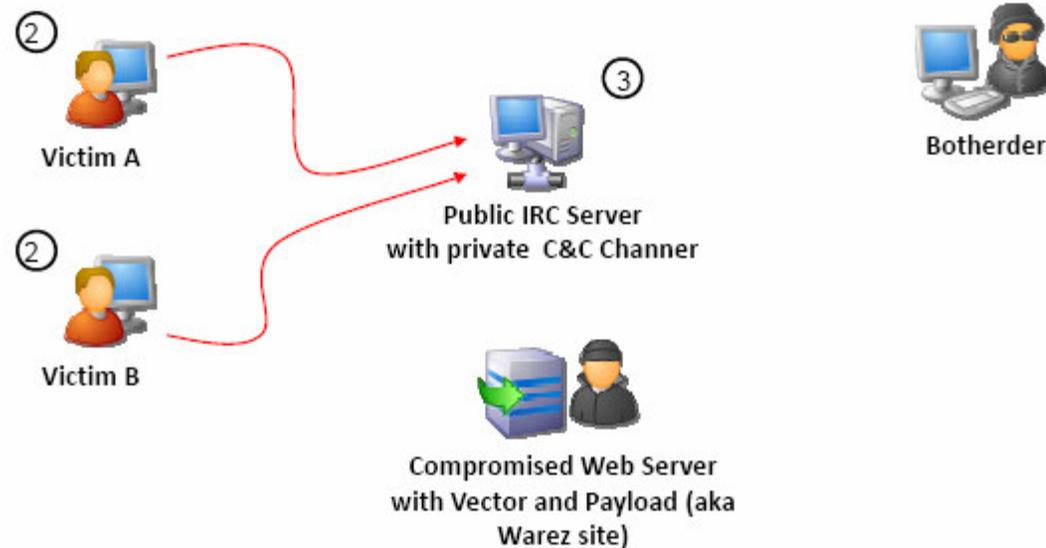
The Scenario

- ① Download of a "Warez" software (Vector and Payload)



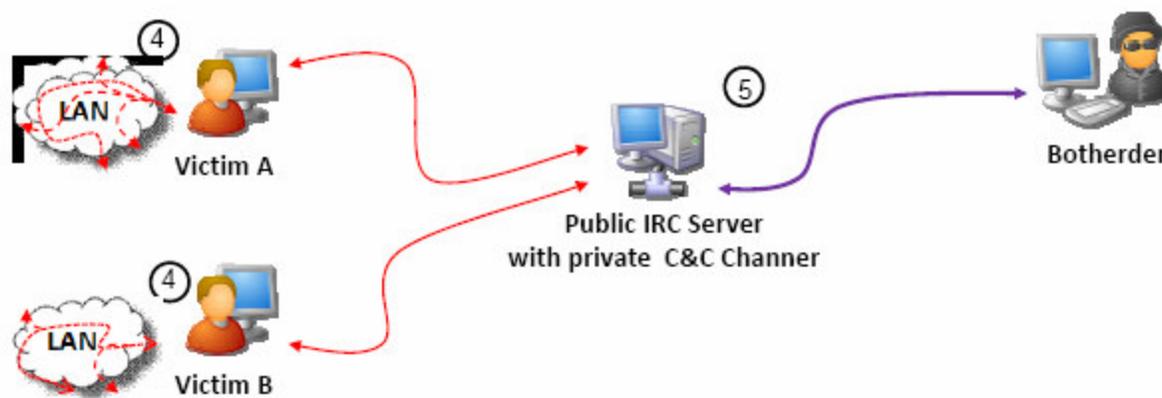
The Scenario

- ② Execution of the software (Bot installed – phase 1)
- ③ Connection to C&C Server (Bot installed – phase 1)



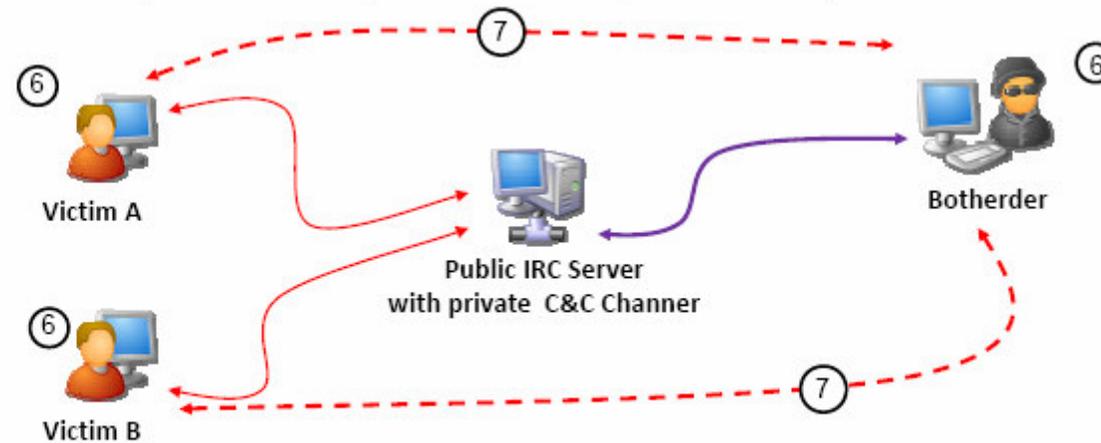
The Scenario

- ④ Local Network Scanning (Bot installed – phase 1 or 2)
- ⑤ Botherder C&C remote control activation (Bot installed – phase 2)



The Scenario

- ⑥ Decision to upgrade/install more software (Bot installed – phase 2)
- ⑦ Botherder's complete control (Bot installed – phase 2 or 3)



So Long, and Thanks for All the Fish...

- So Long, and Thanks for All the Fish¹...

¹ http://en.wikipedia.org/wiki/So_Long,_and_Thanks_For_All_the_Fish

BOTNET: Information Warfare

Black Sun Factory
RED TEAM

Materiale sottoposto a licenza Creative Commons for Attribution-Noncommercial-No Derivative Works 3.0 Unported

