OWASP Stammtisch Frankfurt Sowas wie Botnetze – Die dunkle Gefahr der Zombie Armee

Marius Klimmek
Referent
Deloitte & Touche GmbH
mklimmek@deloitte.de

OWASP
28.05.2015

The OWASP Foundation
http://www.owasp.org

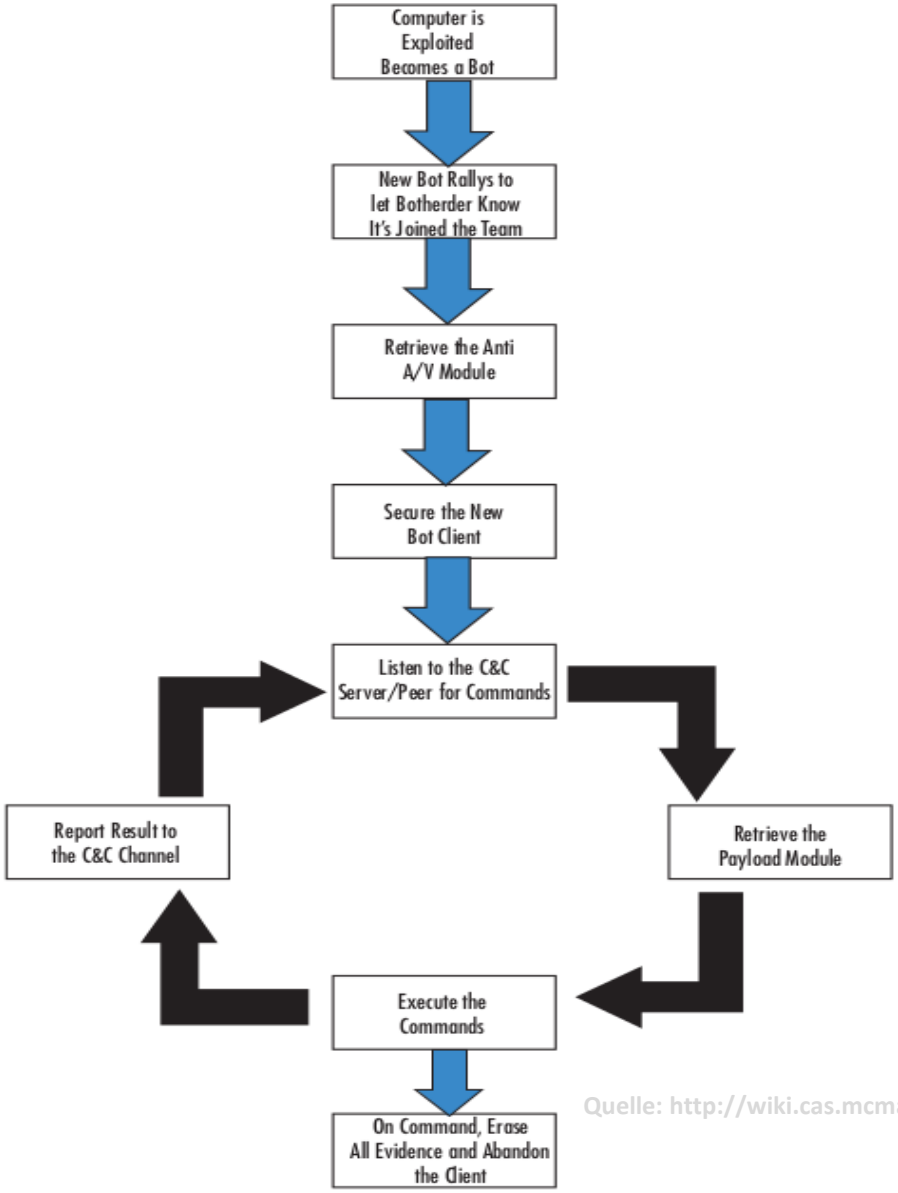
Agenda

- Gefahren und Grundlagen von Botnetzen
- Newsflash
- Botnetz Typen
- Evolution der Botnetze
- Vorstellung Zeus GameOver
- Framework
- Skripte
- Demonstration

Botnetze

Gefahren und Grundlagen von Botnetzen

Lifecycle eines Bots



Quelle: http://wiki.cas.mcmaster.ca/index.php/Bots_%26_Botnets

Gefahren durch Botnetze

- Distributed Denial of Service
- Spam-Mails, insbesondere Phishing-Mails
- Spionage, Spyware
- Betrug, Adware, Klickbetrug
- Bitcoins, Diebstahl sowie Bitcoin-Mining

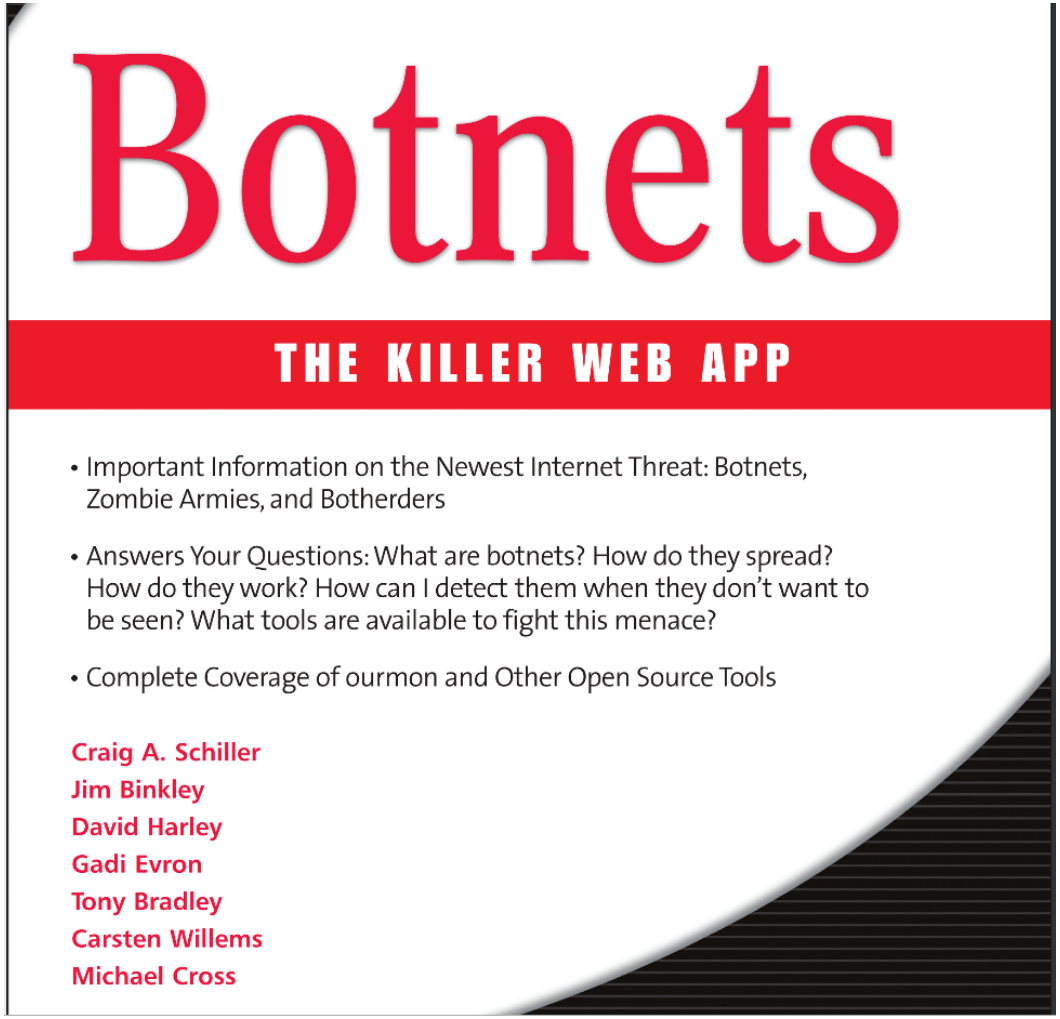
Grundlagen von Botnetzen

Quelle: https://de.wikipedia.org/wiki/Botnet

Botnetze

Newsflash

Newsflash



Quelle: https://www.elsevier.com/books/botnets/bradley/978-1-59749-135-8

Newsflash

26.09.2014 18:52

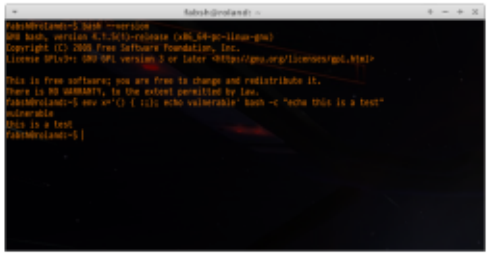
« Vorige | Nächste »

Alert!

Angriffe auf ShellShock-Lücke häufen sich

vorlesen / MP3-Download

Die kürzlich entdeckte Lücke in der Unix-Shell Bash wird nun von Angreifern aktive genutzt, um Webserver anzugreifen. Mittlerweile haben aber alle großen Linux-Distributionen ein zweites Update veröffentlicht, welches die Lücke entgültig stopfen soll.



Eine verwundbare Bash-Version unter Debian Squeeze

Die vor kurzem bekannt gewordene Bash-Lücke, in Anlehnung an den Ersten Weltkrieg unter dem Namen ShellShock bekannt, wird nun aktiv von Angreifern ausgenutzt, um Webserver anzugreifen. Auf GitHub ist Quellcode aufgetaucht, der es auch technisch weniger versierten Hackern erlaubt, verwundbare Systeme anzugreifen. Zudem verzeichnen mehrere Sicherheitsfirmen Angriffe auf Honeypot-Systemen. Auch heise Security liegen Log-Einträge vor, die nahelegen, dass Unbekannte versuchen, die Lücke auf Webservern anzugreifen. Ziel der Angriffe scheint es zu sein, die Zielrechner in Botnetze einzureihen.

Quelle: https://www.heise.de

Newsflash

22.01.2015 08:04

Technology Review « Vorige | Nächste »

Das Internet der (verräterischen) Dinge: Heimvernetzung weckt Interesse von Angreifern

vorlesen / MP3-Download

Intelligente Häuser und das Internet der Dinge gelten als wichtige Zukunftstrends. Wie erste Angriffe zeigen, achten die Hersteller dabei jedoch nicht genug auf die Sicherheit.

Anfang Januar lieferte der Sicherheitsforscher Brian Krebs eine interessante Information über das Bot-Netz Lizard Stresser, das kommerziell für Angriffe auf Webseiten angeboten wird: Anders als konventionelle Botnetze besteht es nicht aus Laptops und Desktop-Computern, sondern hauptsächlich aus geknackten Heimroutern. Nach einem Bericht von *Technology Review* könnte dies der Auftakt zu einer Welle von Angriffen über vernetzte Technik fürs Heim gewesen sein, die sich zunehmender Beliebtheit erfreut.

Quelle: https://www.heise.de

Newsflash

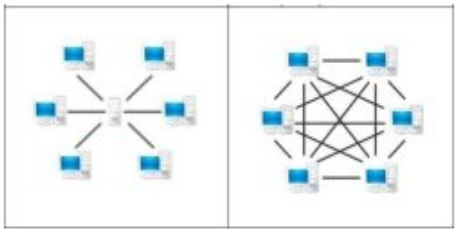
30.05.2013 17:18

« Vorige | Nächste »

P2P-Botnetze viel größer als vermutet

vorlesen / MP3-Download

Über eine Million infizierter Rechner kontrollieren die großen Bot-Netze ZeroAccess und Sality über Peer-to-Peer-Kommunikation; der bekannte Online-Banking-Trojaner Zeus bringt es immerhin auf knapp 200.000. Diese Werte ermittelte ein internationales Forscherteam, indem es sogenannte Sensoren in die Netze einschleuste. Außerdem zeigten sich die P2P-Botnetze deutlich widerstandsfähiger gegen Versuche, sie durch gezielte Eingriffe lahm zu legen, als bisher angenommen wurde.



Bei einem Peer-to-Peer-Netz genügt es nicht mehr, einen einzelnen Server stillzulegen, um die Kommunikation vollständig zu unterbrechen.

Herkömmliche Bot-Netze erhalten ihre Befehle durch einen zentralen Command&Control-Server, der damit auch ihre zentrale Schwachstelle darstellt. Gelingt es, den auszuschalten, hat der Botnetz-Master die Kontrolle über die infizierten Rechner verloren. Deshalb setzen neuere Botnetze bereits seit einiger Zeit auf dezentrale Peer-to-Peer-Strukturen, wie sie etwa auch in Filesharing-Netzen zum Einsatz kommen. Dabei vernetzen sich die infizierten Systeme untereinander; jeder Zombie-PC hat dazu eine Liste von unmittelbaren Kommunikationspartnern, den Peers, die ebenfalls zum gleichen Botnetz gehören.

Quelle: https://www.heise.de

Newsflash

05.06.2014 17:30

« Vorige | Nächste »

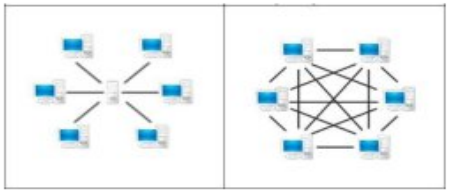
Security-Experten isolierten über 2 Millionen Gameover-Bots

vorlesen / MP3-Download

Im Rahmen der Aktionen gegen das Botnetz Gameover Zeus musste ein riesige Peer-to-Peer-Netz ausgeschaltet werden. Über zwei Millionen infizierte Rechner mussten dazu manipuliert werden.

Anfang Juni legten FBI, Europol und einige IT-Security-Firmen das Gameover-Zeus-Botnetz lahm. Insgesamt über 2 Millionen Rechner waren mit der auf Online-Banking-Betrug spezialisierten Schad-Software infiziert und mussten aufwendig isoliert werden.

Die Gameover-Variante des Zeus-Trojaners (GoZ) setzt primär auf Peer-to-Peer-Kommunikation. Bei herkömmlichen Botnetzen, genügt es, die zentralen Command&Control-Server außer Betrieb zu nehmen, um die Kommunikation und die Verbreitung von Updates zu unterbinden. Ohne C&C-Server ist das Botnetz im wesentlichen tot. Anders bei Peer-to-Peer-Netzen: Hier pflegt jeder Bot eine Liste von anderen, ebenfalls infizierten Rechnern, mit denen er direkten Kontakt hält.

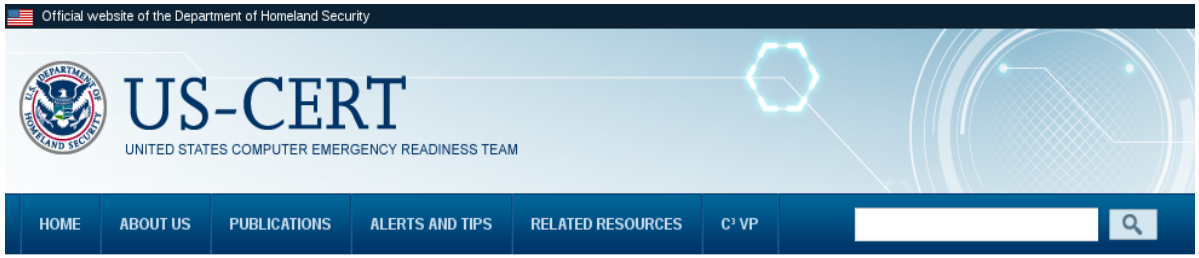


Bei einem Peer-to-Peer-Netz genügt es nicht mehr, einen einzelnen Server stillzulegen, um die Kommunikation vollständig zu unterbrechen.

Die Standard-Methode, solche P2P-Botnetze lahm zu legen, ist das sogenannte Sinkholing. Dabei vergiften die Botnetz-Jäger die Liste der Peers systematisch mit Einträgen eigener Rechner bis der Bot effektiv isoliert ist. Wie Crowd Strike beschreibt, gelang es ihnen, die GoZ-Bots mit solchen in das Bot-Netz eingeschleusten Peer-Listen zu isolieren und die P2P-Kommunikation lahm zu legen. Über die Grundlagen solcher Aktionen berichtete heise Security bereits in P2P-Botnetze viel größer als vermutet.

Quelle: https://www.heise.de

Newsflash



Alert (TA14-150A)

More Alerts

GameOver Zeus P2P Malware

Original release date: June 02, 2014 | Last revised: August 18, 2014

Print Tweet Send Share

Systems Affected

- Microsoft Windows 95, 98, Me, 2000, XP, Vista, 7, and 8
- Microsoft Server 2003, Server 2008, Server 2008 R2, and Server 2012

Overview

GameOver Zeus (GOZ), a peer-to-peer (P2P) variant of the Zeus family of bank credential-stealing malware identified in September 2011, [1] uses a decentralized network infrastructure of compromised personal computers and web servers to execute command-and-control. The United States Department of Homeland Security (DHS), in collaboration with the Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ), is releasing this Technical Alert to provide further information about the GameOver Zeus botnet.

Description

GOZ, which is often propagated through spam and phishing messages, is primarily used by cybercriminals to harvest banking information, such as login credentials, from a victim's computer. [2] Infected systems can also be used to engage in other malicious activities, such as sending spam or participating in distributed denial-of-service (DDoS) attacks.

Prior variants of the Zeus malware utilized a centralized command and control (C2) botnet infrastructure to execute commands. Centralized C2 servers are routinely tracked and blocked by the security community. [1] GOZ, however, utilizes a P2P network of infected hosts to communicate and distribute data, and employs encryption to evade detection. These peers act as a massive proxy network that is used to propagate binary updates, distribute configuration files, and to send stolen data. [3] Without a single point of failure, the resiliency of GOZ's P2P infrastructure makes takedown efforts more difficult. [1]

Impact

A system infected with GOZ may be employed to send spam, participate in DDoS attacks, and harvest users' credentials for online services, including banking services.

Quelle: https://www.us-cert.gov/

Newsflash

THE FBI FEDERAL BUREAU OF INVESTIGATION

CONTACT US | ABOUT US | MOST WANTED | NEWS | STAT

Stories

Home • News • Stories • 2012 • January • 'Gameover' Malware Targets Bank Accounts

Twitter (227) Facebook (1,716) Share

Malware Targets Bank Accounts
'Gameover' Delivered via Phishing E-Mails

01/06/12

Cyber criminals have found yet another way to steal your hard-earned money: a recent phishing scheme involves spam e-mails—purportedly from the National Automated Clearing House Association (NACHA), the Federal Reserve Bank, or the Federal Deposit Insurance Corporation (FDIC)—that can infect recipients' computers with malware and allow access to their bank accounts.

The malware is appropriately called "Gameover" because once it's on your computer, it can steal usernames and passwords and defeat common methods of user authentication employed by financial institutions. And once the crooks get into your bank account, it's definitely "game over."

Gameover is a newer variant of the Zeus malware, which was created several years ago and specifically targeted banking information.

How the scheme works: Typically, you receive an unsolicited e-mail from NACHA, the Federal Reserve, or the FDIC telling you that there's a problem with your bank account or a recent ACH transaction. (ACH stands for Automated Clearing House, a network for a wide variety of financial transactions in the United States.) The sender includes a link in the e-mail that will supposedly help you resolve whatever the issue is. Unfortunately, the link goes to a phony website, and once you're there, you inadvertently download the Gameover malware, which promptly infects your computer and steals your banking information.

After the perpetrators access your account, they conduct what's called a distributed denial of service, or DDoS, attack using a botnet, which involves multiple computers flooding the financial institution's server with traffic in an effort to deny legitimate users access to the site—probably in an attempt to deflect attention from what the bad guys are doing.

How Can You Protect Yourself?

- Obviously, make sure your computer's anti-virus software is up to date.

- Don't click on e-mail attachments from unsolicited senders. NACHA, FDIC, and the Federal Reserve all say they don't send out unsolicited e-mails to bank

Quelle: https://www.fbi.gov

Newsflash

08.08.2014 15:43

« Vorige | Nächste »

Zeus-Trojaner: Ein Hacker dreht den Spieß um

vorlesen / MP3-Download

Was Sicherheitsforscher so machen, wenn sie Langeweile haben? Zum Beispiel einen Zeus-Trojaner auseinander nehmen und den Botnetz-Master mit seiner eigenen Webcam fotografieren.

Raashid Bhat hat den im Anhang einer Mail enthaltenen Zeus-Trojaner analysiert und die gewonnenen Informationen konsequent genutzt. So kaperte er nicht nur den Kontroll-Server des Bot-Netzes sondern präsentiert in seiner Analyse auch noch ein Foto, das durchaus den Botnetz-Master vor seinem Rechner zeigen könnte.

In der an die E-Mail angehängten ZIP-Datei mit einem angeblichen Bild fand sich – wie kaum anders zu erwarten – eine EXE-Datei namens `image.scr`. Der Debugger und Dissassembler IDA Pro verriet schnell, dass es sich um eine Variante des Online-Banking-Trojaners Zeus handelte. Dessen weitere Analyse bescherte dem Forscher die IP-Adresse des Command&Control-Servers (C2C) und einen RC4-Schlüssel für die Kommunikation mit selbigem.

Ein Botnetz-Master bei der Arbeit?
Bild: Raashid Bhat

Über eine bekannte Sicherheitslücke bestimmter Zeus-Versionen – auch Kriminelle spielen offenbar keine Updates ein – konnte Bhat in der C2C-Web-Applikation eigenen PHP-Code einschleusen und ausführen. Die Lücke beruht darauf, dass der infizierte Client Dateien auf den C2C-Server hochlädt, was sich ausnutzen lässt, eine PHP-Datei dort zu platzieren.

Im weiteren wird die Beschreibung etwas vage. Wenn man es drauf anlegt, könnte man demnach dem Botnetz-Master bei seinem nächsten Login auf den C&C-Server einen speziellen Metasploit-Exploit unterjubeln. Wenn man das etwa mit dem Meterpreter-Befehl `webcam_snap` tun würde, landete beim nächsten Login des Botnetz-Masters ein Schnappschuss von dessen Webcam auf dem PC des vermeintlichen Opfers. Ob das darunter abgebildete Konterfei tatsächlich einer solchen Aktion entsprang, lässt Bhat jedoch wohlweislich offen. (ju)

Quelle: https://www.heise.de

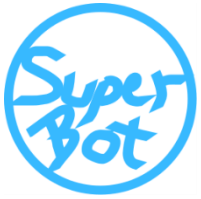
Botnetze

Botnetz Typen

Botnetz Typen

- Bot/Zombie
- Bots führen Angriffe aus
- Rechner werden ausspioniert

- Master/C&C-Server/CnC-Server/C2-Server
- Hat die Kontrolle über das komplette Botnetz
- Verteilt Befehle



- Superbot/Proxybot
- Mittelschicht zwischen Bot und Master
- Absicherung des Masters
- Datensammelstelle

Botnetz Typen

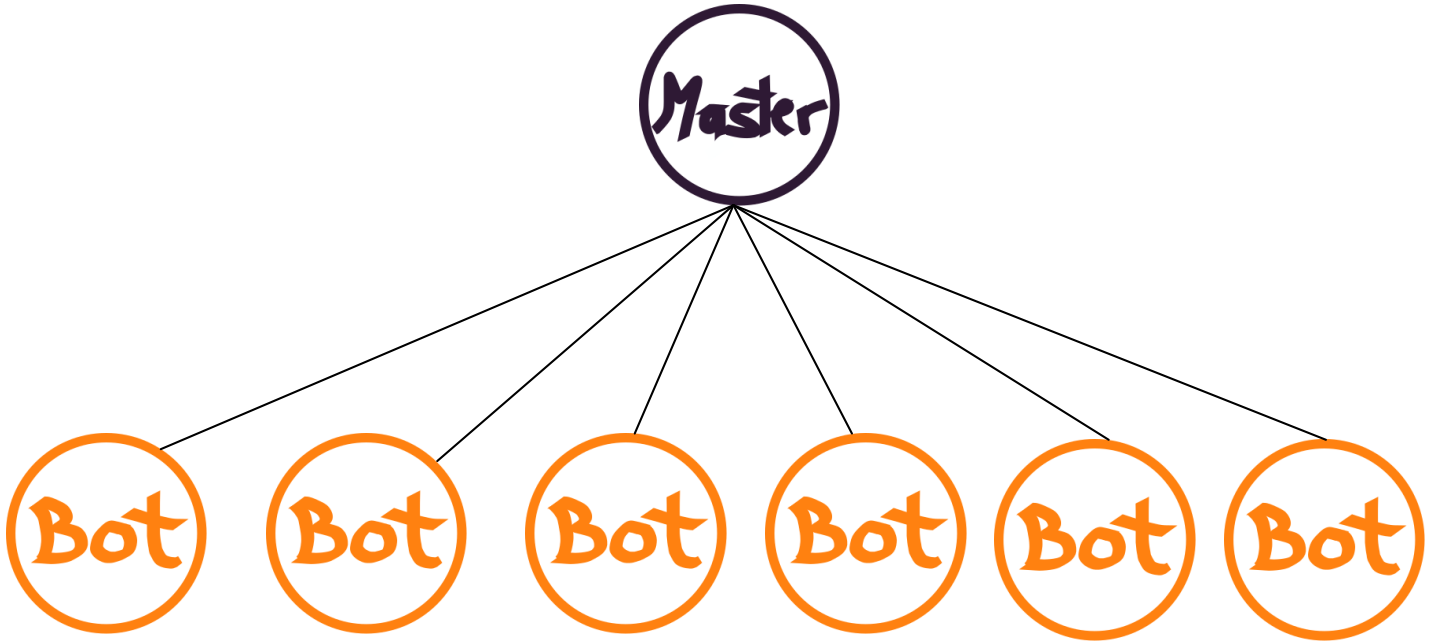
- Bootstrap/Rendevouz-Point
- Anlaufstelle von Bots
- Liste mit Bots steht zur Verteilung bereit

- Target/Opfer
- Angriffsvektoren

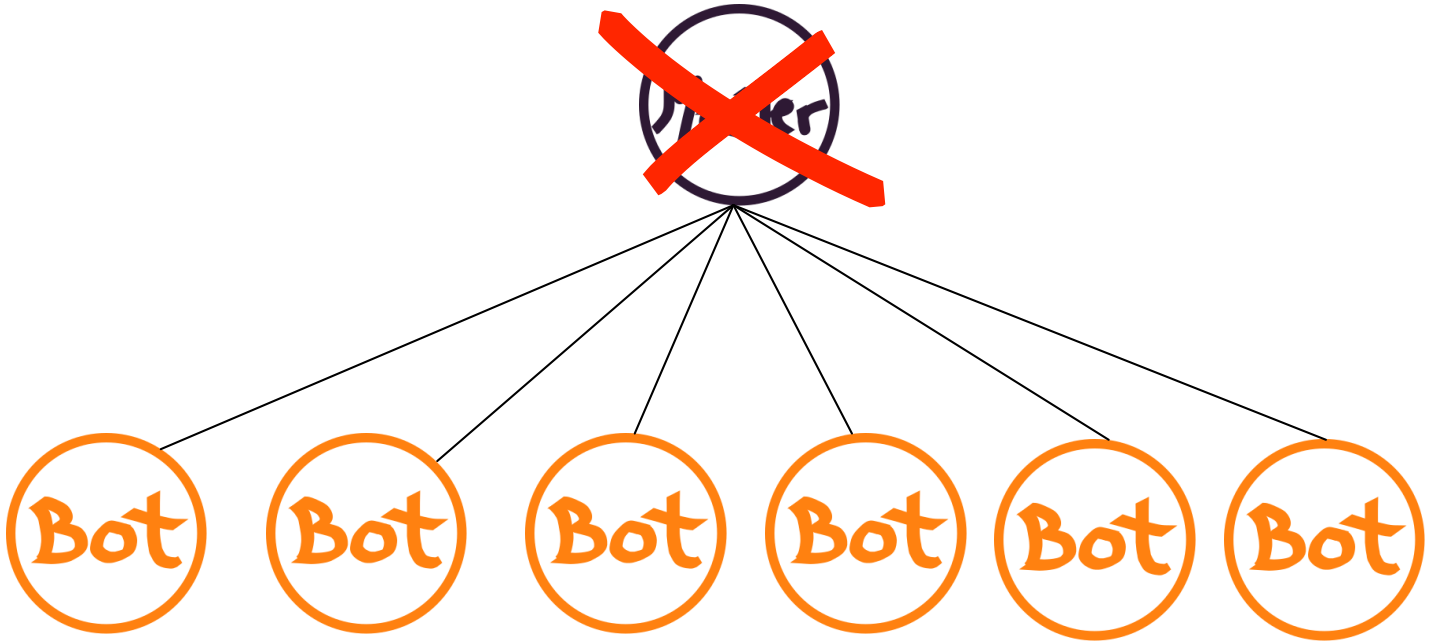
Botnetze

Evolution der Botnetze

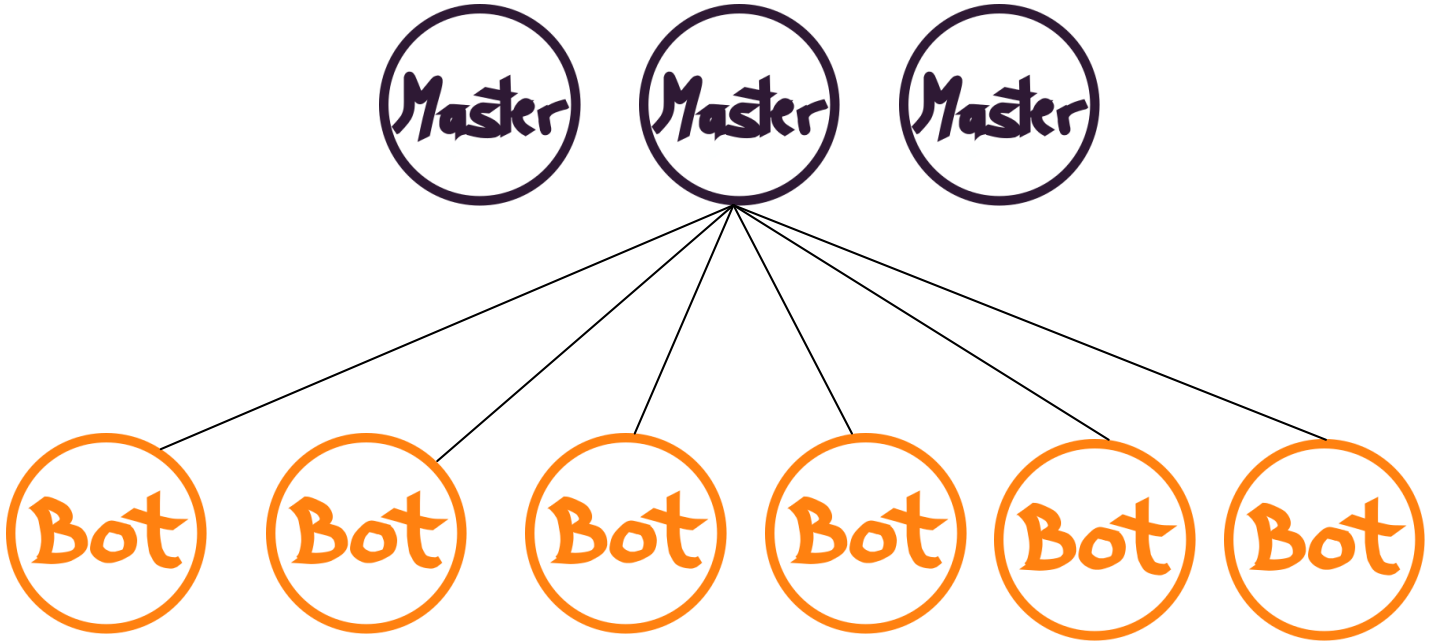
Evolution der Botnetze



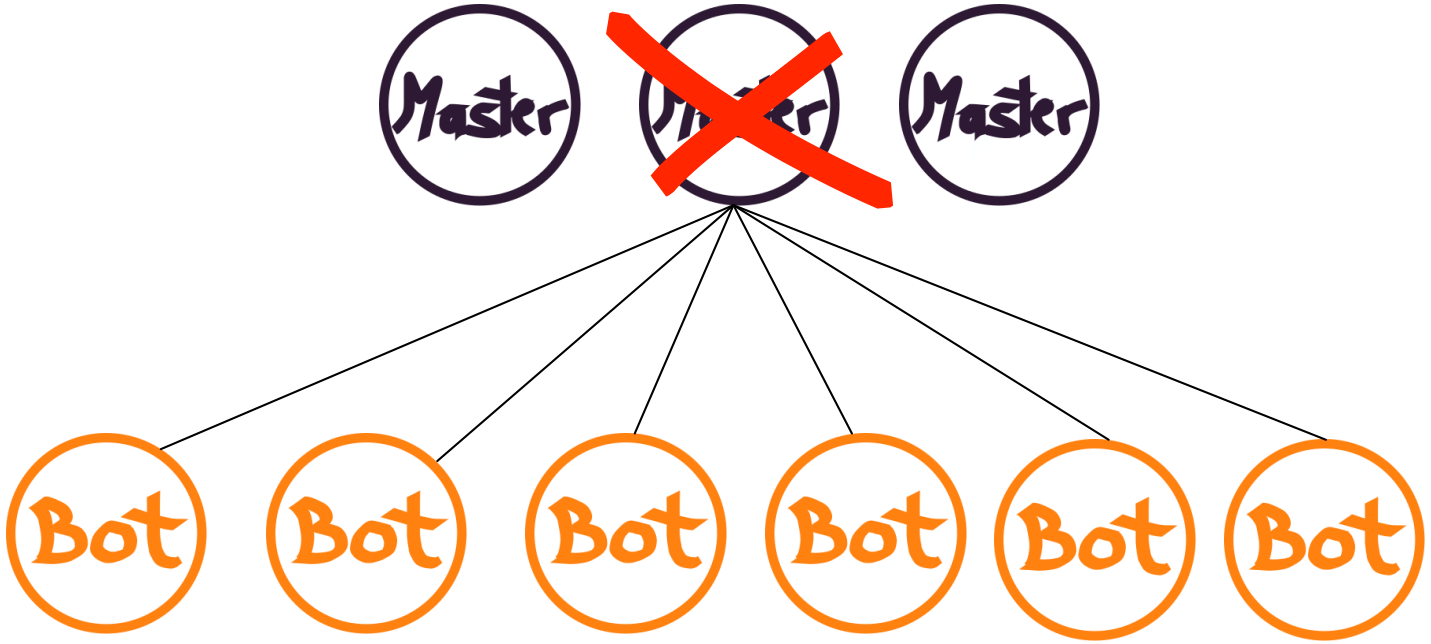
Evolution der Botnetze



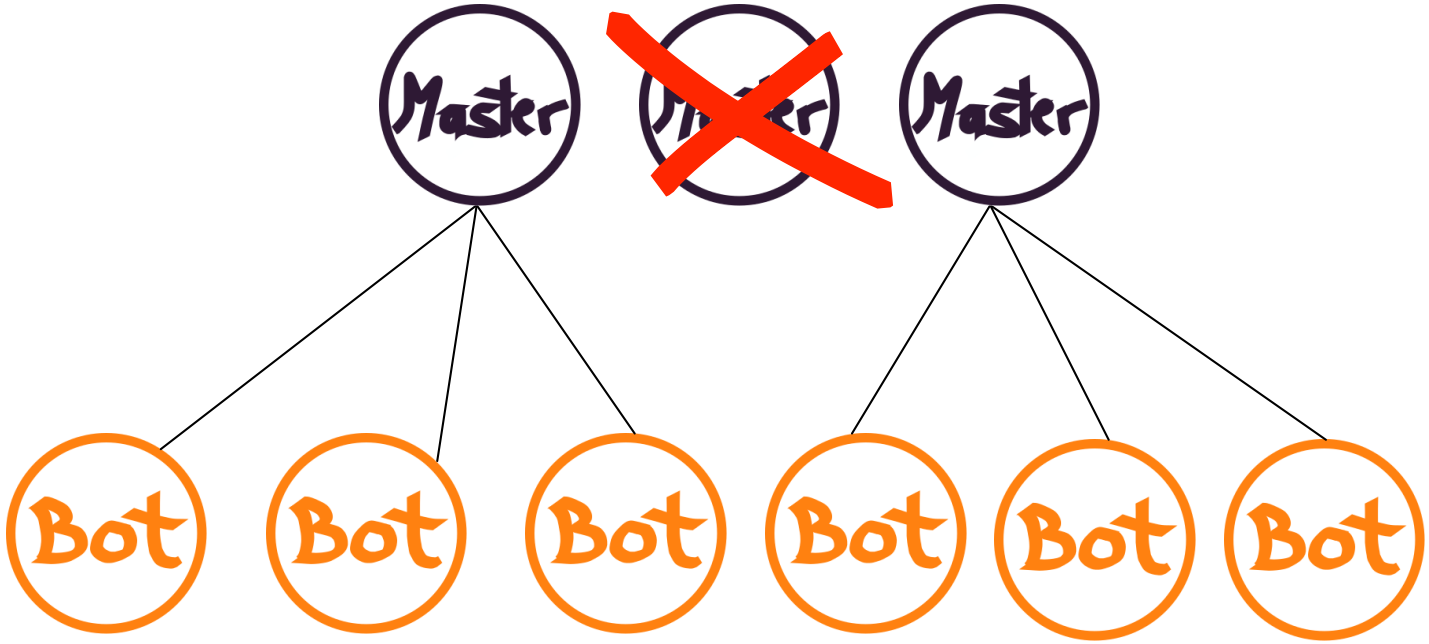
Evolution der Botnetze



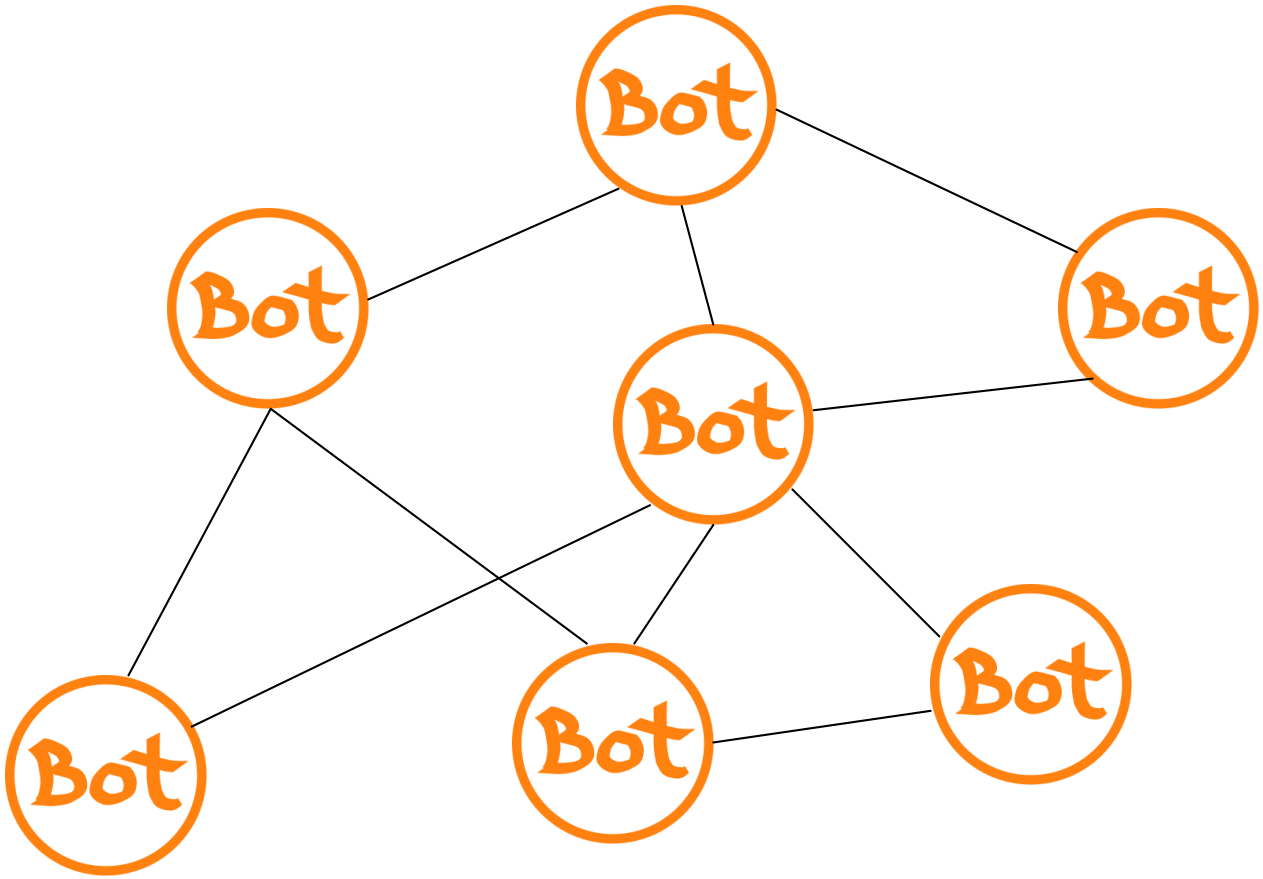
Evolution der Botnetze



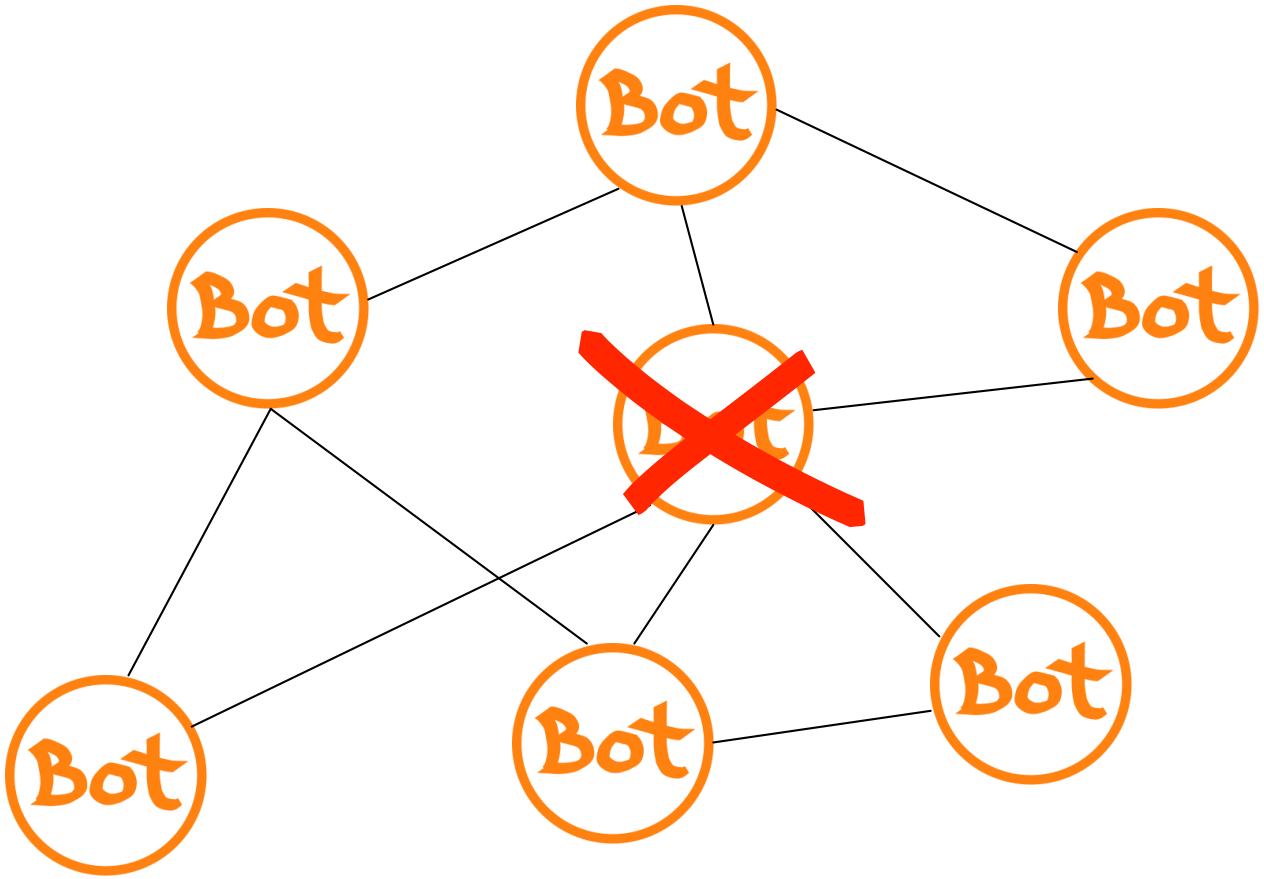
Evolution der Botnetze



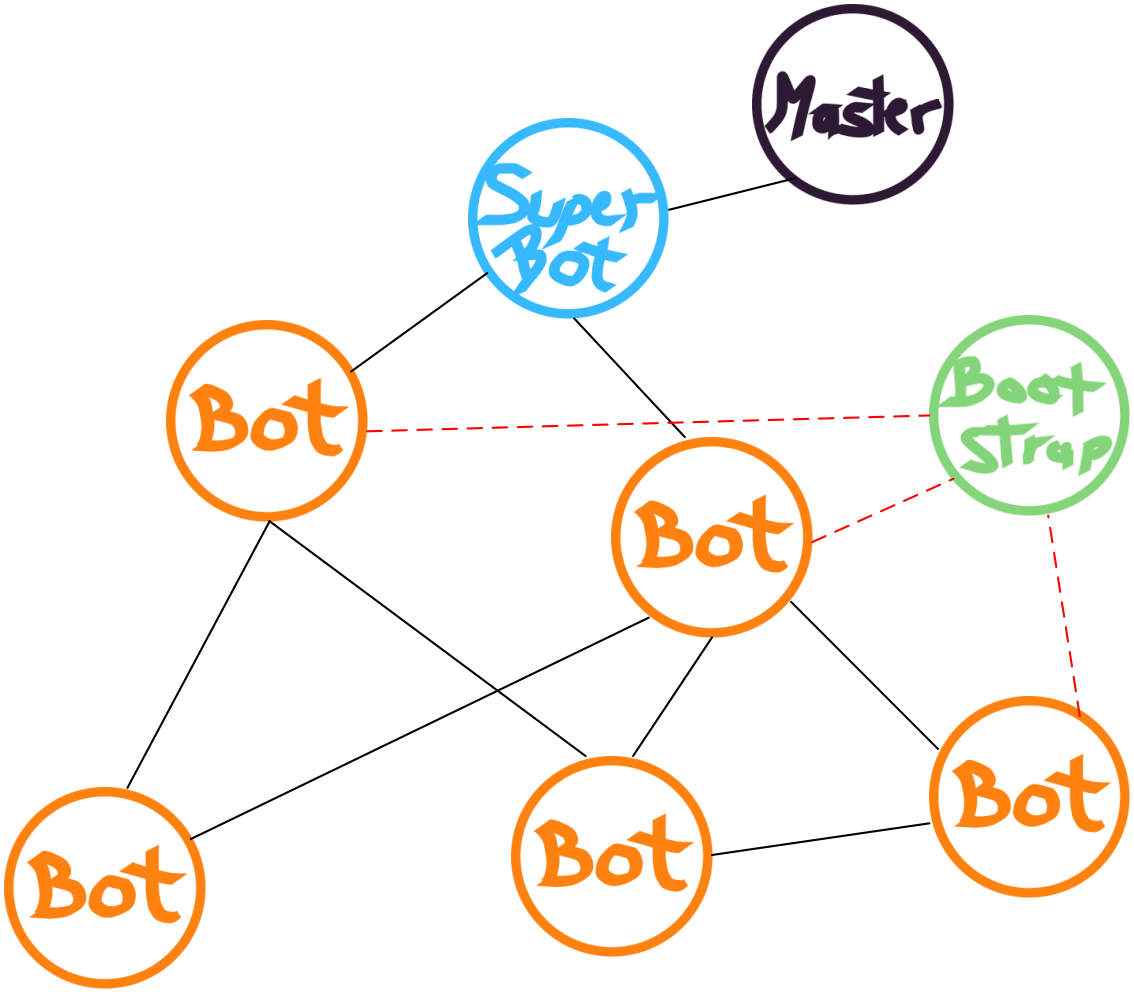
Evolution der Botnetze



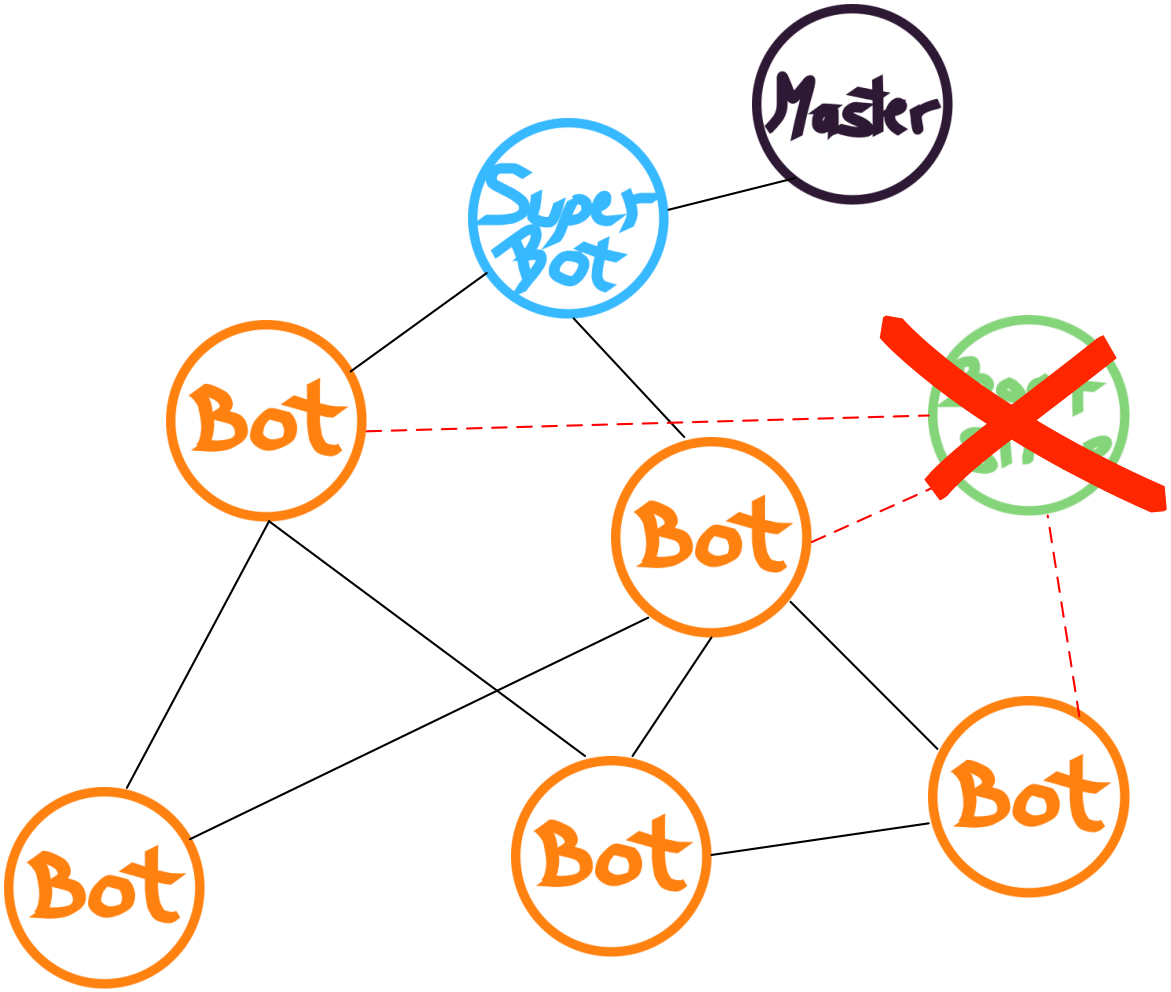
Evolution der Botnetze



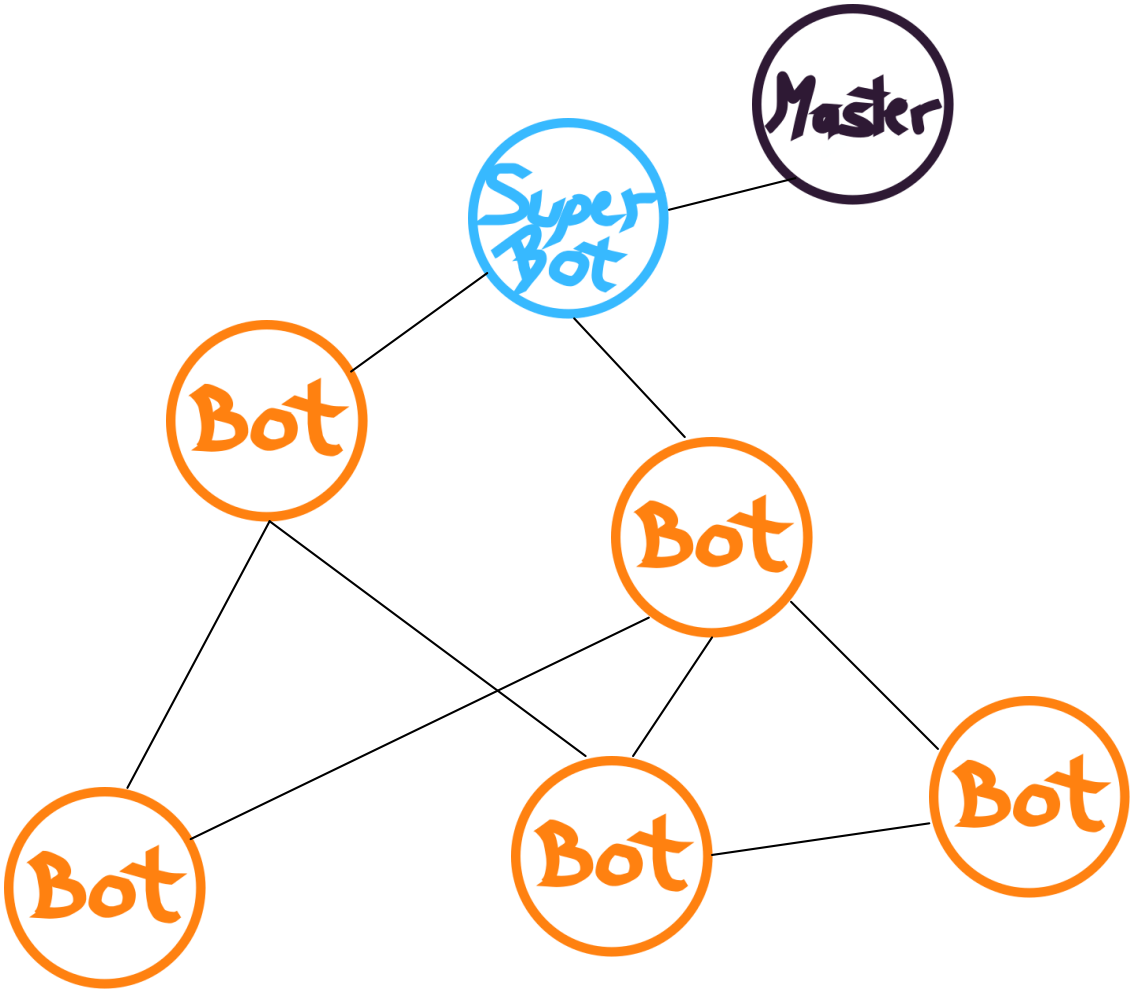
Evolution der Botnetze



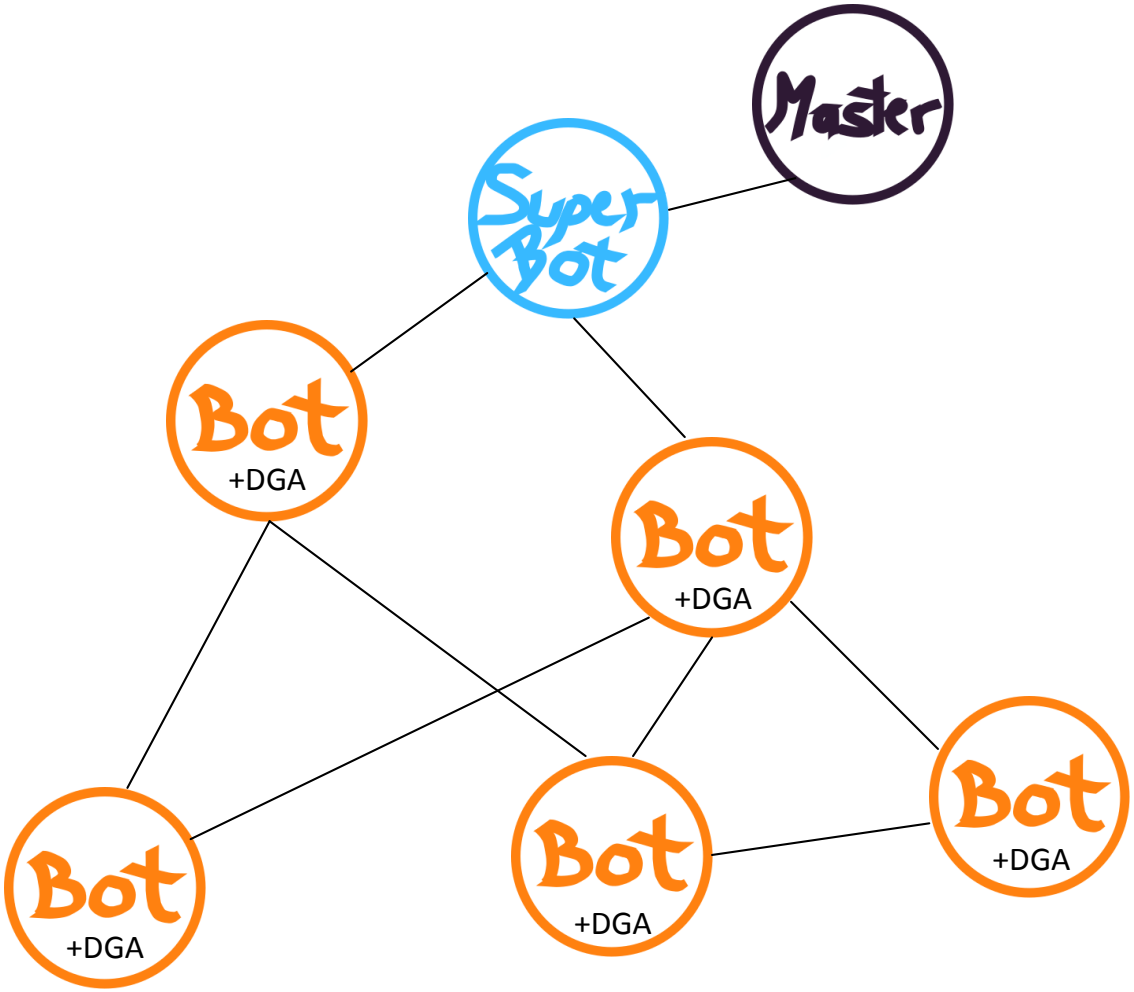
Evolution der Botnetze



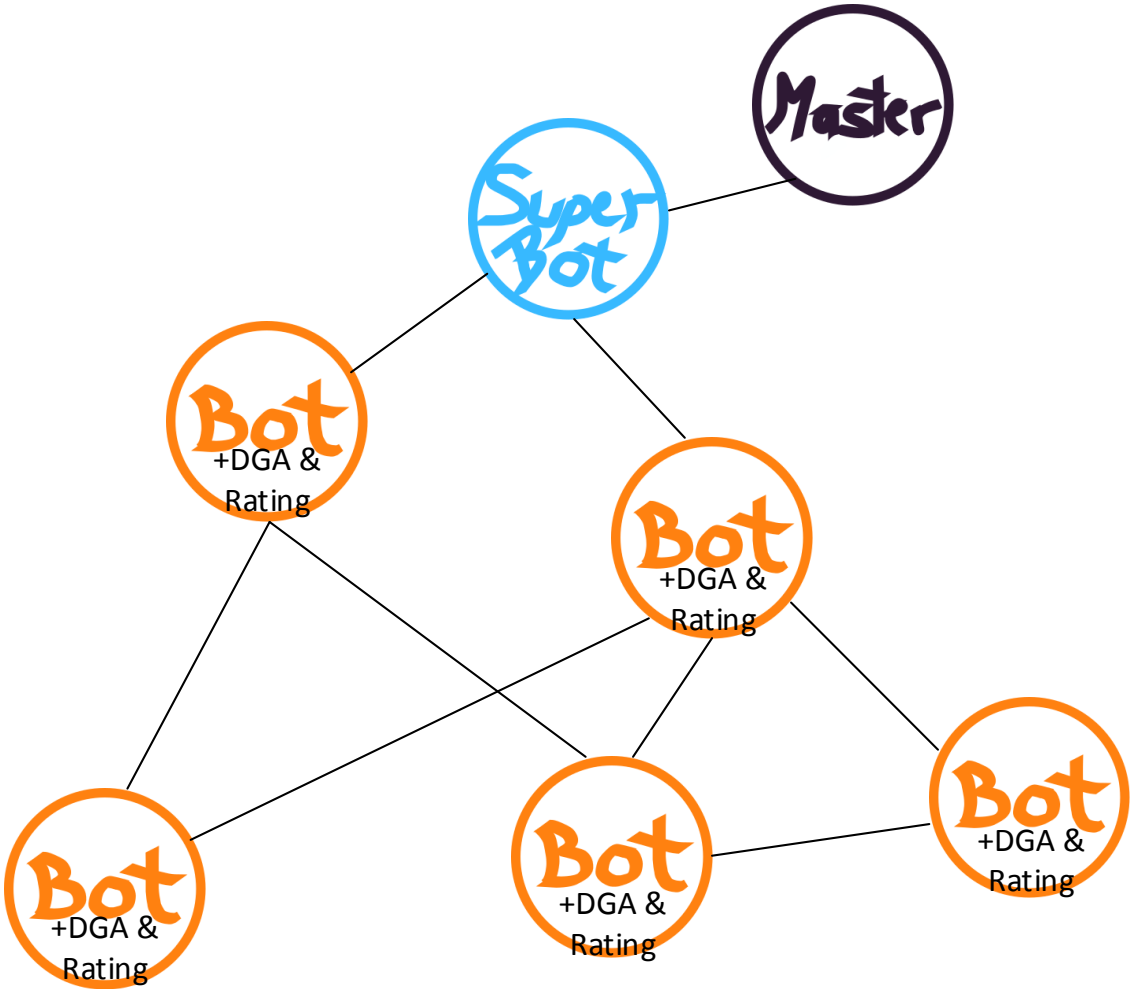
Evolution der Botnetze



Evolution der Botnetze



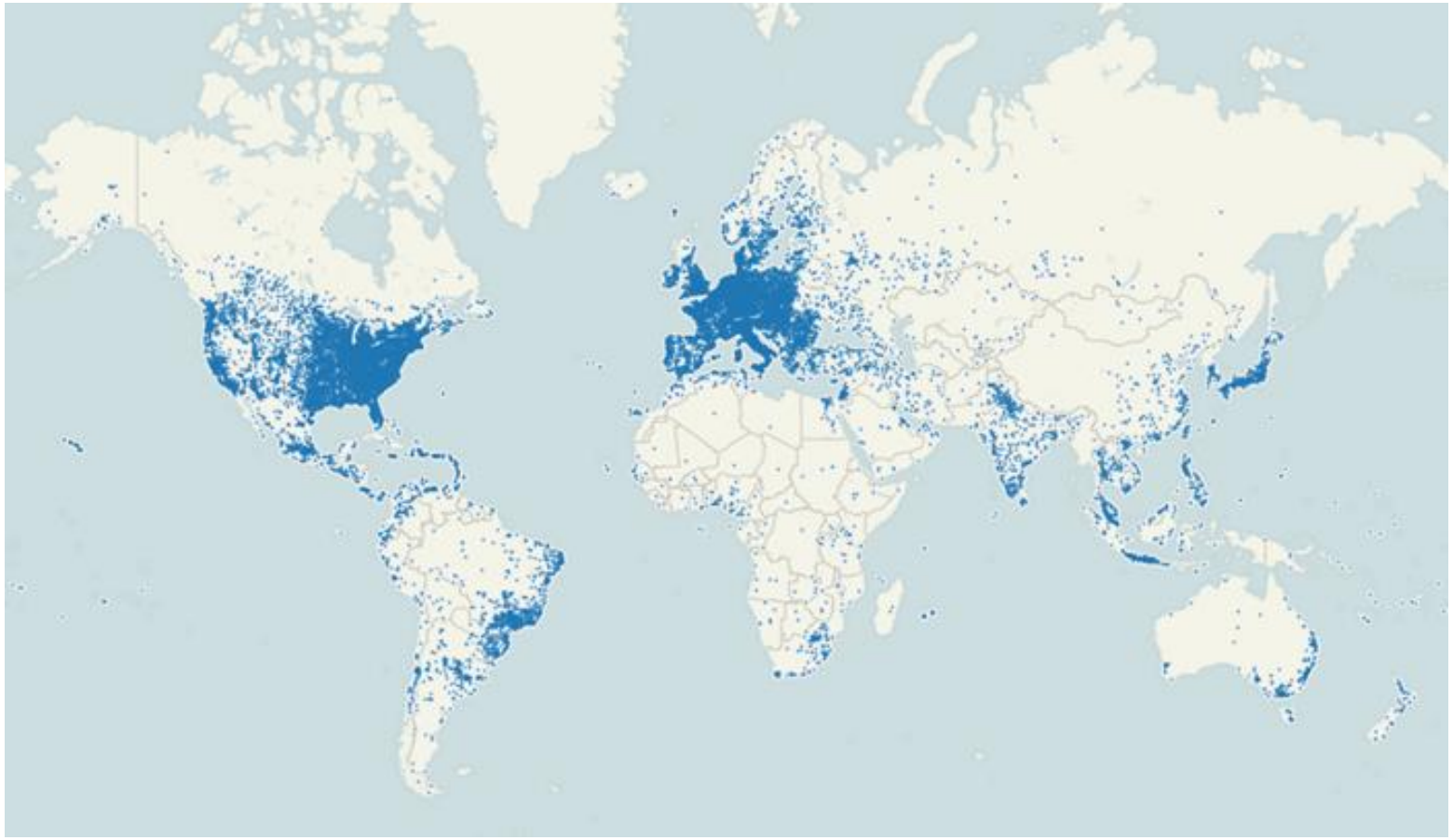
Evolution der Botnetze



Botnetze

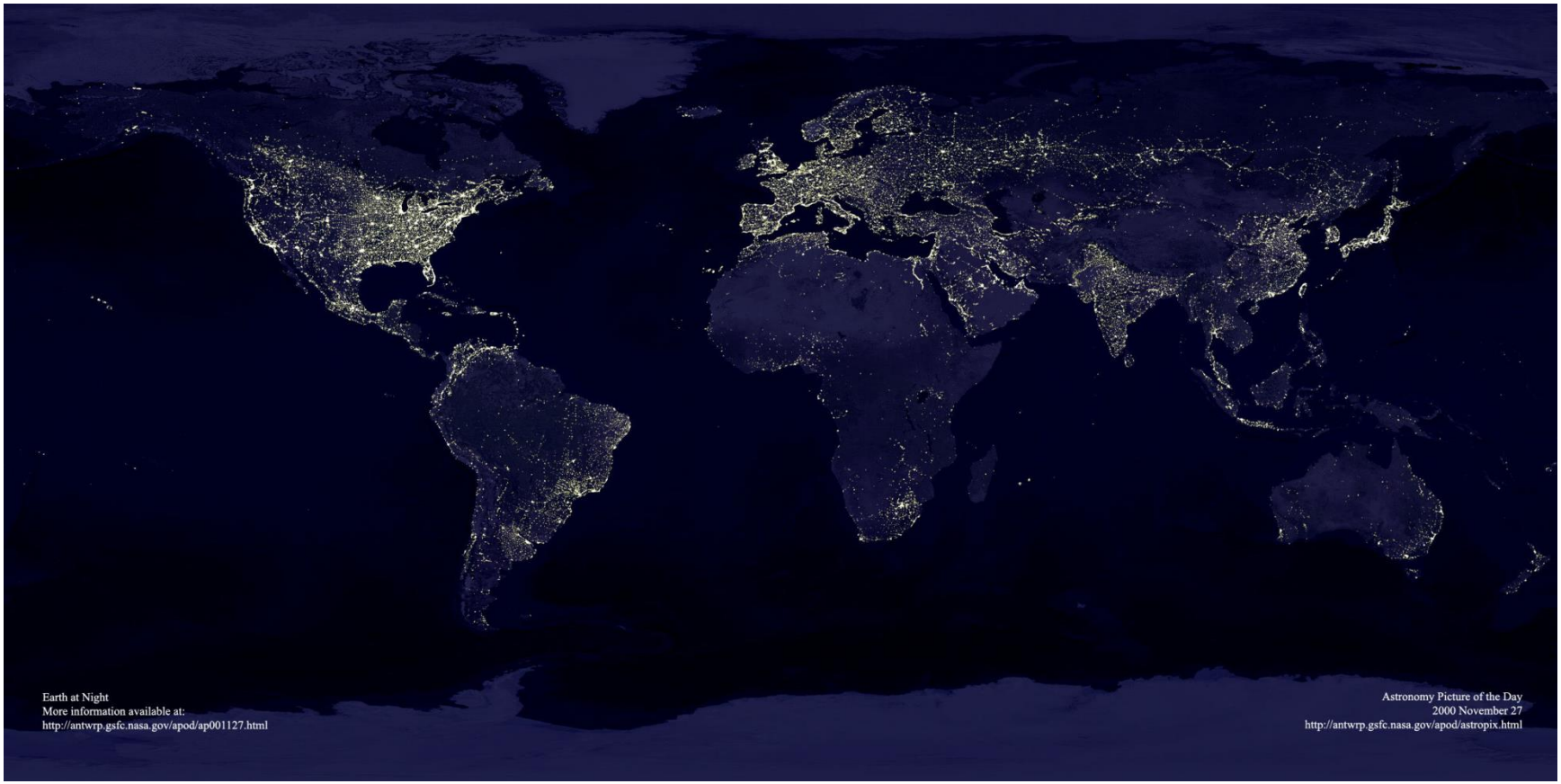
Vorstellung Zeus GameOver

Ausbreitung



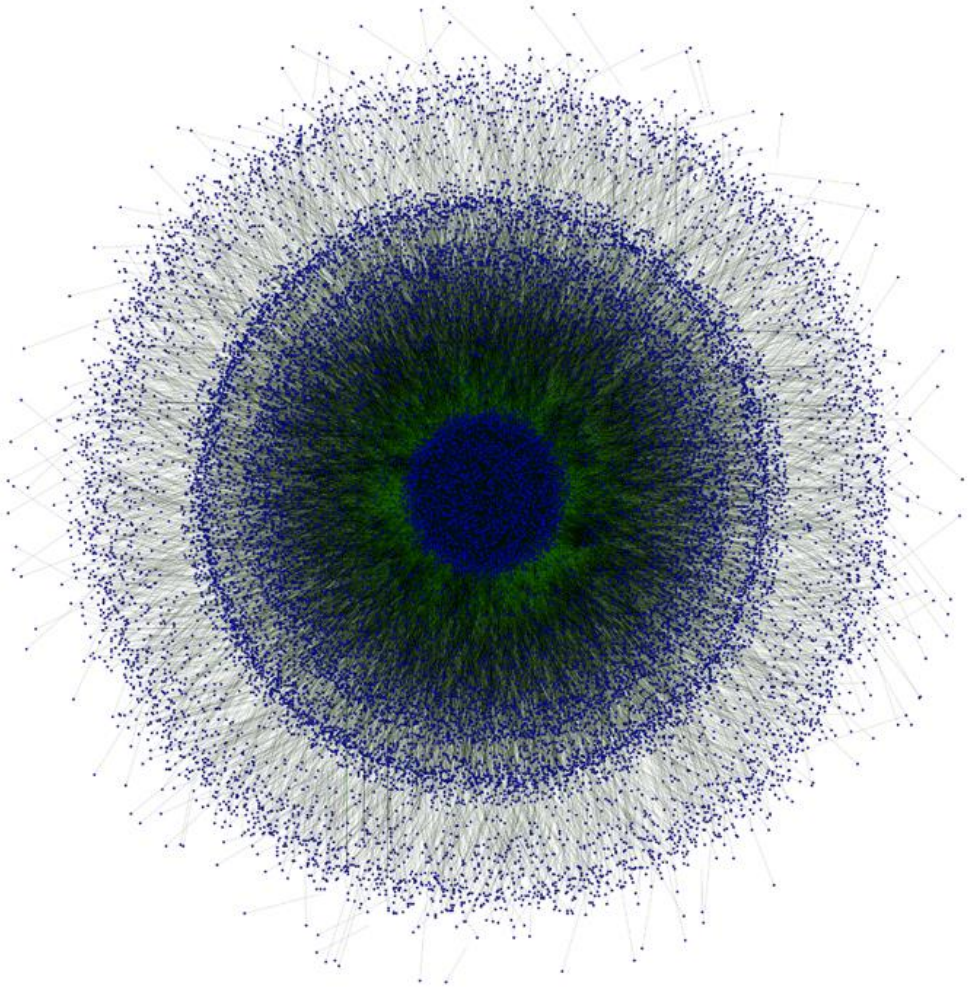
Quelle: http://www.secureworks.com/cyber-threat-intelligence/threats/The_Lifecycle_of_Peer_to_Peer_Gameover_ZeuS/

Unsere Erde bei Nacht vs. Ausbreitung II



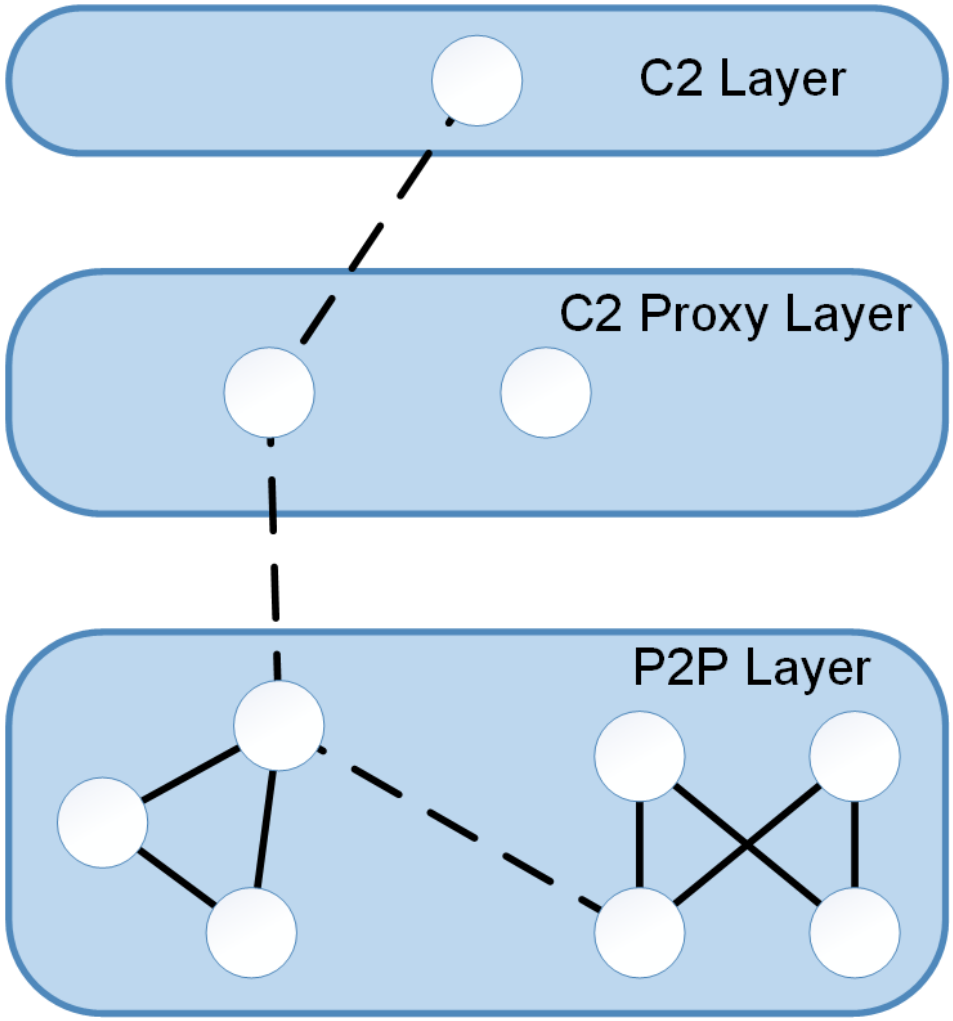
Quelle: http://images.die-erde.com/erde/earthlights2_dmsp_big.jpe

Visuelle Darstellung



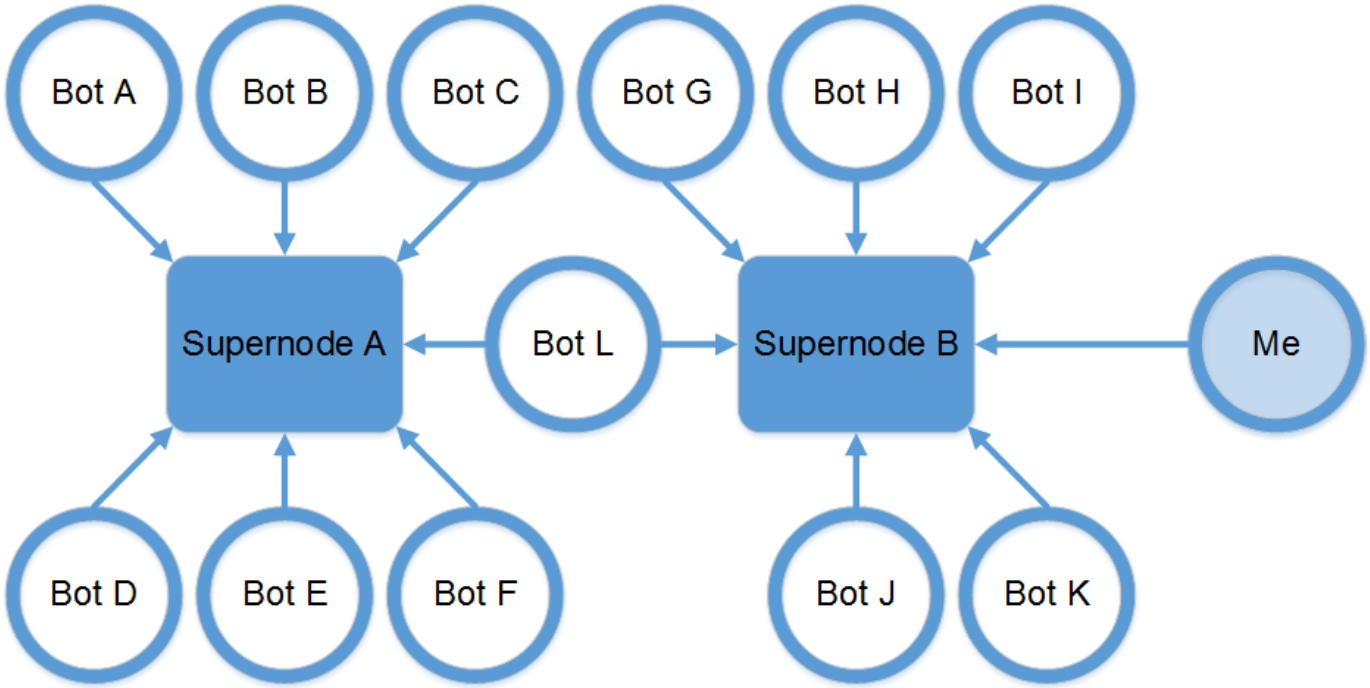
Quelle: http://krebsonsecurity.com/wp-content/uploads/2014/06/gameoverp2p.png

Netzwerktopologie I

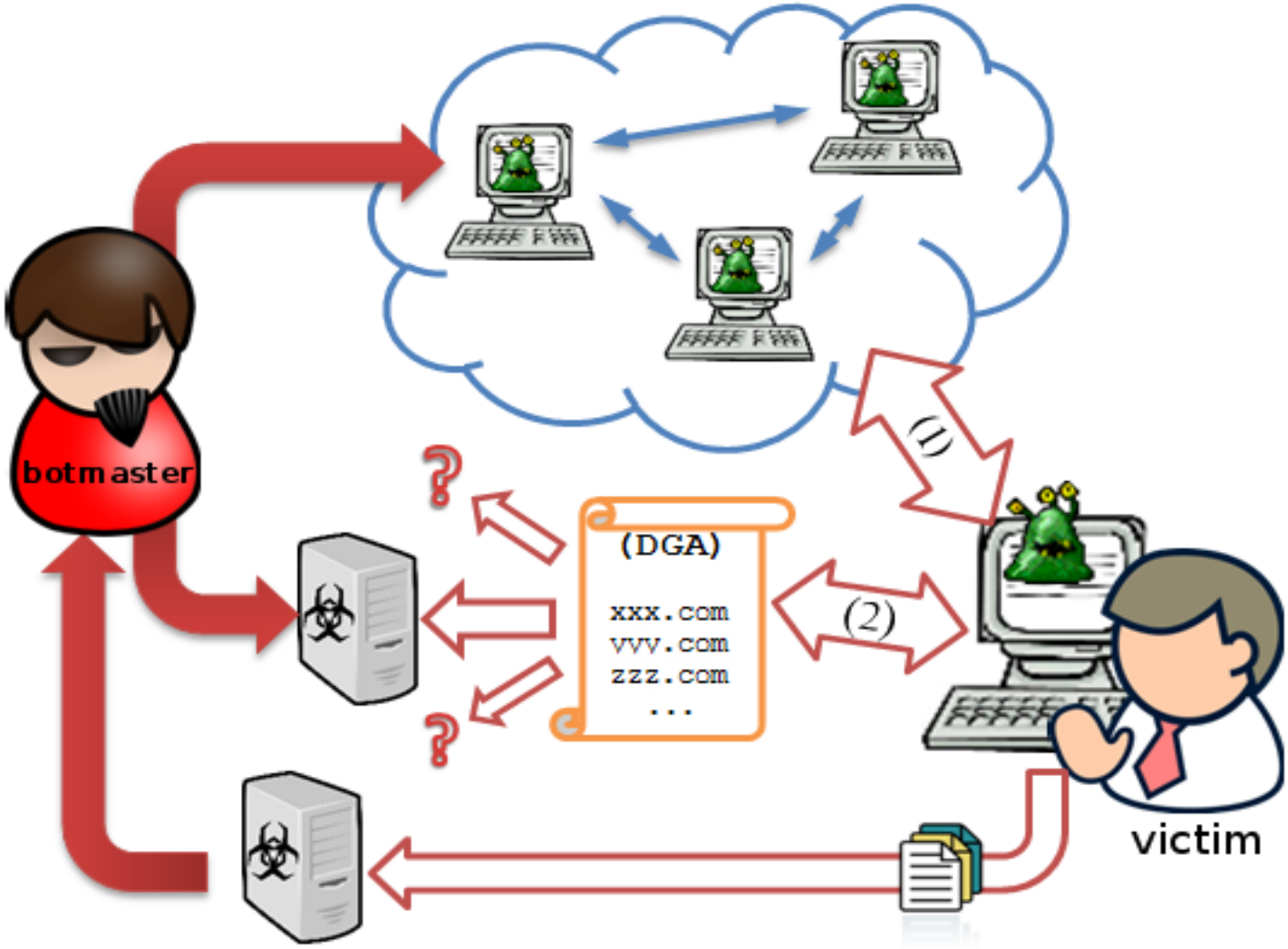


Quelle: http://www.cert.pl//PDF/2013-06-p2p-rap_en.pdf

Netzwerktopologie II

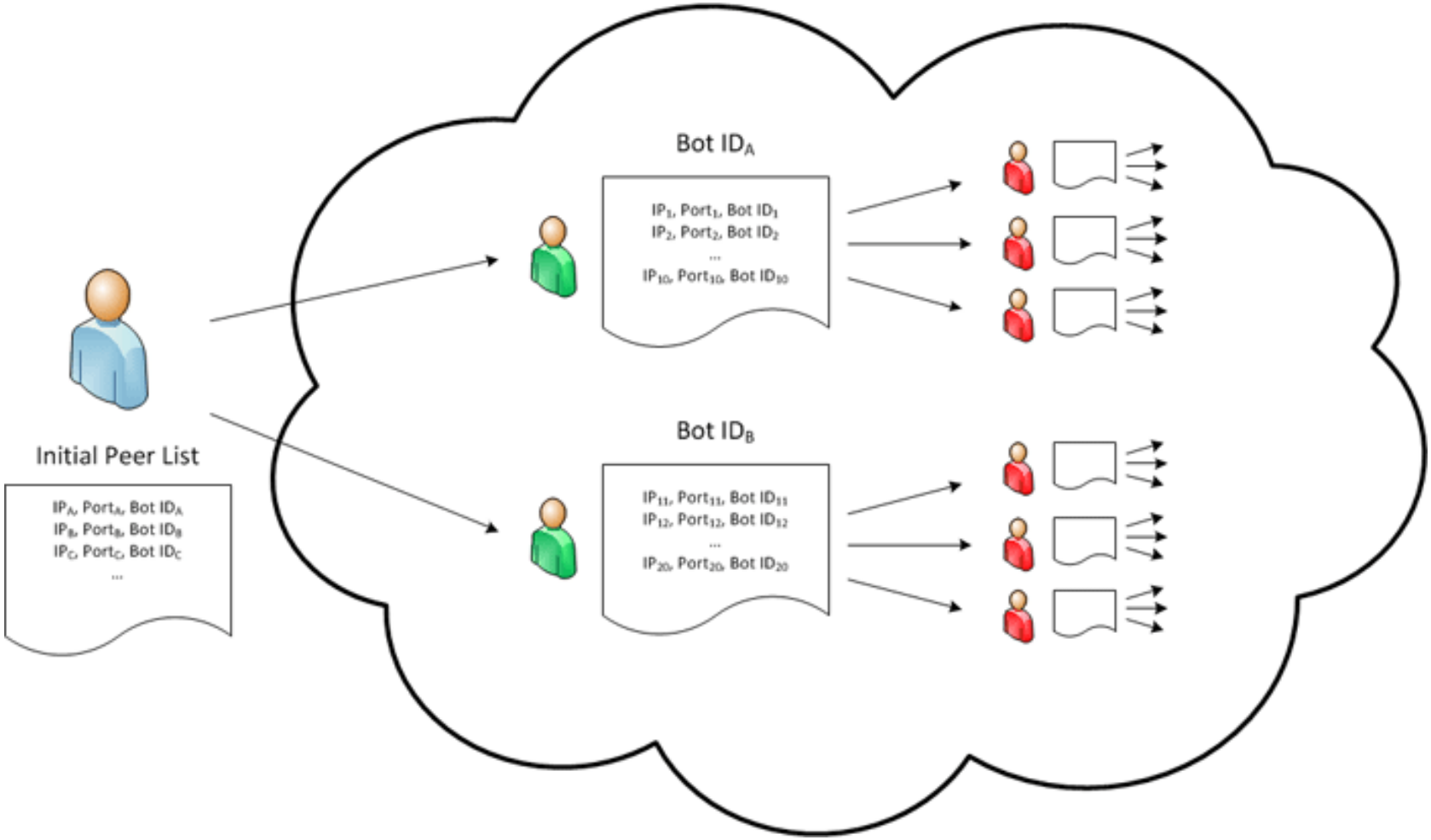


Funktionsweise



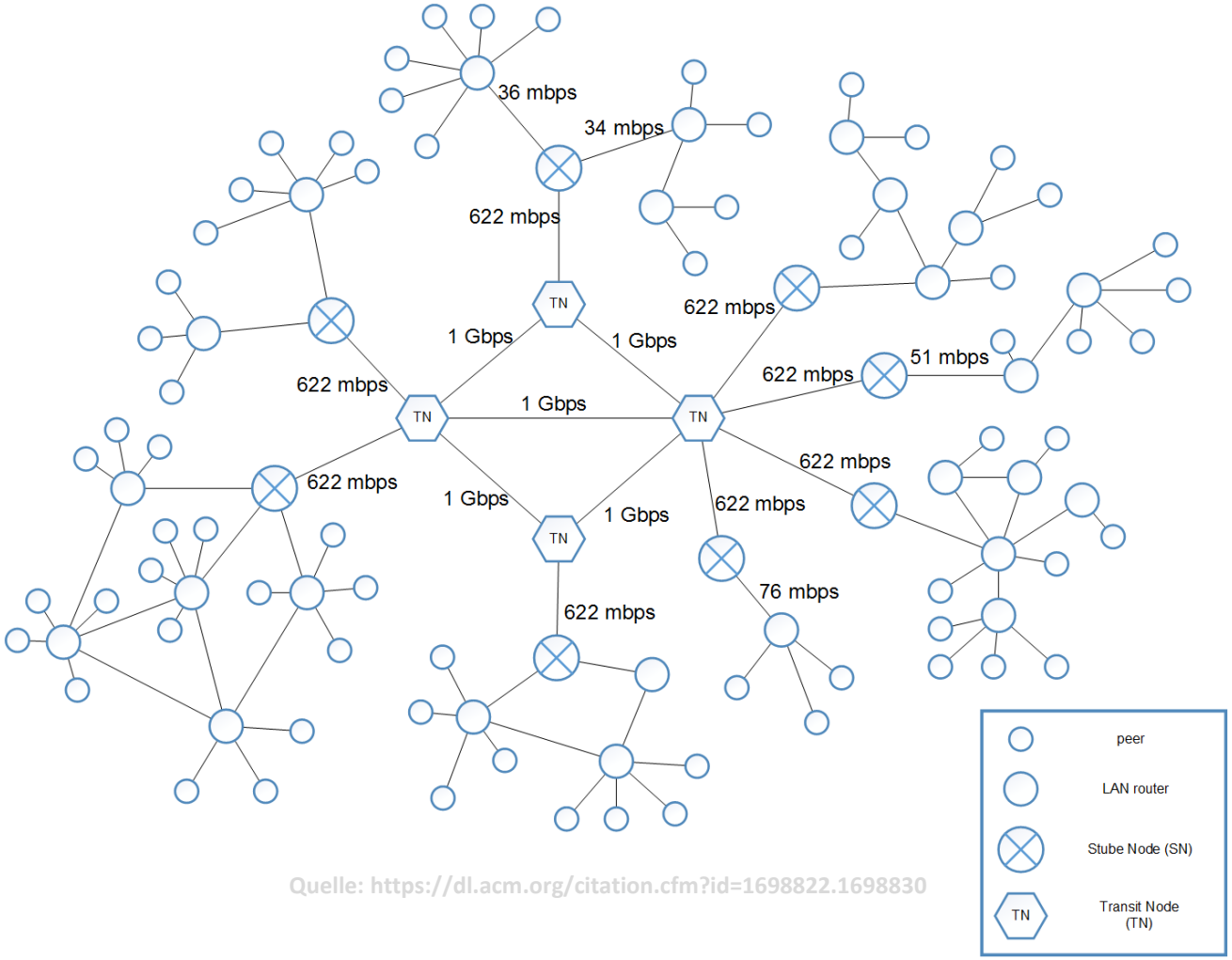
Quelle: http://www.cert.pl//PDF/2013-06-p2p-rap_en.pdf

Peer-to-Peer Netzwerk Aufbau



Quelle: http://www.secureworks.com/cyber-threat-intelligence/threats/The_Lifecycle_of_Peer_to_Peer_Gameover_ZeuS/

Peer-to-Peer Netzwerkgeschwindigkeit



Quelle: https://dl.acm.org/citation.cfm?id=1698822.1698830

Peer-to-Peer Nachricht I

Size (bytes)	Field name	Description
1	randByte	random vallue, different from 0
1	TTL	TTL field, or random value (when unused)
1	junkSize	number of extra bytes at the end of the packet
1	cmd	command (determines the type of packet)
20	SSID	session ID
20	senderID	sender node ID

Quelle: http://www.cert.pl//PDF/2013-06-p2p-rap_en.pdf

Peer-to-Peer Nachricht II

Size(bytes)	Description
44	P2P Header
0 or more	The message body (depends on header)
hdr.junkSize	Random bytes (appended at the end of packet)

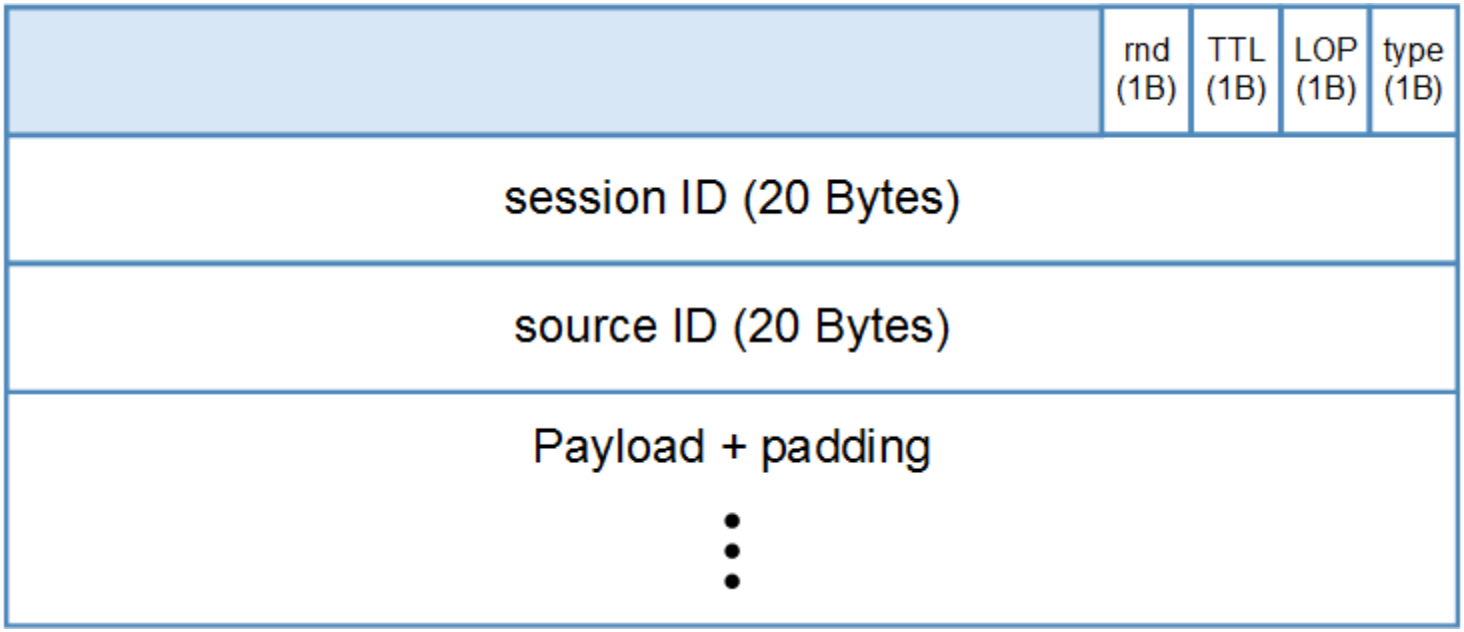
Quelle: http://www.cert.pl//PDF/2013-06-p2p-rap_en.pdf

Peer-to-Peer CMD Befehle

CMD value	Description
0x00	version query
0x01	+ response
0x02	peer-list query
0x03	+ response
0x04	data query
0x05	+ response
0x06	super-node address broadcast
0x32	super-node address broadcast

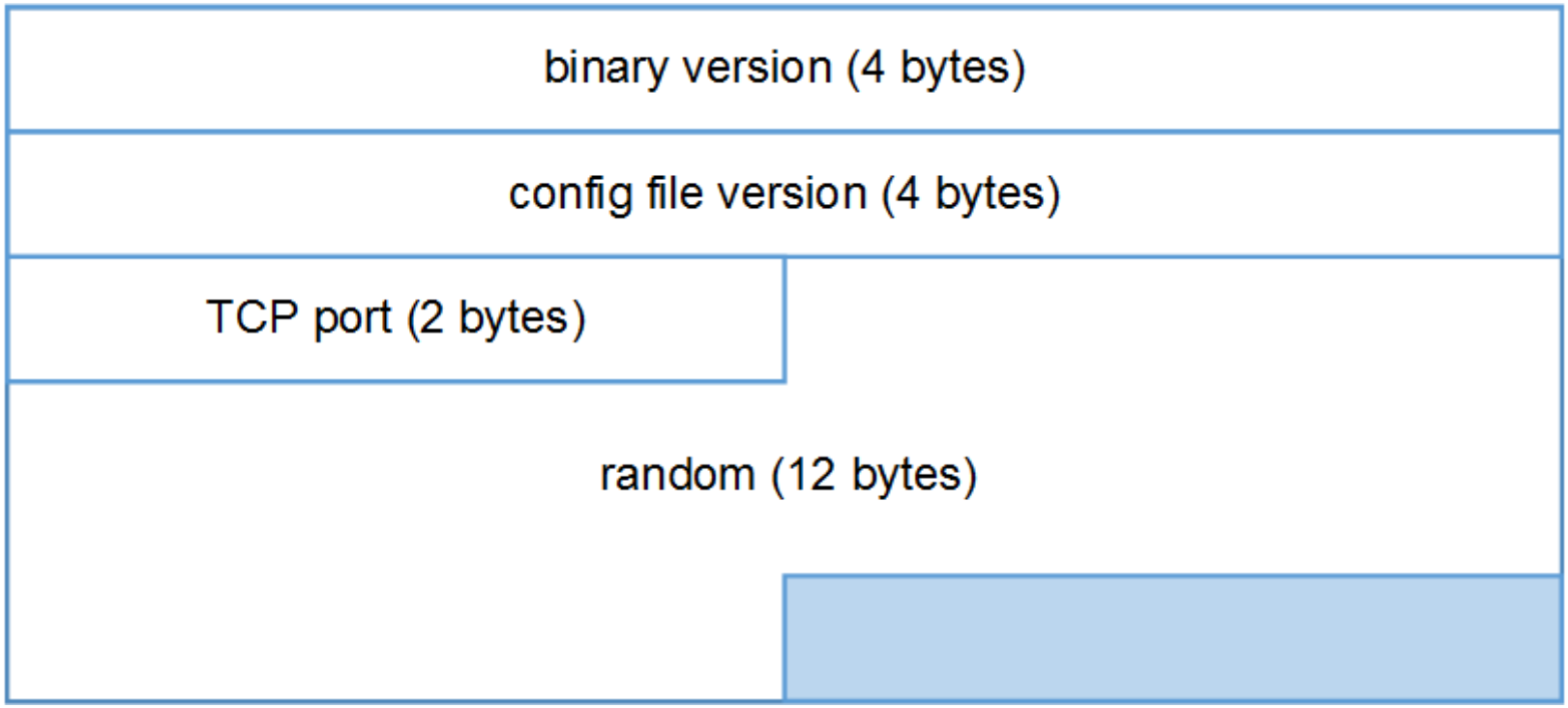
Quelle: http://www.cert.pl//PDF/2013-06-p2p-rap_en.pdf

Peer-to-Peer Header



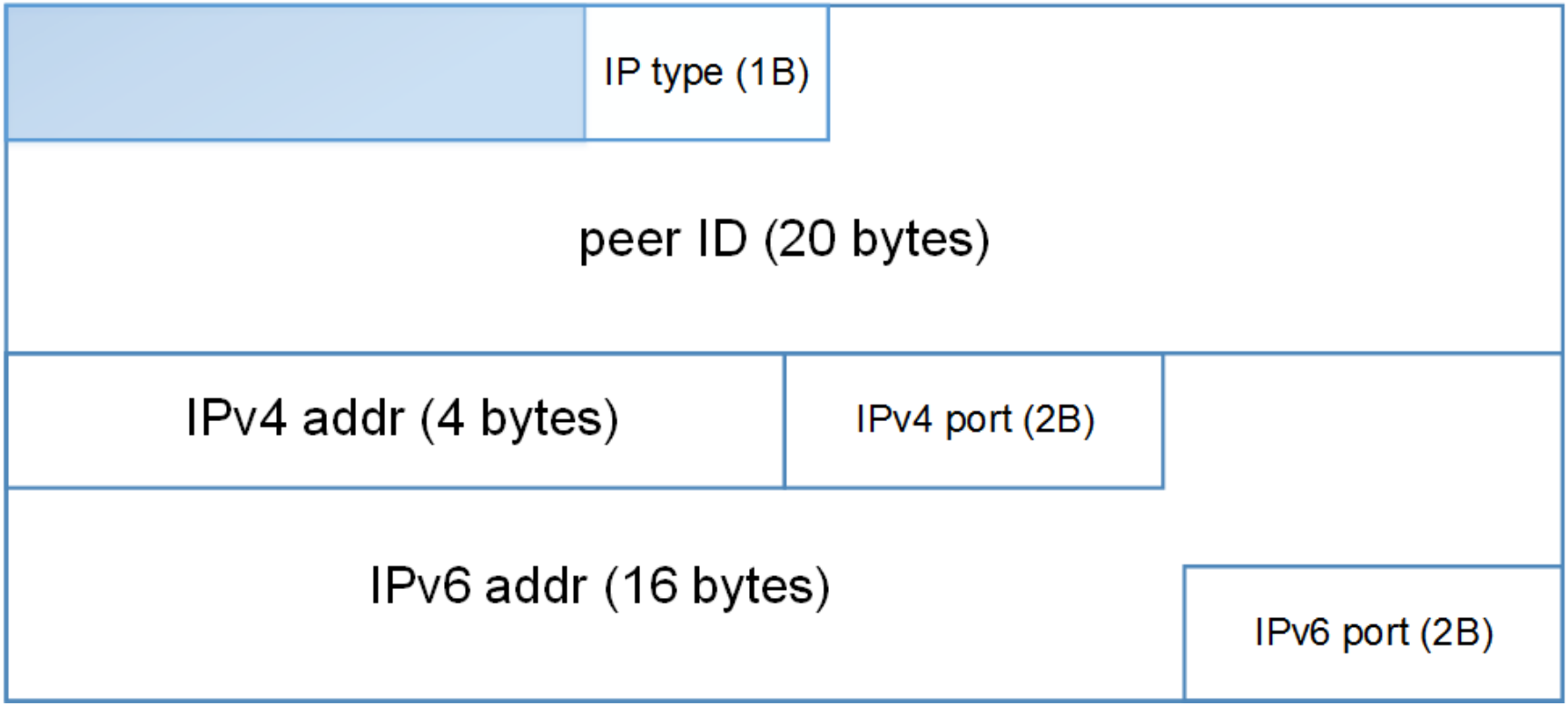
Quelle: http://www.cert.pl//PDF/2013-06-p2p-rap_en.pdf

Peer-to-Peer Version Response Header



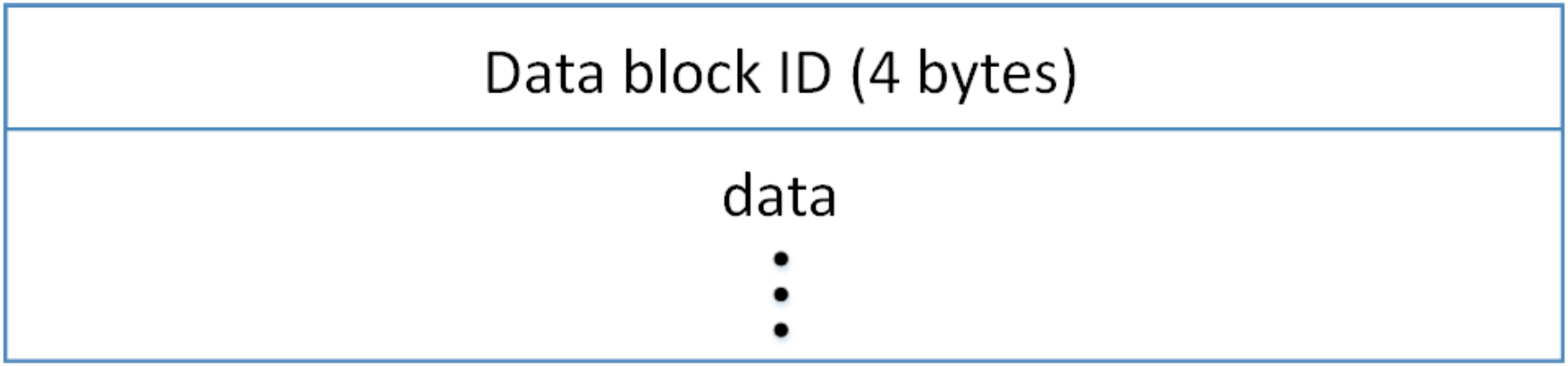
Quelle: http://www.cert.pl//PDF/2013-06-p2p-rap_en.pdf

Peer-to-Peer Peer List Response Header



Quelle: http://www.cert.pl//PDF/2013-06-p2p-rap_en.pdf

Peer-to-Peer Data Response Header

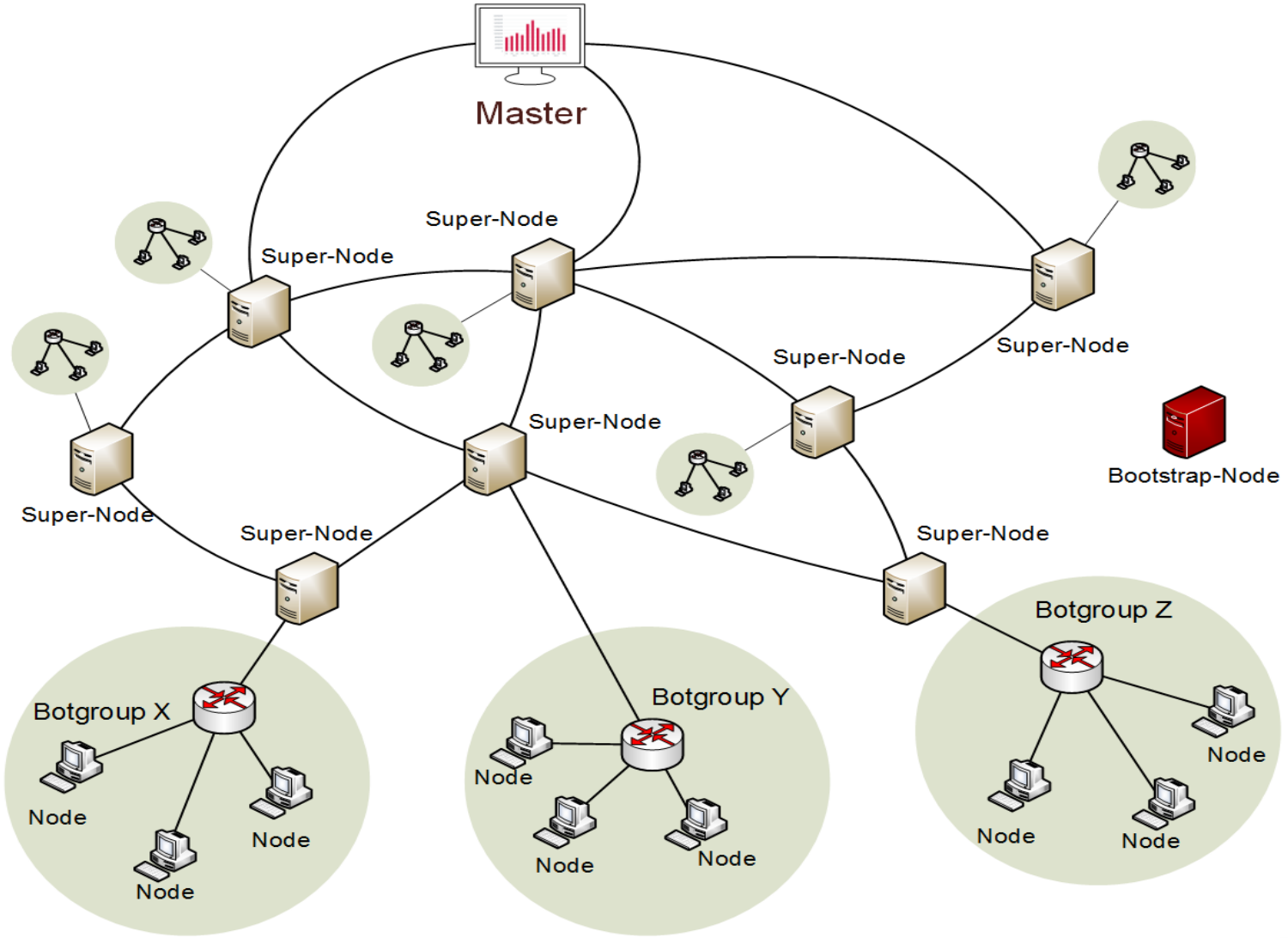


Quelle: http://www.cert.pl//PDF/2013-06-p2p-rap_en.pdf

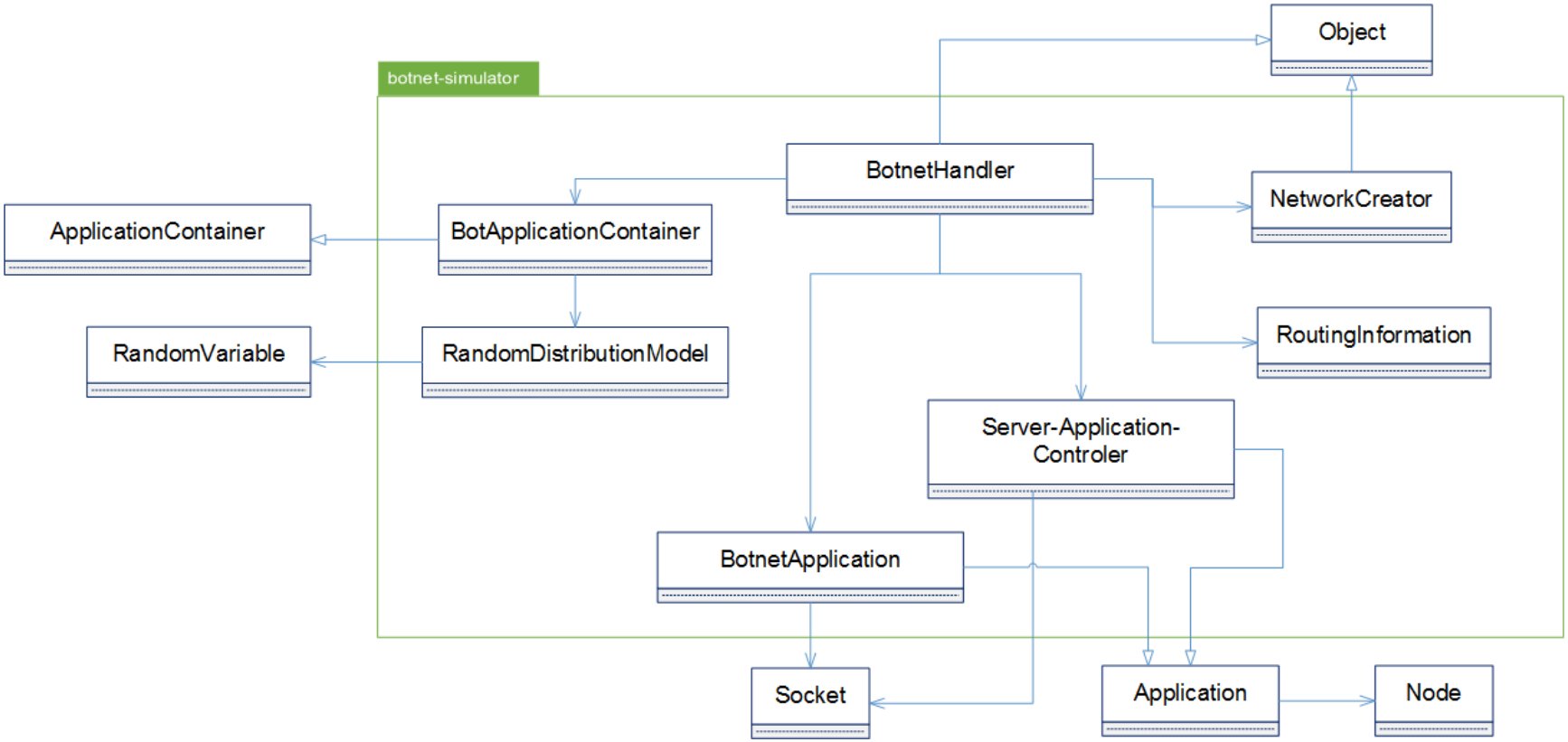
Botnetze

Framework

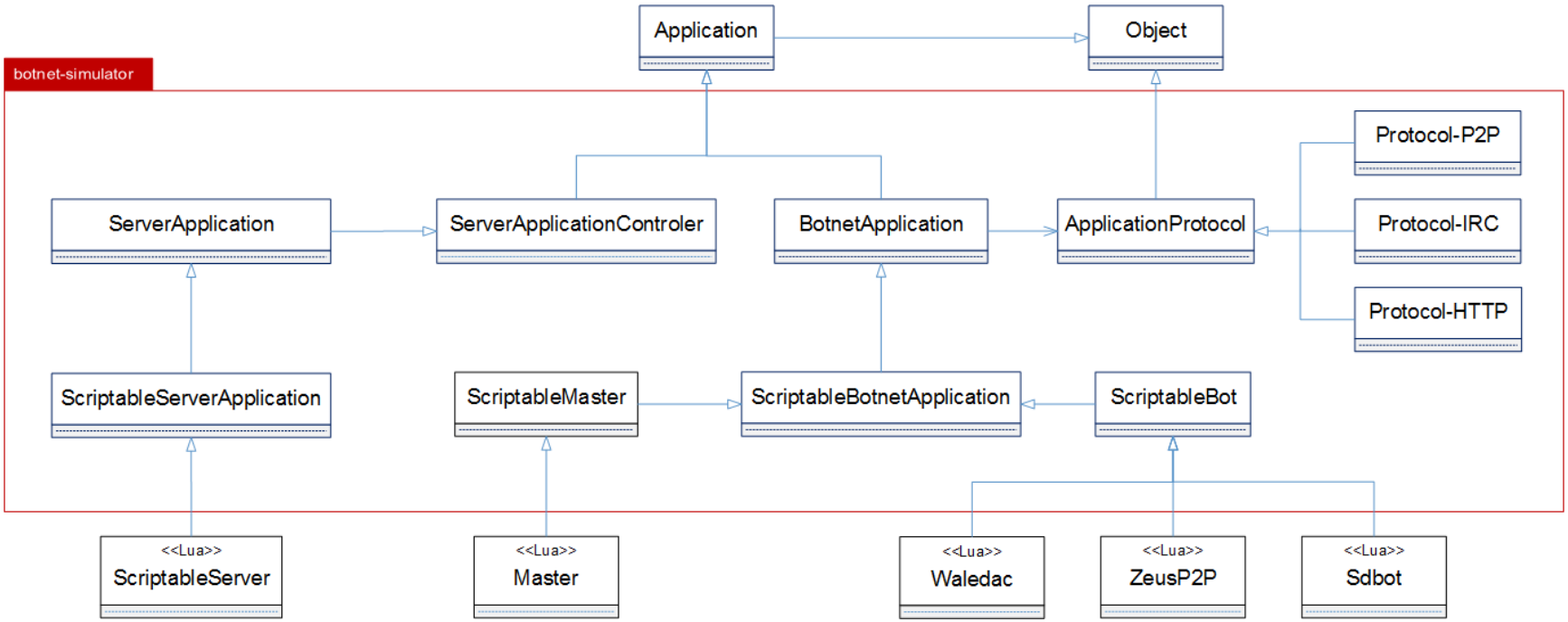
Netzwerk Aufbau



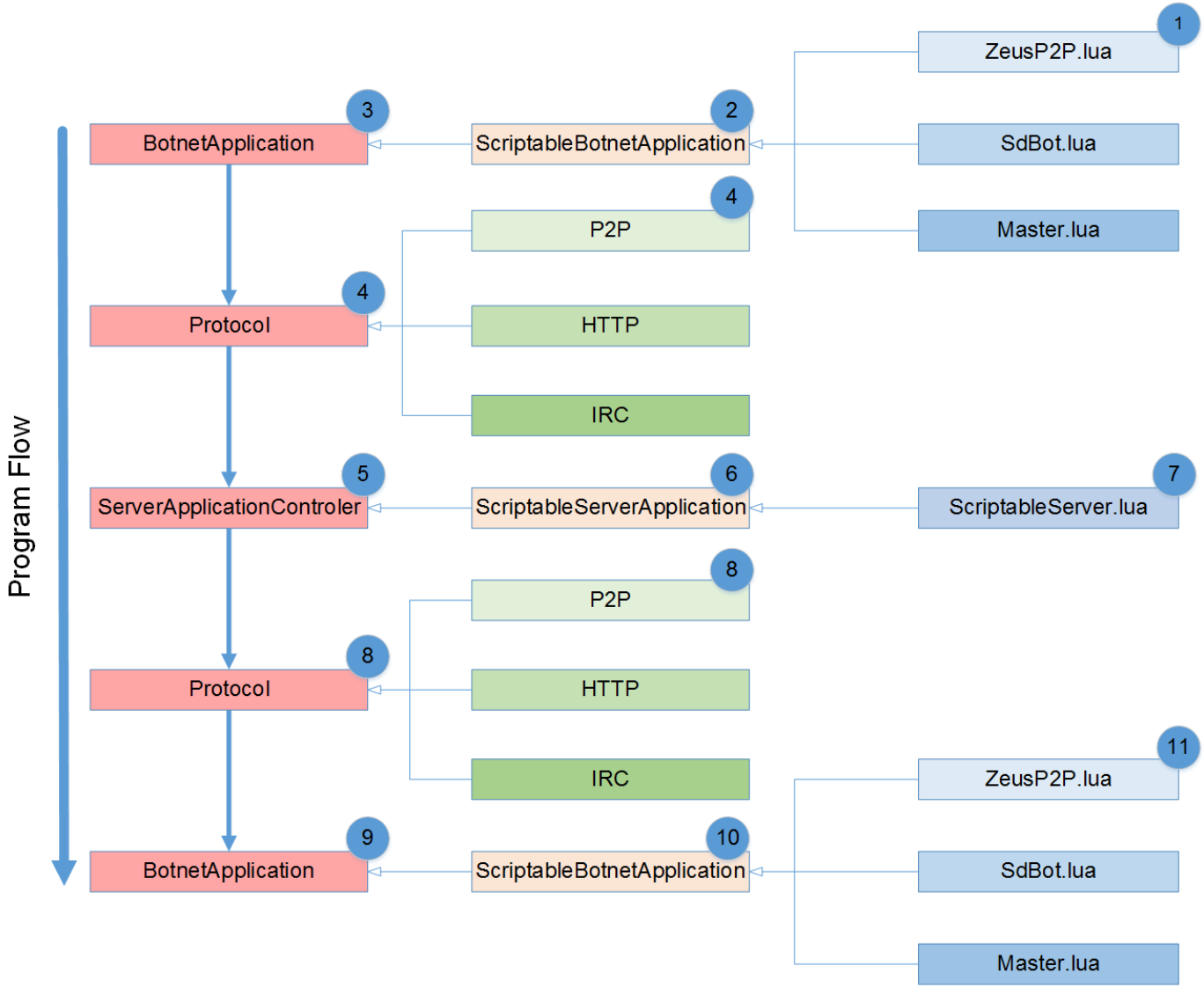
Klassendiagramm I



Klassendiagramm II



Ablaufdiagramm



Botnetze

Skripte

Framework

- Fluctuations Model
  - Statischtiche Mittel zur Veränderung des Botnetzverhalten
  - Downtime, Onlinetime, On-Off Switcher
- Botnet Configuration
  - Erstellen von Botnetzgruppen
- Botnet Simulator
  - Variablen können vordefiniert werden
  - Dynamische Handhabung

Lua

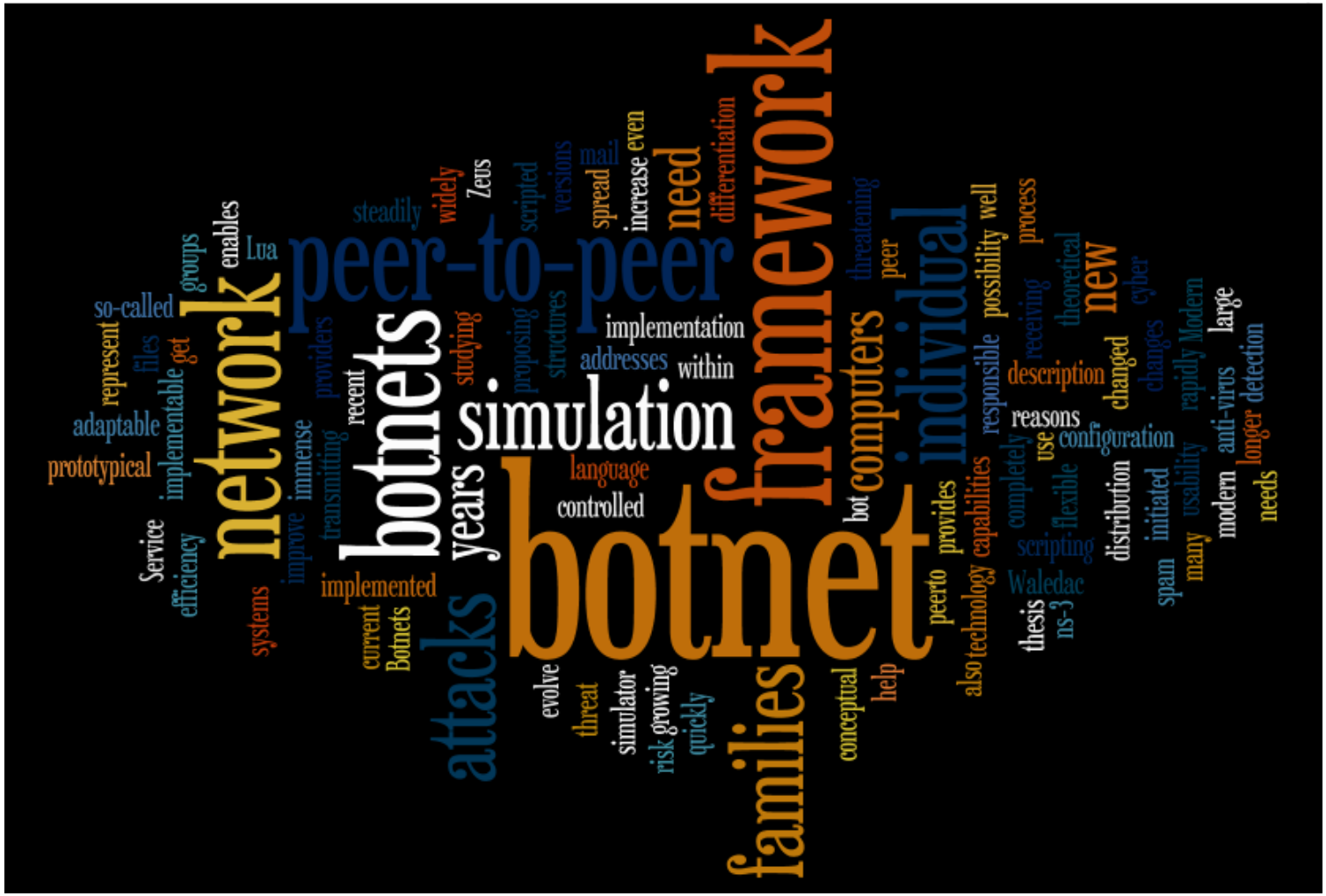
- Init()
  - Wird beim Programmstart geladen
- Connected()
  - Wird geladen, sobald der Bot “Online” geht
- ProcessCommand()
  - Falls eine Nachricht ankommt, kann hier reagiert werden

Botnetze

Demonstration

Demonstration

It's time for Questions



Quelle: https://sophosnews.files.wordpress.com/2012/03/botguy.jpg%3Fw%3D500%26h%3D375