
BOTNETS

Detection, Classification, and Countermeasures

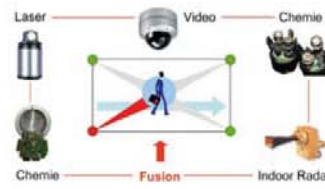
Prof. Dr. Peter Martini, Fraunhofer FKIE and Univ. of Bonn, Germany

October 5, 2011



Fraunhofer-FKIE

Fraunhofer Institute for Communication, Information Processing, and Ergonomics



FKIE is a research institute active in the areas of defense and security.
FKIE develops models, methods and tools for Network Enabled Capabilities.

■ Research Areas

- Command and Control Systems
- Communication Systems
- Multisensor Data Processing for Surveillance
- Human Factors & Human-Machine-Systems
- Information & Knowledge Management
- Unmanned Systems
- Cyber Defense

Location	Wachtberg
Founded in	1963
Staff	> 300
Budget	> 24 Mio €
Director	Prof.Dr. Peter Martini
WWW	www.fkie.fraunhofer.de

FKIE – Cyber Defense

Defense and Public Security

- **Protection against „Cyber Attacks“**
 - Protection of Critical IT Infrastructures
 - Protection of Command&Control in „Cyber-Physical Systems“

- **Always in Our Minds: Practical Relevance**
 - „Thinking starts at the Application“
 - Focus: Defense and Public Security
 - Support for Decision Makers, Users, Operators
 - Training, Consulting, Implementation Support
 - Protection and Quick Restoration of the Reliability and the Trustworthiness of Computer Systems and Networks

Introduction

Cyber War

Cyber War

Fact of Fiction ?

Freitag, 26. November 2010

Schlagzeilen | Hilfe | RSS | Newsletter | Mobil | Wetter | TV-Programm

SPIEGEL ONLINE WISSENSCHAFT

NACHRICHTEN VIDEO THEMEN FORUM ENGLISH DER SPIEGEL SPIEGEL TV ABO SHOP

Home | Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | einestages | UniSPIEGEL | SchulSPIEGEL | Reise | Auto

Nachrichten > Wissenschaft > Technik > Cyberwar [Login](#) | [Registrierung](#)

THEMA Cyberwar

Alle Artikel, Hintergründe und Fakten

Krieg der Staatshacker

In den Datennetzen sind kriminelle Angriffe von kriegerischen kaum zu unterscheiden. Doch in den letzten Jahren häufen sich Attacken, die sich als Spionage- oder Sabotageversuche im staatlichen Auftrag deuten lassen. Eine reale Gefahr - oder nur ein fiktives Szenario, um eine autoritäre Kontrolle des Internets vorzubereiten?

Corbis

Tages-Anzeiger 24.11.10: "Stuxnet was a worldwide test of weapons"

The screenshot shows a Mozilla Firefox browser window displaying the Tages-Anzeiger website. The article title is "«Stuxnet war ein weltweiter Waffentest»" (Stuxnet was a worldwide test of weapons). The author is identified as Sandro Gaycken. The article text states: "Der Sicherheitsexperte und Autor Sandro Gaycken über die neue Qualität von Würmern, falsche Terrorwebsites westlicher Geheimdienste und den Unterschied zwischen Cybercrime und Cyberwar." (The security expert and author Sandro Gaycken on the new quality of worms, fake terrorist websites of Western intelligence services and the difference between cybercrime and cyberwar.)

The article includes a photo of several men in military uniforms looking at a computer screen. Below the photo, a caption reads: "1/8 | Unter Beobachtung: Stuxnet war offenbar gefährlicher als bisher angenommen, wie ein Bericht des US-Senats zeigt." (Under observation: Stuxnet was apparently more dangerous than previously assumed, as a report from the US Senate shows.)

On the right side of the page, there is a "Digital" section with a list of articles, including "Ein Jahrzehnt Handy-Multimedia", "Apples Problem mit Songs und Sonderzeichen", and "Tagesschau-Störung durch Demonstrantin". There are also advertisements for ADTECH, Mobile, and Krankenkassen 2011.

2009: „Conficker“

French fighter planes grounded by computer virus

French fighter planes were unable to take off after military computers were infected by a computer virus, an intelligence magazine claims.

by Kim Willsher in Paris
Published: 11:43AM GMT 07 Feb 2009

French fighter jets were unable to take off after military computers were attacked by a virus. Photo: AFP

The aircraft were unable to download their flight plans after databases were infected by a Microsoft virus they had already been warned about several months beforehand.

At one point French naval staff were also instructed not to even open their computers.

Scripts Currently Forbidden | <SCRIPT>: 49 | <OBJECT>: 0

Conficker entmystifiziert

Felix Leder und Tillmann Werner von der Universität Bonn stellen heute die Ergebnisse ihrer Analyse des Conficker-Wurms vor. Sie beschreiben nicht nur in einem Paper aus der Reihe "know your Enemy" die Funktionsweise des Wurms, sondern sie präsentieren auch eine Reihe von Tools, mit denen man vor dem Wurm immunisieren oder ihn aufspüren und auch sauber entfernen kann. Und schließlich haben sie auch ein Problem entdeckt, über das man anscheinend Conficker sogar direkt angreifen könnte.

Sollte es noch eines Beweises bedürft haben, dass Conficker kein Werk von Anfängern ist, hat die Analyse von Leder und Werner den jetzt erbracht. So enthält der Wurm beispielsweise ein sehr intelligentes Auto-Update-Verfahren: Er leitet die verwundbaren Funktionsaufrufe zur Umwandlung eines relativen Pfades wie `\\.\.\` in das kanonische `\\.` auf sich um. Kommt dort ein Funktionsaufruf an, der versucht, die Sicherheitslücke auszunutzen, wie es Conficker selbst tut, dann dekodiert er den darin enthaltenen Shellcode. Der versucht typischerweise den eigentlichen Wurmcode nachzuladen, die dafür verwendete URL extrahiert Conficker aus dem Shellcode und lädt das Wurm-Programm dann selber.

Doch damit nicht genug. Conficker testet sehr genau, ob es sich um eine aktuellere Version seiner selbst handelt. Er erwartet dazu eine digitale Signatur, die mit einem geheimen RSA-Schlüssel des Wurm-Autors erstellt sein muss. Es ist quasi aussichtslos, Conficker auf diesem Weg etwas unterzuschleichen; die Entwickler haben für den Wurm einen dezentralen Auto-Update-Mechanismus implementiert, den die Forscher für praktisch unknackbar halten.

Trotzdem lassen sich die Ergebnisse von Leder und Werner gezielt gegen den Wurm einsetzen. Indem sie im Hauptspeicher nach den eindeutigen RSA-Keys zum Überprüfen der digitalen Signaturen suchen, können sie die

Conficker Memory Disinfector
Felix Leder, Tillmann Werner 2009
(leder, werner)@cs.uni-bonn.de

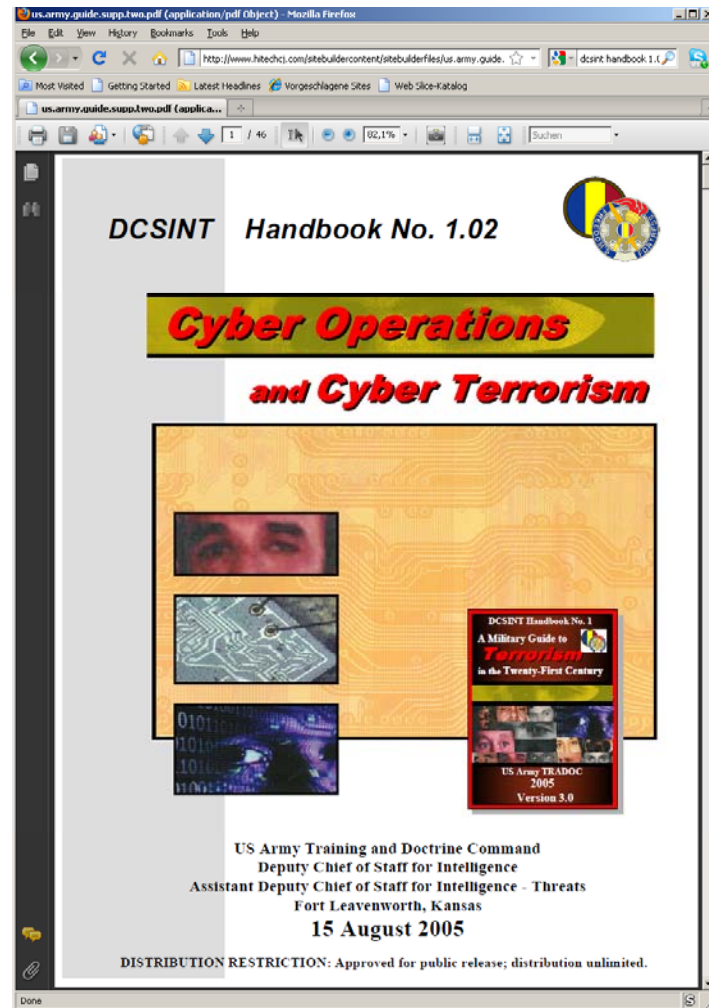
Examining [8] [System Process]: Error
no match
Examining [4] System: no match

Scripts Currently Forbidden | <SCRIPT>: 18 | <OBJECT>: 0

Goals of Cyber Attacks

A Handbook from Aug. 15, 2005

http://www.hitechj.com/sitebuildercontent/sitebuilderfiles/us.army.guide.supp.two.pdf



1. Loss of Integrity

- Modification of Data

2. Loss of Availability

- Slowing-Down or Blocking of Systems/Functions

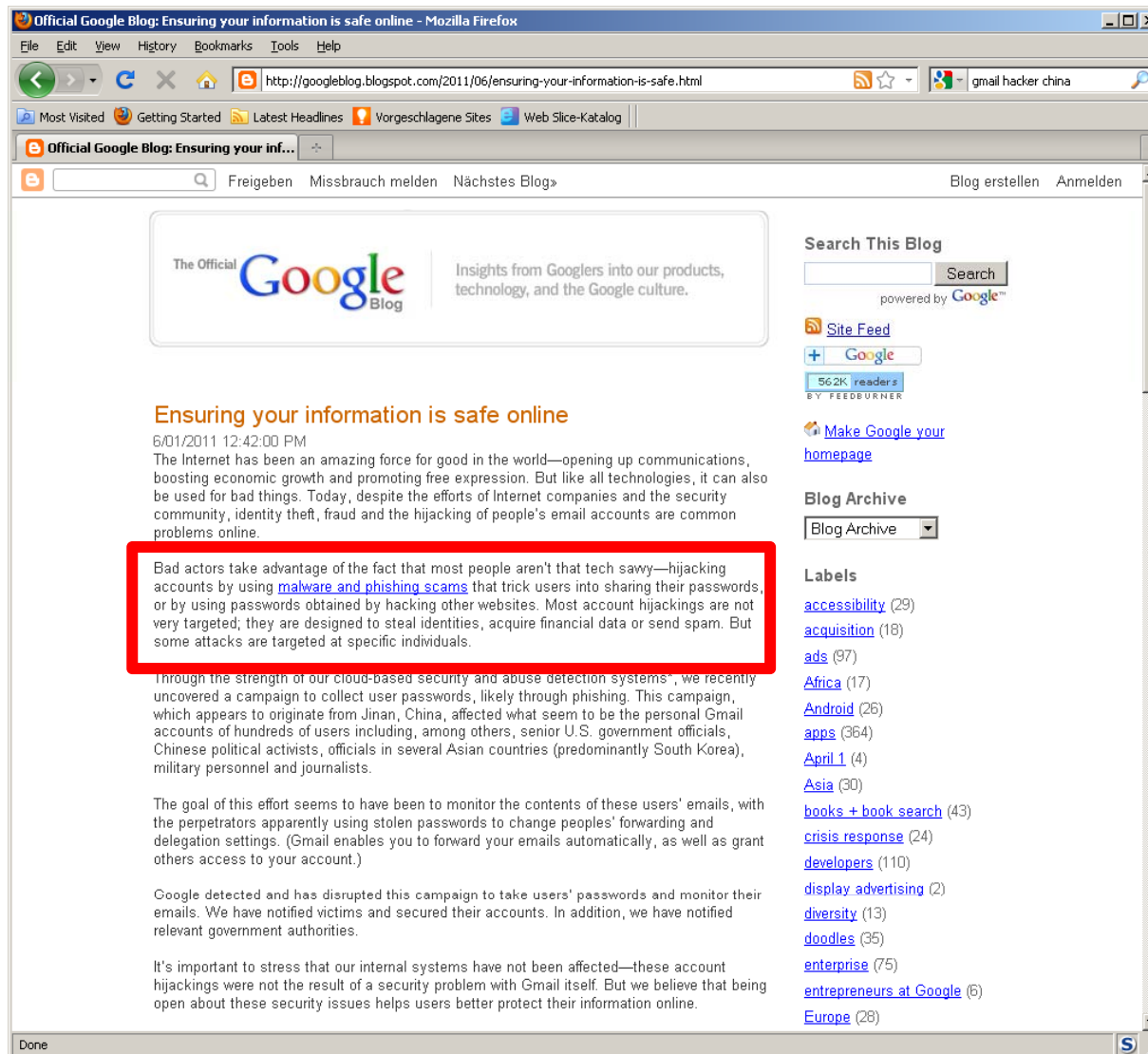
3. Loss of Confidentiality

- Espionage, Battle for the Public Opinion

4. Physical Destruction

- Supervisory Control and Data Acquisition (SCADA)

Example: Gmail-Hacking; Google (June 1, 2011 12:42)



Reuters (June 1, 2011 7:30pm EDT)

The screenshot shows a Mozilla Firefox browser window with the URL <http://www.reuters.com/article/2011/06/01/us-google-hacking-idUSTRE7506U320110601>. The page features the Reuters logo and navigation menu. The main article is titled "Google reveals Gmail hacking, likely from China" and is attributed to Alexei Oreskovic and Edwin Chan. The article text reads: "(Reuters) - Hackers likely based in China tried to break into hundreds of Google mail accounts, including those of senior U.S. government officials, Chinese activists and journalists, the Internet company said on Wednesday. The unknown perpetrators, who appeared to originate from Jinan in Shandong province, recently tried to crack and monitor email accounts by stealing passwords, but Google detected and 'disrupted' their campaign,". The page also includes a "Most Popular" sidebar with links to other news items, social media sharing buttons (Facebook, Twitter, RSS, YouTube), and a "Follow Reuters" section.

http://www.reuters.com/article/2011/06/01/us-google-hacking-idUSTRE7506U320110601

China blamed for Gmail hack attack; cyber warfare in focus - International Business Times - Mozilla Firefox

http://www.ibtimes.com/articles/156054/20110601/china-cyber-warfare-us-google-gmail-login-details-passwords-security-hackers-t

China blamed for Gmail hack attack; ...

U.S. Edition Mobile Most Popular Topics Archives

INTERNATIONAL BUSINESS TIMES US

SEARCH IBTIMES

THE INTELLIGENT INVESTOR
Subscribe now for Free

News Markets Careers Life & Style Topics Video Research Tools Local

World US Politics Society Companies Economy Markets Economy Companies Tech Law Real Estate Sports Slideshows Picture This In Depth

China blamed for Gmail hack attack; cyber warfare in focus

TOP STORIES 1 of 3
Greek government expected to present new budget plan

Article Comments

Share Tweet Rate this Story +2 0

Print Email Order Reprints Text Size + -

By IB Times Staff Reporter | June 1, 2011 10:42 PM EDT

A cyber attack that originated from the Chinese city of Jinan that selectively targeted key government officials in the U.S. and its allies has focused uneasy limelight on [China](#), even as the western governments are tinkering with their military rule books to call cyber attacks 'acts of war'.



Chinese hackers broke into the personal Gmail accounts of senior officials and military personnel of the U.S. government and its allies and stole sensitive data, Google revealed on Wednesday, setting the stage for an era of heightened cyber tension between the world's top military powers.

Hackers unleashed malware or phishing scam to hijack the accounts of government functionaries, military top brass and journalists in what appears to be a selective attack on key targets, especially political rivals of [China](#), from where the cyber criminals launched their attack.

The hack attack came to light just a day after it was revealed that the U.S. government was planning to bring in legislation declaring cyber attacks as acts of war.

The latest hack attack, which might bring Google and the Chinese administration into a fresh fist fight, was precisely planned and executed, raising doubts if the Chinese state had authorized it.

War on Drugs Has

Related Articles

- China responds to ethnic riots in Inner-Mongolia
- Apple supplier Foxconn reopens polishing sites
- How far would you go for an iPad 2 and iPhone? Teenager Sells Kidney

Related Topics

- China
- White House
- Books

Get US Emails & Alerts

ADVERTISE WITH US

Follow IBTimes

Facebook Twitter RSS Email

IBTIMES TV MORE VIDEOS

Politics & Policy
Google: FBI Will Investigate Allegations of China's Involvement in Hacking of Gmail

Moody's
1:11
Moody's May Downgrade Risk
15:06
Forex Technical Update for EUR, JPY, and AUD
1:32
Libya: Russian President Calls For Negotiations With Wells Fargo

Most Popular on US

Scripts Currently Forbidden | <SCRIPT>: 42 | <OBJECT>: 0

Done

BBC (June 2, 2011 08:33 GMT)

BBC Mobile News Sport Weather Travel TV Radio More

NEWS ASIA-PACIFIC

Home UK Africa Asia-Pac Europe Latin America Mid-East South Asia US & Canada Business Health SciEnvironment Tech Entertainment Video

2 June 2011 Last updated at 08:33 GMT

China rejects Gmail spying claims

China has rejected allegations of involvement in a cyber-spying campaign targeting the Google e-mail accounts of top US officials, military personnel and journalists.

A foreign ministry spokesman said it was "unacceptable" to blame China.

Google has not blamed the Chinese government directly, but says the hacking campaign originated in Jinan.

The US company said its security was not breached but indicated individuals' passwords were obtained through fraud.

Chinese political activists and officials in other Asian countries were also targeted, **Google said**.

Washington investigation

It is extremely difficult for analysts to determine whether governments or individuals are responsible for such attacks, says the BBC's Adam Brookes in Washington.

But the fact that the victims were people with access to sensitive - even secret - information raises the possibility that this was cyber-espionage rather than cyber-crime, adds our correspondent.

However, Chinese foreign ministry spokesman Hong Lei told a news briefing: "Blaming these misdeeds on China is unacceptable."

"Hacking is an international problem and China is also a victim. The claims of so-called support for hacking are completely unfounded and have ulterior motives."

On Wednesday, Google said it had "detected and has disrupted" a campaign to take users' passwords and monitor their emails.

"We have notified victims and secured their accounts," said the company. "In addition, we have notified relevant government authorities."

Top Stories

- E. coli: Russia bans EU imports
- Japan PM survives vote challenge
- Carmakers hit in new market slide
- Yemeni tribesmen 'march on Sanaa'
- Risk of Greece default 'at 50:50'

Features & Analysis

- 12 people, one idea: How a loop of red ribbon conquered the world
- Eye for an eye: One woman's campaign after horrific acid attack
- Dance to excite: Mark Madrell on US Republicans as Mitt Romney prepares to run
- Shockproof?: Why Algeria's sparks of discontent have failed to ignite

Most Popular

Shared

- Tesco mistake leads to beer rush 1
- Software clues unravel Mac theft 2
- Global war on drugs has 'failed' 3
- Nature 'is worth billions' to UK 4

Scripts Currently Forbidden | <SCRIPT>: 74 | <OBJECT>: 0

“Malware” and “Botnets”

Malware and Botnets

The Basics

- **Definition:** *Malware* (short for *malicious software*) is software designed to perform activities on or grant access to a computer system without the owner's knowledge or consent.
- **First Appearance:** depends on definition, known cases are
 - 1971 – Creeper / Worm (spreading in ARPANET)
- 1986 – Brain / Virus

"I'm the creeper, catch me if you can!"

- (another worm named "Reaper" was used to remove Creeper)

Welcome to the Dungeon (c) 1986 Basit * Amjad (pvt) Ltd.
BRAIN COMPUTER SERVICES 730 NIZAM BLOCK ALLAMA IQBAL TOWN
LAHORE-PAKISTAN PHONE: 430791,443248,280530. Beware of
this VIRUS.... Contact us for vaccination...

Malware and Botnets

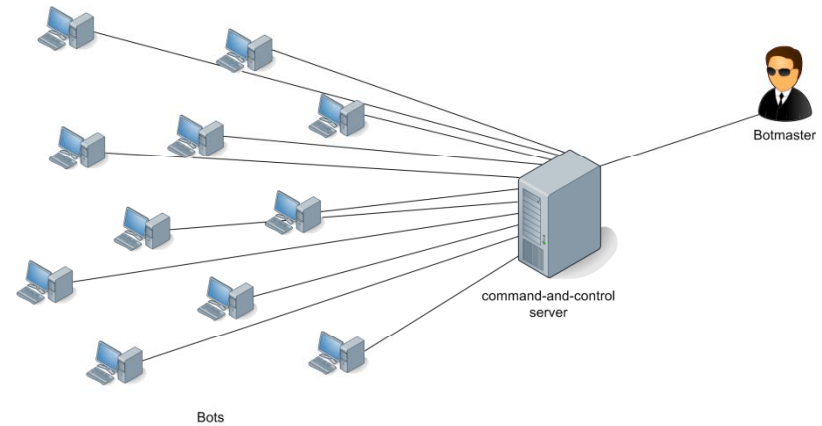
The Basics (2)



- **Classical types of malicious software:**
 - Virus (self-replicating code)
 - Worm (autonomous, network-based spreading)
 - Trojan Horse (deceptive program, carrying other malware)
 - Keylogger (intercepts keystrokes)
 - Spyware (gathers data from an infected machine)
 - Rootkit (grants hidden access to a system)
 - Dialer (uses modem to generate profits over premium numbers)
 - Scareware (social engineering of users)
 - Ransomware (performs extortion by e.g. encrypting the hard drive)
- Today, these classifications are no longer useful, as most malware combines various aspects of functionality.

Malware and Botnets

The Basics (3)



- **Definition:** Botnets combine infected computer systems into a network of compromised systems (bots, zombies) operated and controlled by a third party (botmaster/botherder).
- Botnets combine classical malware functionality to a dangerous weapon with lots of application areas.
- Motivations:
 - Financial interests
 - Spam
 - Financial Fraud
 - Identity Theft
 - Extortion
 - Political interests
 - Denial of Service ('07 against Estonia, ...)
 - Espionage ('08 GhostNet)
 - Sabotage ('09 Stuxnet)

“Malware” and “Botnets”

Life Expectancy of Malware

Symantec Security Response

http://www.symantec.com/security_response/index.jsp

Backdoor.Coreflood

Risk Level 1: Very Low

Discovered: November 29, 2002

Updated: December 3, 2002 3:19:23 PM

Type: Worm

Infection Length: 173,056 bytes

Systems Affected: Windows 98, Windows 95, Windows XP, Windows Me, Windows Vista, Windows NT, Windows 2000

SUMMARY

Backdoor.Coreflood is a Trojan horse that opens a back door on the compromised computer.

Antivirus Protection Dates

- Initial Rapid Release version November 29, 2002
- Latest Rapid Release version May 31, 2011 revision 023
- Initial Daily Certified version November 29, 2002
- Latest Daily Certified version May 31, 2011 revision 034
- Initial Weekly Certified release date December 4, 2002

Click [here](#) for a more detailed description of Rapid Release and Daily Certified virus definitions.

Threat Assessment

Wild

- Wild Level: Low
- Number of Infections: 0 - 49
- Number of Sites: 0 - 2
- Geographical Distribution: Low
- Threat Containment: Easy
- Removal: Easy

Damage

- Damage Level: Medium
- Payload: Opens a back door on the compromised computer.
- Releases Confidential Info: Gathers information relating to online transactions.

Distribution

- Distribution Level: Low

TECHNICAL DETAILS

This Trojan may be downloaded and installed by another threat, which may have been downloaded while visiting compromised websites.

“Malware” and “Botnets” Coreflood

Case 3:11-cv-00561-VLB Document 1 Filed 04/11/11 Page 1 of 18

UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

UNITED STATES OF AMERICA, :
 :
 Plaintiff, :
 : No. 3:11 CV _____
 v. :
 :
 JOHN DOE 1, JOHN DOE 2, JOHN :
 DOE 3, JOHN DOE 4, JOHN DOE 5, :
 JOHN DOE 6, JOHN DOE 7, JOHN :
 DOE 8, JOHN DOE 9, JOHN DOE 10, :
 JOHN DOE 11, JOHN DOE 12, AND : April 11, 2011
 JOHN DOE 13, :
 :
 Defendants. :

COMPLAINT

NOW COMES the United States of America, by and through its attorney, David B. Fein, United States Attorney for the District of Connecticut, and alleges the following:

1. This is a civil action brought under Title 18, United States Code, Sections 1345 and 2521 to enjoin the Defendants from continuing to engage in wire fraud, bank fraud, and unauthorized interception of electronic communications, in violation of Title 18, United States Code, Sections 1343, 1344, and 2511, by means of malicious computer software known as "Coreflood."

“Malware” und “Botnets”

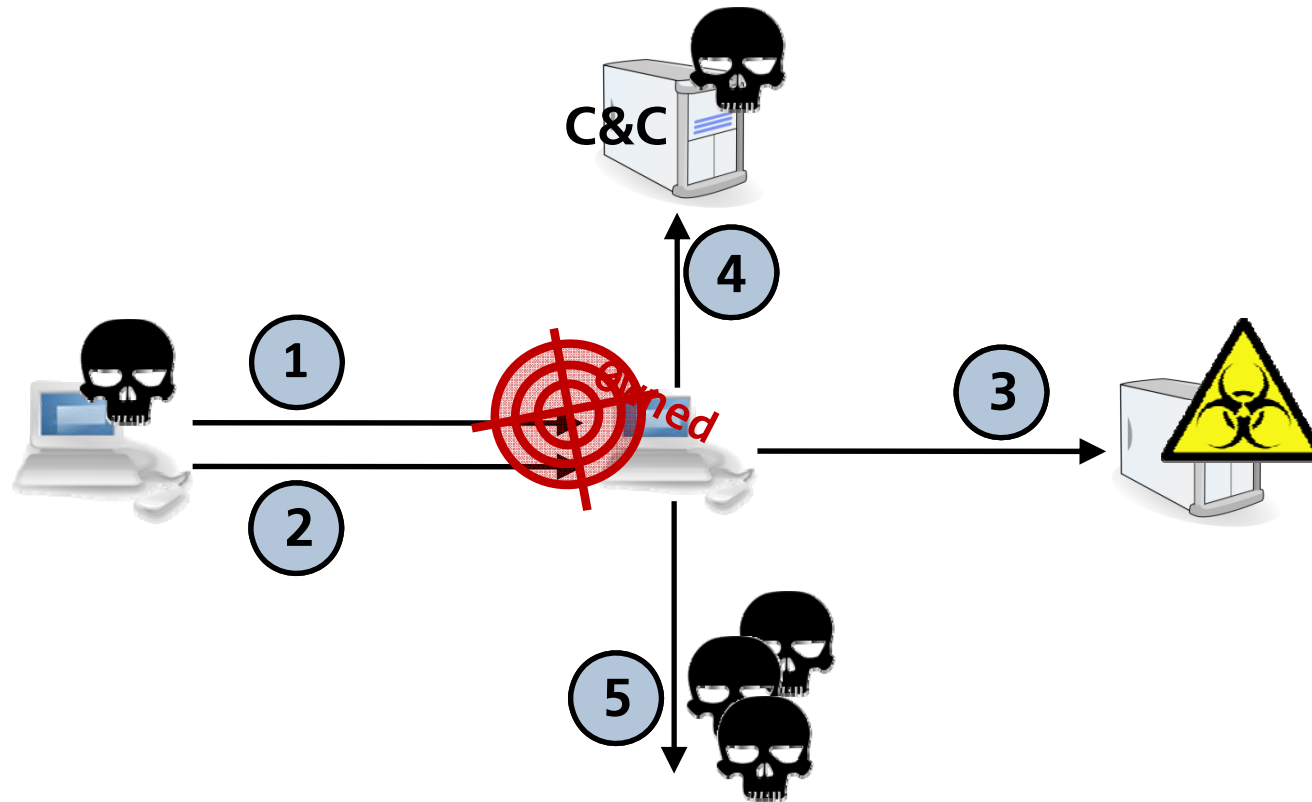
Coreflood

13. The victims of the fraud scheme described above included, inter alia:

- a. A real estate company in Michigan, from whose bank account there were fraudulent wire transfers made in a total amount of approximately \$115,771;
- b. A law firm in South Carolina, from whose bank account there were fraudulent wire transfers made in a total amount of approximately \$78,421;
- c. An investment company in North Carolina, from whose bank account there were fraudulent wire transfers made in a total amount of approximately \$151,201; and
- d. A defense contractor in Tennessee, from whose bank account there were fraudulent wire transfers attempted in a total amount of approximately \$934,528, resulting in an actual loss of approximately \$241,866.

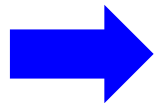
Botnets

How to Set Up a Botnet



Botnets

Takeover by USB Devices



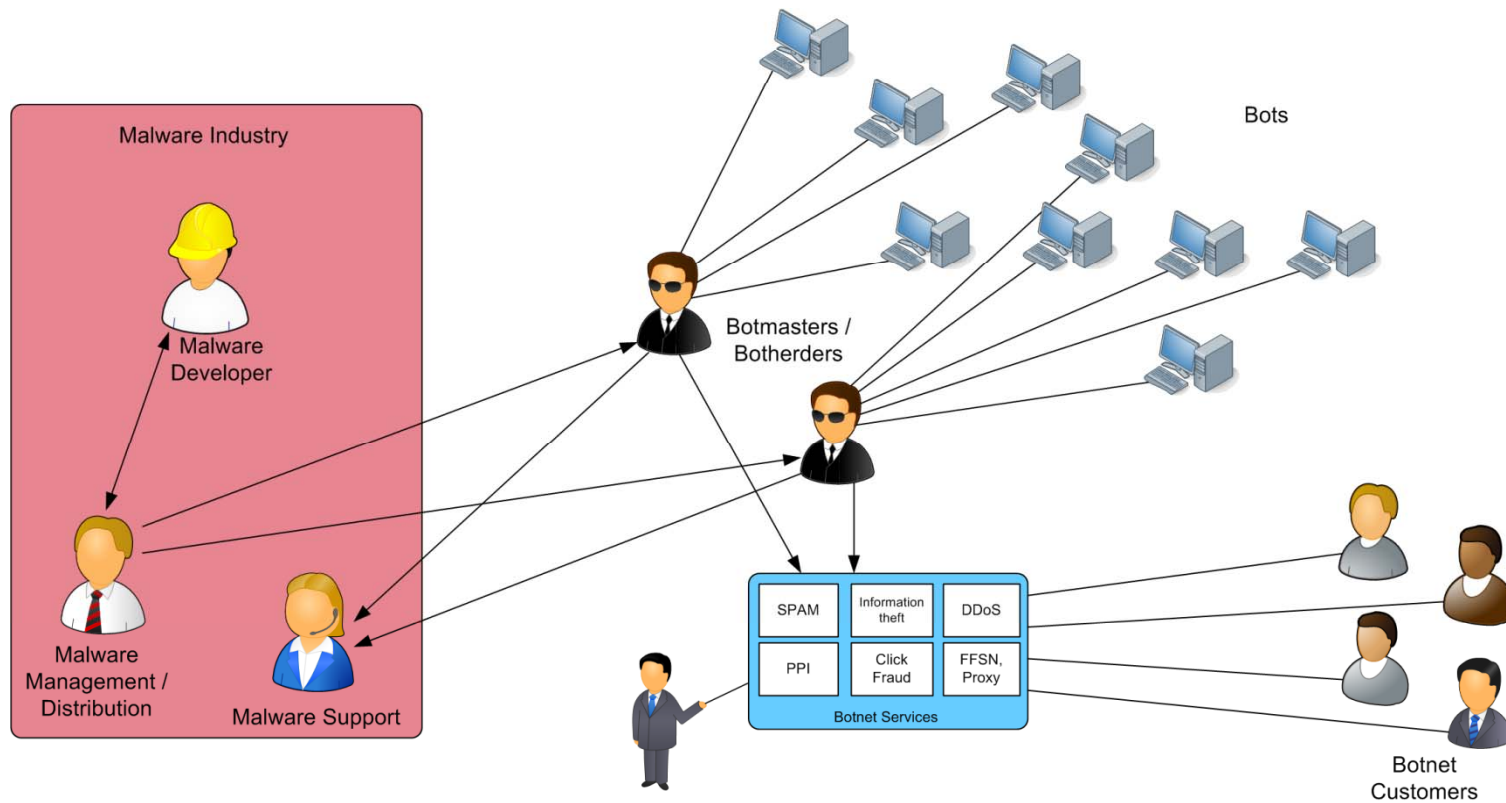
Botnets as autonomous or partially autonomous systems

- Autonomous proliferation
- Autonomous coordination of infected systems
- Configuration of future activities in case of pre-defined conditions
 - Time-of-Day
 - Geo-Location
 - System Environment (Operating System, I/O devices, ...)
 - ...

Malware Economy

Roles and services

- Around malware, a complete economy has evolved.

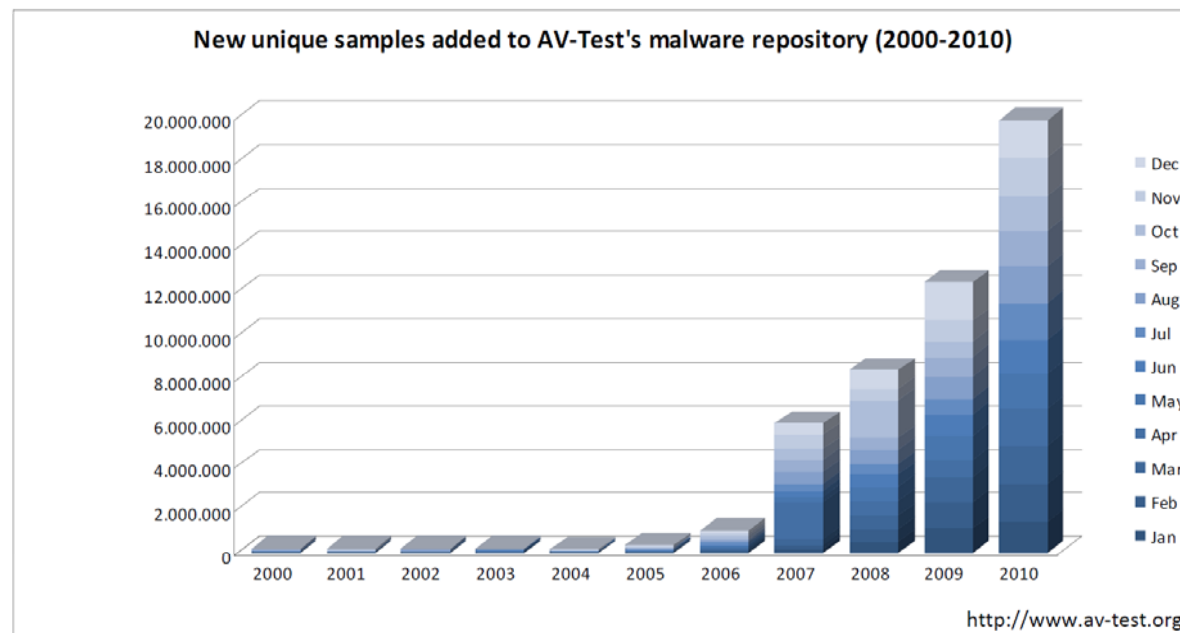


Analysis of Malware and Botnets

A large zoo of malware

Collecting malware samples

■ AV-Test: tracking of malware samples



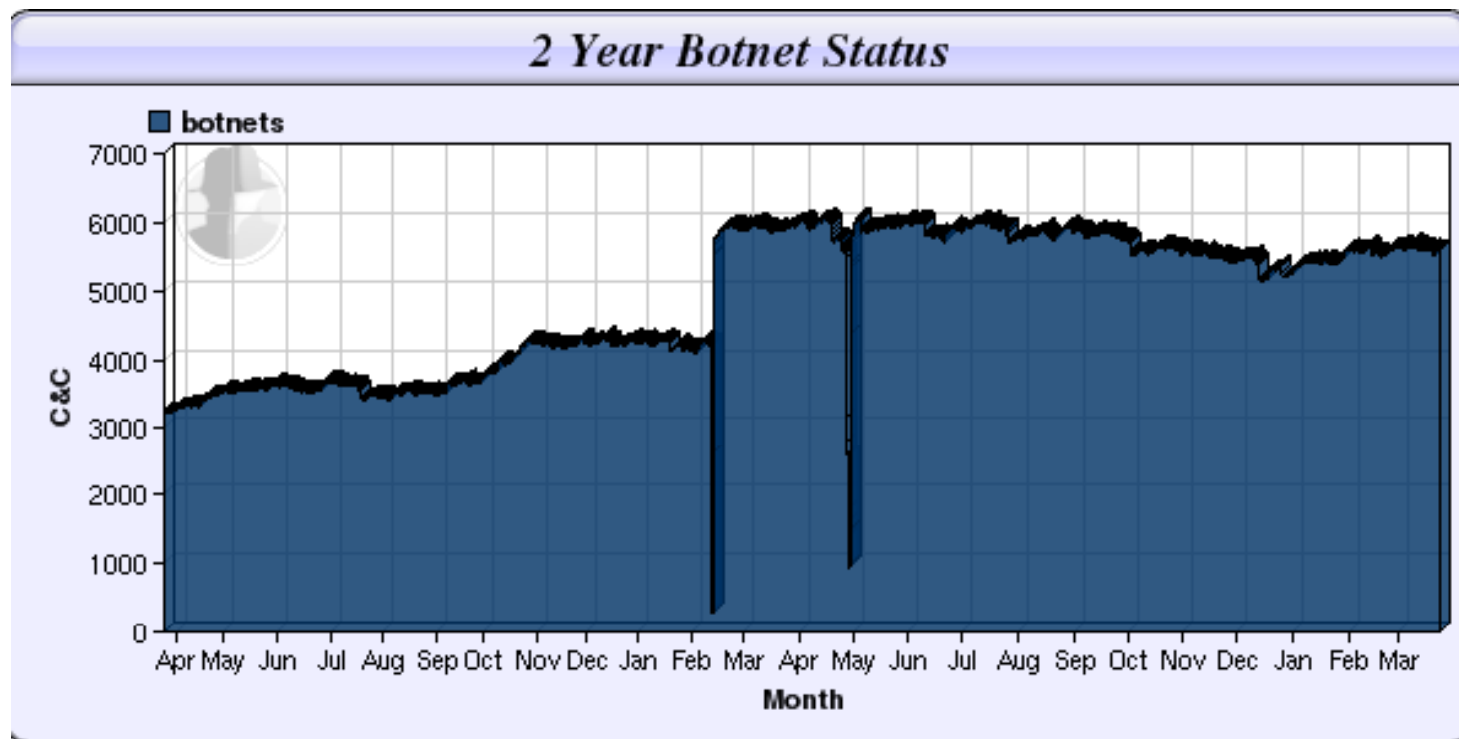
[<http://www.av-test.org>]

2010: New Malware Samples
~ 55.000 per day
~ 2.300 per hour
~ 38 per minute

➔ **Scanning for viruses only provides limited protection.**

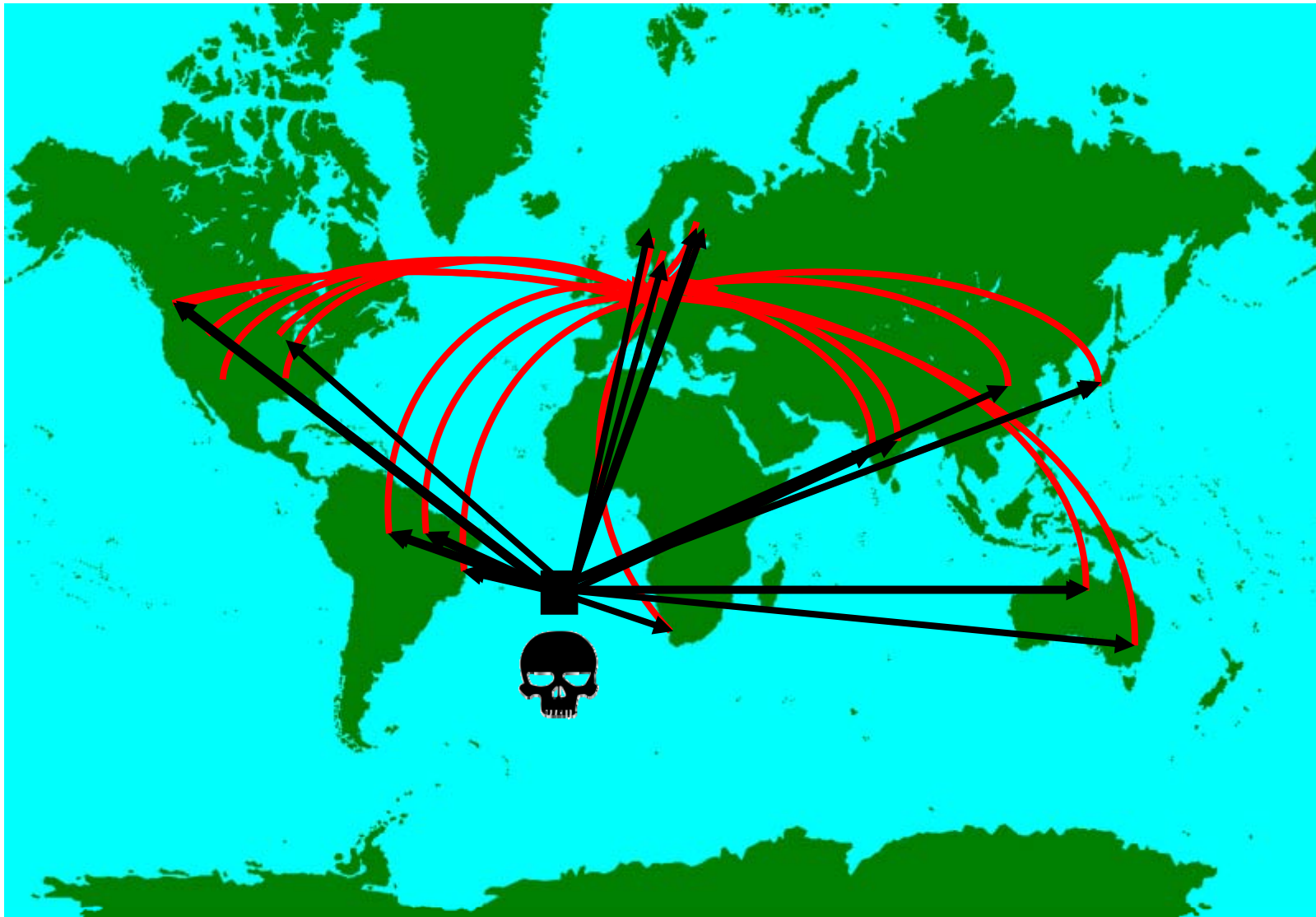
A large zoo of botnets as well...

- **Shadowserver:** tracking of known C&C servers



[<http://www.shadowserver.org/wiki/pmwiki.php/Stats/BotnetCharts>]

DDoS-Attacks: Distributed Denial of Service



Public Domain Image, http://en.wikipedia.org/wiki/File:World_Map_flat_Mercator.png

Botnets: Detection & Counter-Measures

Selected Methods

■ Passive Techniques

- Traffic Analysis
- DNS-based Approaches
- Analysis of Spam
- Analysis of Log Files
- Honeypots
- Evaluation of AV Feedback

■ Active Techniques

- Sinkholing
- Infiltration
- DNS Cache Snooping
- Tracking of Fast-Flux Networks
- IRC-based detection & monitoring
- Enumeration of Peer-to-Peer Networks

■ Other Techniques

- Reverse Engineering
- C&C forensics & abuse desks

Botnets: Detection & Counter-Measures

Selected Methods

■ Passive Techniques

- **Traffic Analysis**
- DNS-based Approaches
- Analysis of Spam
- Analysis of Log Files
- **Honeypots**
- Evaluation of AV Feedback

■ Active Techniques

- **Sinkholing**
- Infiltration
- DNS Cache Snooping
- Tracking of Fast-Flux Networks
- IRC-based detection & monitoring
- Enumeration of Peer-to-Peer Networks

■ Other Techniques

- **Reverse Engineering**
- C&C forensics & abuse desks

„Traffic Sinkholing“

... Take a Detour

- Redirect bot communication to a “sinkhole”
 - List of infected systems → Estimation of real size
 - If acceptable: Block commands
- Challenge
 - **Global Cooperation** (ISP level or really global)



Example: Conficker

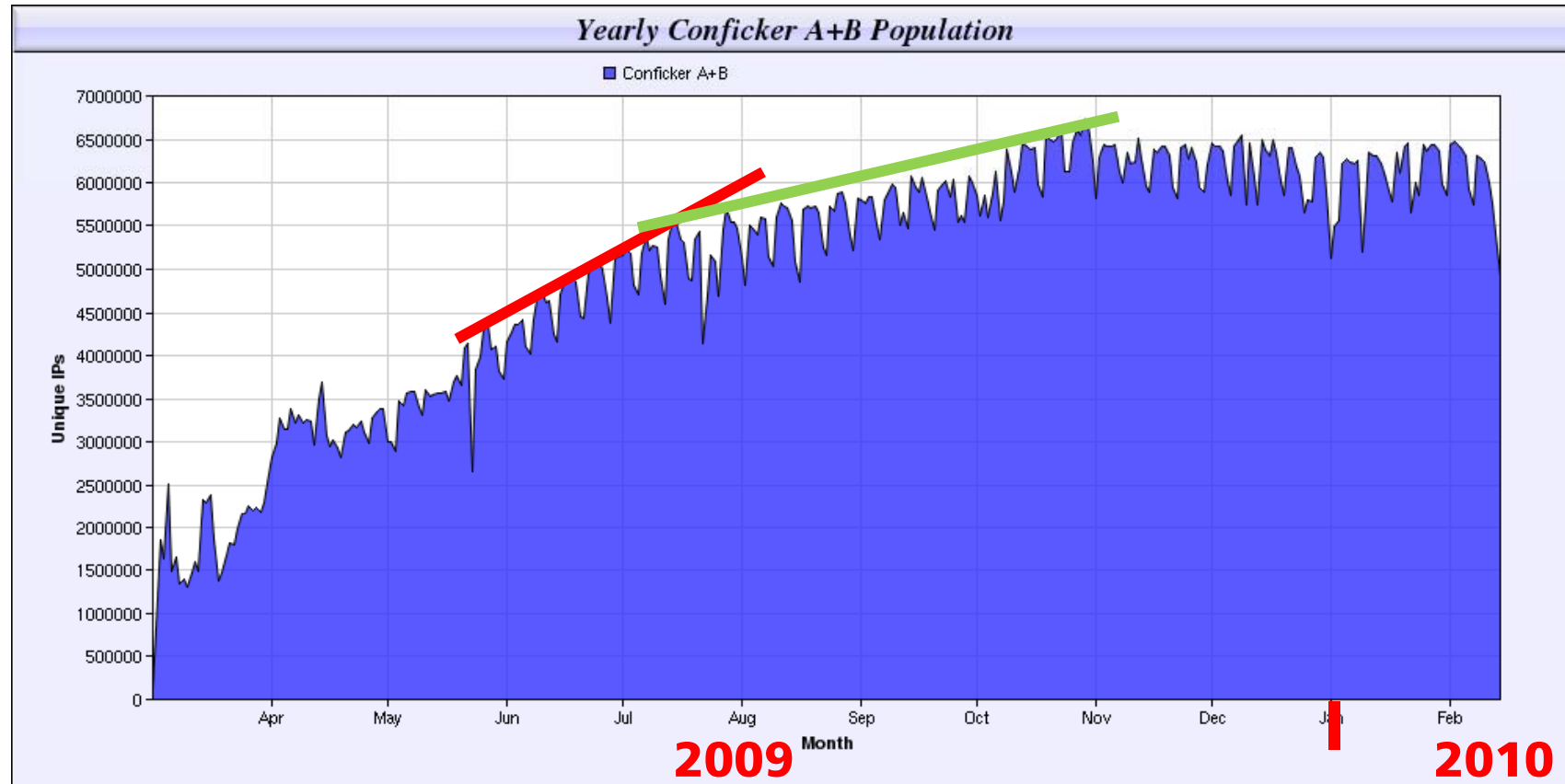
A Domain Name generated by Conficker

YJOLENTXKSY.NET

Domain Name: YJOLENTXKSY.NET
Registrar: KEY-SYSTEMS GMBH
Whois Server: whois.rppproxy.net
Referral URL: <http://www.key-systems.net>
Name Server: NS1.MYDOMAIN-IN.NET
Name Server: NS2.MYDOMAIN-IN.NET
Name Server: NS3.MYDOMAIN-IN.NET
Status: ok
Updated Date: 14-may-2009
Creation Date: 04-mar-2009
Expiration Date: 04-mar-2010

Conficker

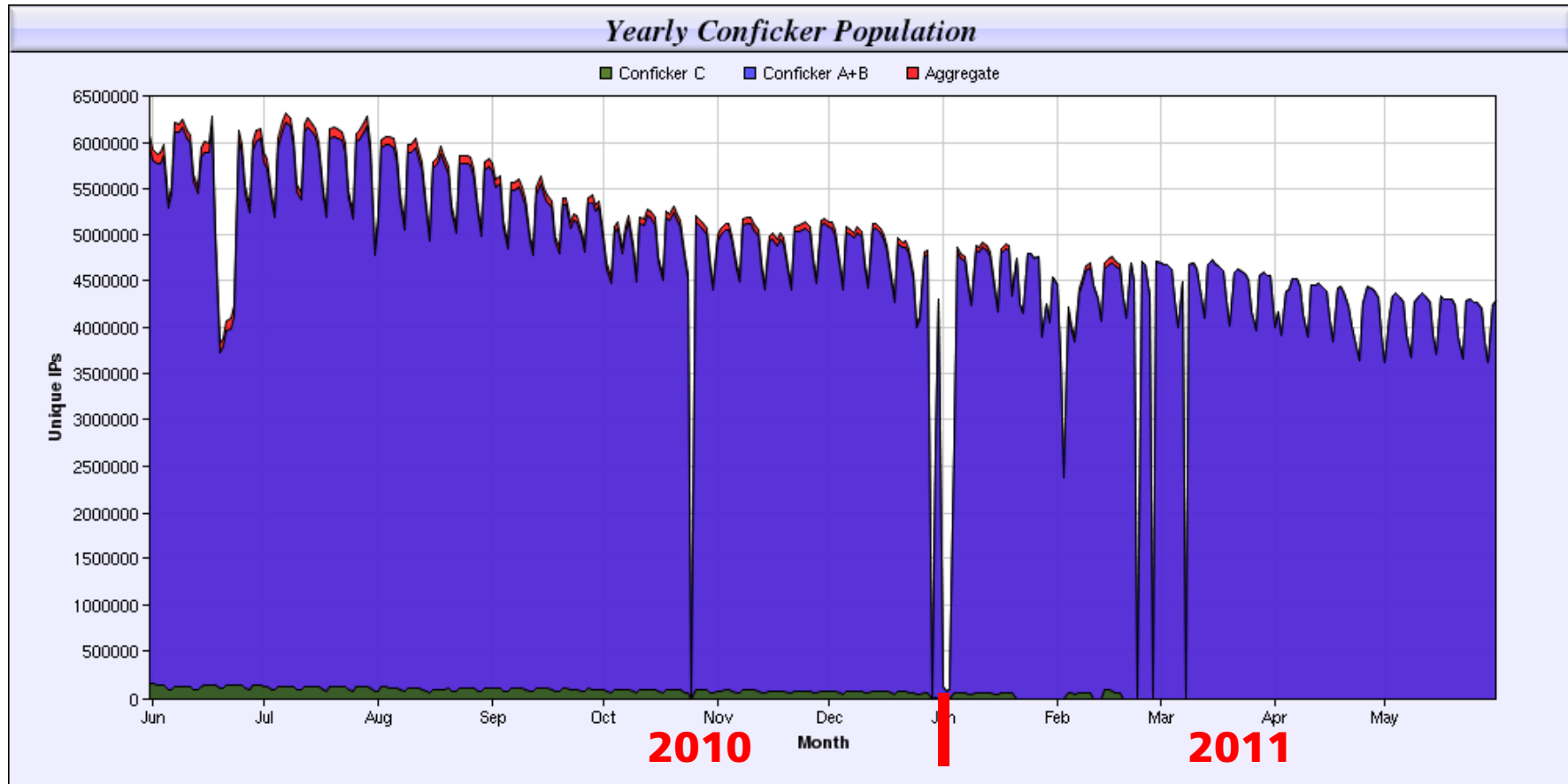
Number of Infected Systems



Quelle: <http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking>

Conficker

Number of Infected Systems



Quelle: <http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking>

Approaches to detection & measurement of botnets

Example method: Sinkholing

■ Conficker Sinkhole: “Population Data”

- „Many people equate **one IP to one system**, but that is **not usually the case**.” (impact: NAT, mobile devices, dial-up, ...)
- „The daily numbers should represent the **potential maximum level** of the infection, but in previous test cases usually prove to be much less than that maximum. So, **take the range of 25% to 75%** of the values that we display as the possible infection population and you will be close to the real value. And yes, this is a very large range, and you can see why **we do not like to quote any numbers for infection populations**, and why you will see very high and low numbers get quoted regularly depending on the **purpose of the person making the quote**.”

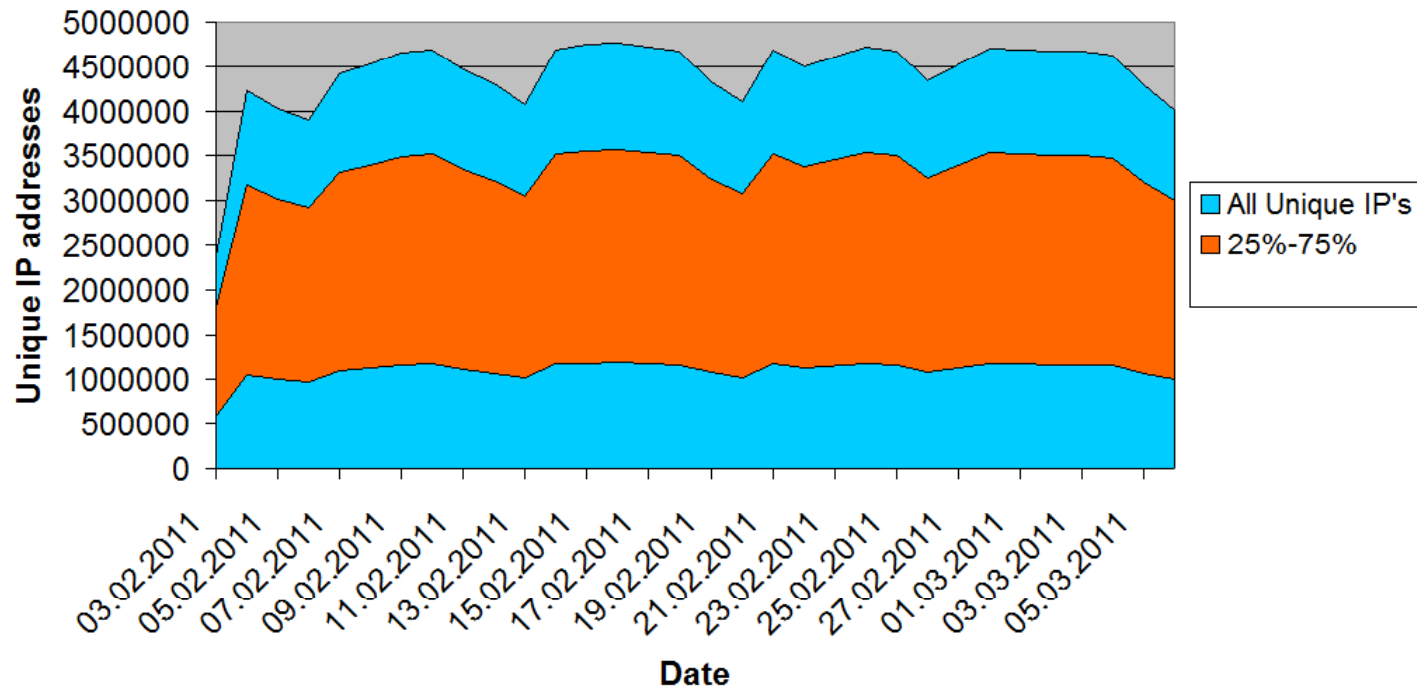
[Conficker Working Group Website: Section on infection tracking
<http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking>]

Approaches to detection & measurement of botnets

Example method: Sinkholing

■ Daily Conficker Sinkhole Data with 25-75% region marked

Conficker A+B+C Sinkhole



[Conficker Working Group Website: Section on infection tracking
<http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking>]

Advanced Malware Analysis Challenges

- Only **binary code** from executables is given
 - Blackbox view
 - Reverse Engineering
 - Static Analysis
 - Dynamic Analysis / Debugging
- Malware uses various mechanisms to **complicate analysis**
 - Timing traps
 - Obfuscation
 - Runtime modification of code
 - Cryptography
 - ...

Advanced Malware Analysis

Blackboxing / Sandboxing

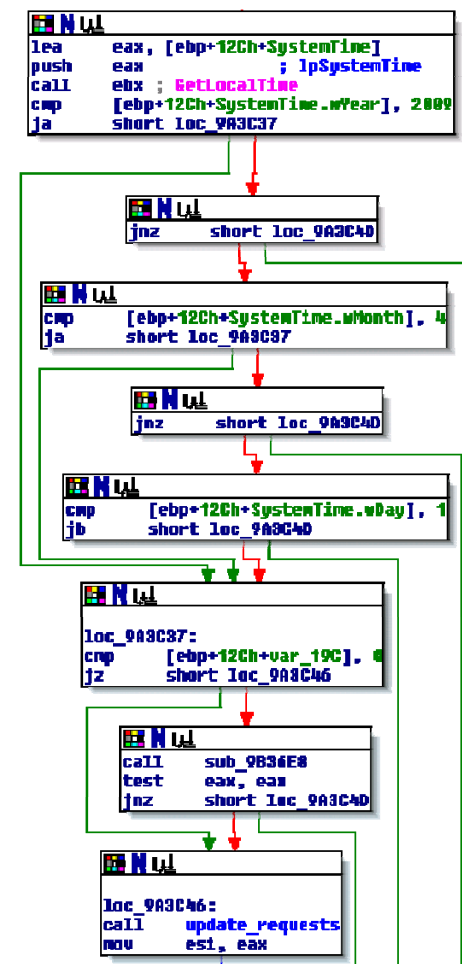
- Execution of malware in a **controlled** environment
 - secured against spreading
 - closely monitored
- Observation of behavior provides **insights** into the malware **functionality**
 - Integration / hooking into system
 - Malicious functionality (theft, spam, DDoS, spreading)
 - Command-and-control protocols and servers

Advanced Malware Analysis

Reverse Engineering

■ Static analysis

- Analysis without execution
- Assembly / Basic Block level
- Control flow analysis
- Data and Structure available
 - Strings, constants, ...
 - Functions, relationships, ...
- Detailed study of algorithms possible

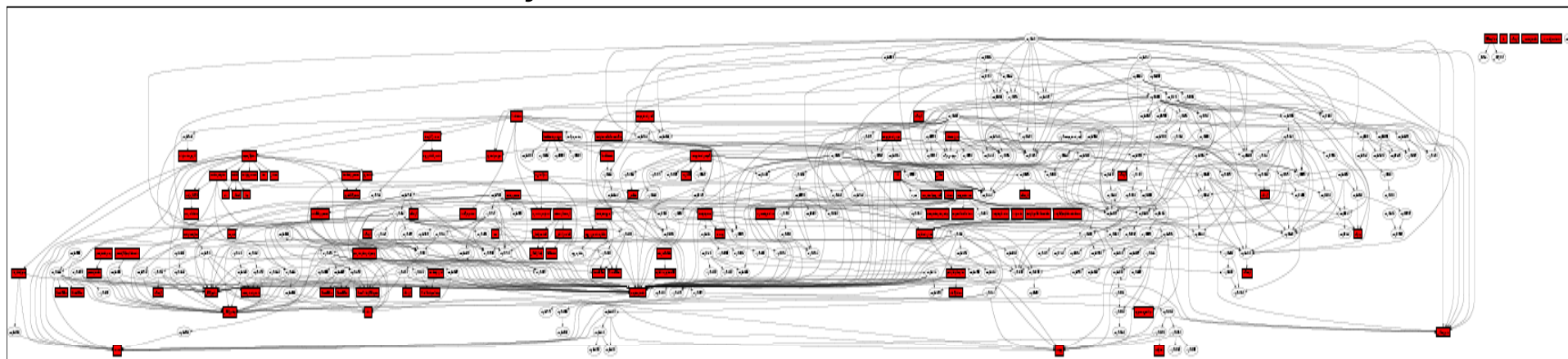


Advanced Malware Analysis

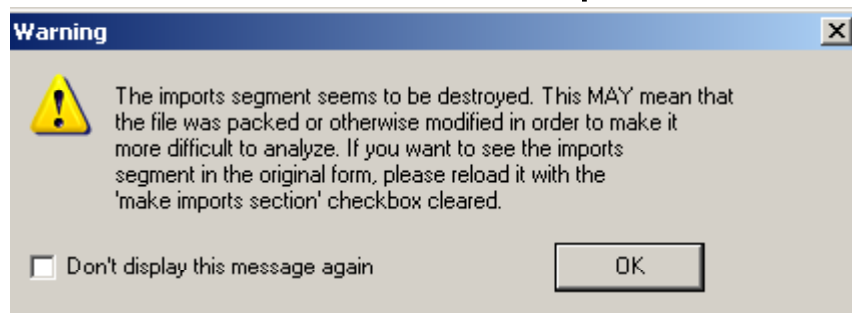
Reverse Engineering

- **Static analysis: Stepping stones**

 - Malware can easily consists of 1000+ functions



 - Malware can be packed (decrypts only during runtime)



Advanced Malware Analysis

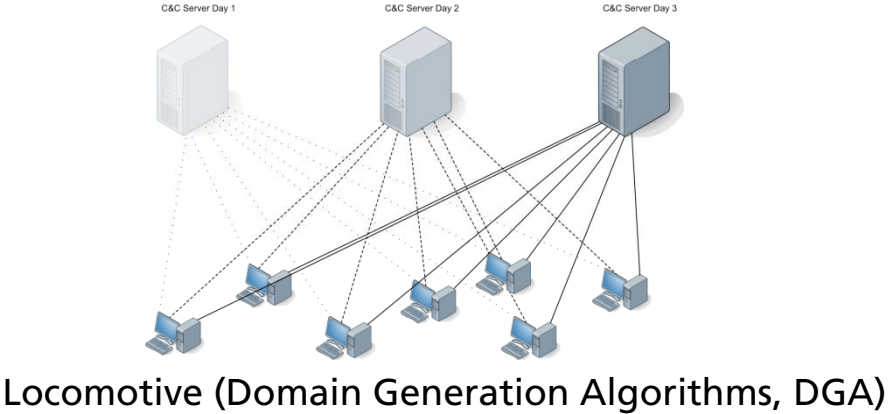
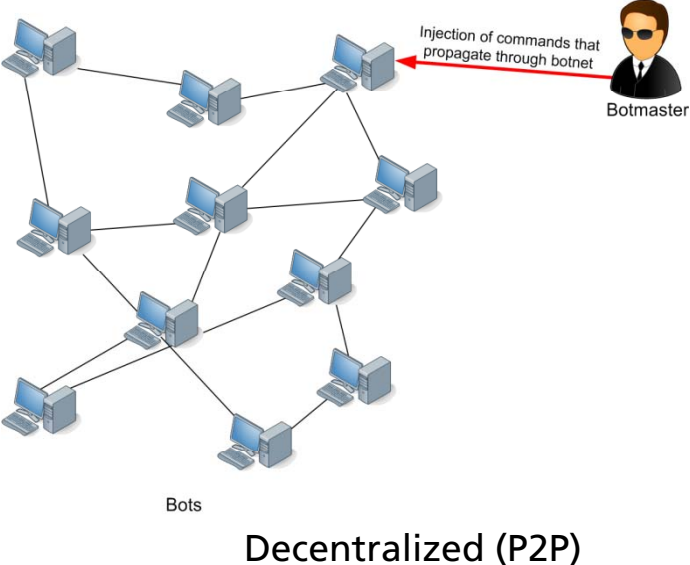
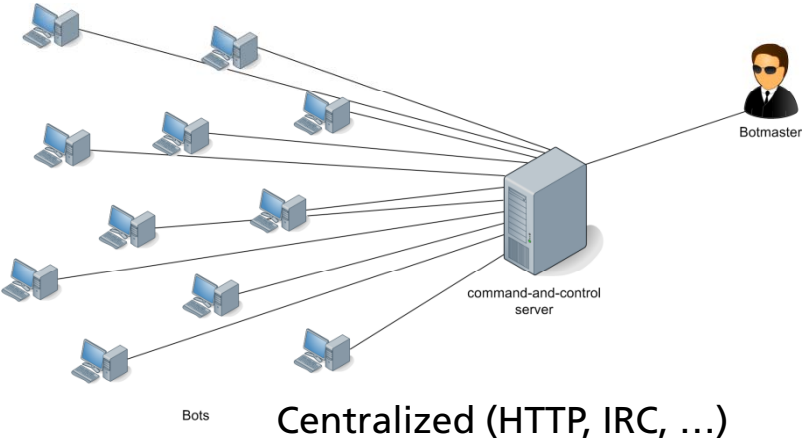
Benefits of analysis

- **Derivation of signatures** for
 - Anti-virus
 - Intrusion Detection Systems (IDS)
- Investigation of **C&C infrastructure**
 - C&C servers
 - C&C protocol
 - Weaknesses and possible vulnerabilities

Botnet Mitigation

Approaches to botnet countermeasures

Botnet Command&Control Structures



Approaches to botnet countermeasures

Current practices and challenges

■ Takedown of C&C Servers

- Abuse request to hosting provider: disconnect / power off server
- Challenge: non-cooperative (bulletproof) hosting

■ Handling of C&C domains

- Abuse request to registrar in charge: deregistration
- Register unused C&C domains in advance

■ De-Peering of rogue ISPs

- Benign ISP's decision cooperation needed to stop services
- Court: Restraining order (e.g. FTC vs. 3FN / Pricewert)

Approaches to botnet countermeasures

Current practices and challenges

- **Actions against botnet C&C infrastructure do not affect infections**
 - Systems remain instable and vulnerable
 - Many computers infected with multiple malware
 - Pay-per-install and update features can be used to extend botnet population
- **Incomplete takedowns may raise botnet resilience**
 - Infrastructure may be migrated after regaining control
 - „Teaching“ botmasters to update and enhance

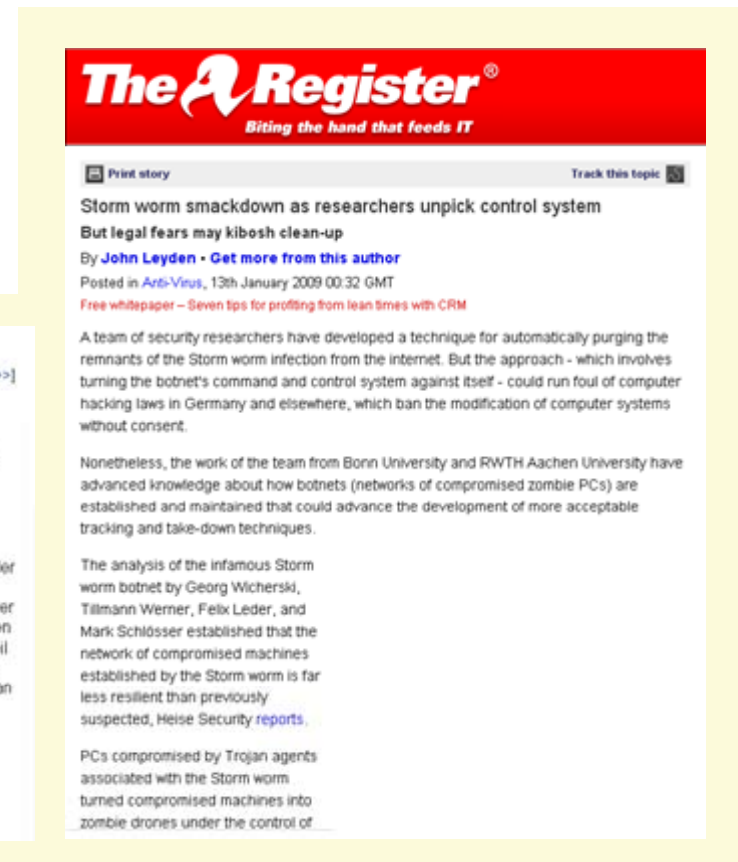
Combating Botnets

Examples of Successfully Investigated Botnets

- Storm Worm (2008)
- Waledac (2008)
- Kraken (2008)
- Conficker (2008-2009)



The screenshot shows a news article from Heise Security. The article title is "Sturmurm-Botnetz sperrangelweit offen" (Storm Worm botnet wide open). The text describes how a team of researchers from Bonn University and RWTH Aachen analyzed the botnet, finding it was not as perfect as it seemed. They discovered that the botnet was composed of infected computers that followed the commands of a control server and used peer-to-peer techniques to find new servers. The article also mentions that the researchers were able to turn some of the botnet's components against itself, which is a significant achievement in botnet takedown.



The screenshot shows a news article from The Register. The article title is "Storm worm smackdown as researchers unpick control system" (Storm worm smackdown as researchers unpick control system). The text describes how a team of security researchers developed a technique for automatically purging the remnants of the Storm worm infection from the internet. The article also mentions that the researchers were able to turn the botnet's command and control system against itself, which is a significant achievement in botnet takedown.

Additional Reading



Botnets: Measurement, Detection, Disinfection and Defence — ENISA - Mozilla Firefox

http://www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-and-defence

enisa European Network and Information Security Agency A EUROPEAN UNION AGENCY

Home About ENISA **Our Activities** Publications Press & Media Events Recruitment Public Procurement

you are here: home > our activities > resilience > botnets > botnets: measurement, detection, disinfection and defence

Resilience

- Policies and Strategy
- Providers' Measures
- Technologies
- Recommendations
- Related Areas
- Press Corner
- Workshops
- Contact Us

Botnets

- Botnets: 10 Tough Questions
- Botnets: Measurement, Detection, Disinfection and Defence
- Presentations from the workshop: Botnets, Measurement, Detection, Disinfection and Defence
- Policy statement
- Cyber Europe 2010

Botnets: Measurement, Detection, Disinfection and Defence

"Botnets: Measurement, Detection, Disinfection and Defence" is a comprehensive report on how to assess botnet threats and how to neutralise them. It is survey and analysis of methods for measuring botnet size and how best to assess the threat posed by botnets to different stakeholders. It includes a comprehensive set of 25 different types of best-practices to measure, detect and defend against botnets from all angles. The countermeasures are divided into 3 main areas: neutralising existing botnets, preventing new infections and minimising the profitability of cybercrime using botnets. The recommendations cover legal, policy and technical aspects of the fight against botnets and give targeted recommendations for different groups.

Publication date: Mar 07, 2011

Authors:
 Editor: Dr. Giles Hogben
 Authors: Daniel Plohmann, Elmar Gerhards-Padilla, Felix Leder

Downloads

Full report: ENISA_Botnets_Measurement_Defence.pdf — PDF document, 3958Kb

Language: English

Print this —

Share

Done

videos

- enisa
- enisa

flyers

- Botnets - Measurement, Defence and Disinfection
- Inter-X: Resilience of the Internet Interconnection Ecosystem
- Measurement Frameworks and Metrics for Resilient Networks and Services
- Reporting Major Security Incidents - Implementation of Article 13a
- Trusted Information Sharing

press releases

Take Home Messages

1. Complex IT Systems are vulnerable

- The Anti Virus Industry lost the battle a long time ago.
- There is a whole economy around malicious software.
- Botnets add Command&Control: They pave the way for organized attacks.

2. The Genie is out of the Bottle: Botnets are here to stay with us

- Deterrence does not really work today (issue of attribution).
- International Co-Operation is essential: Co-Operative Defense against Cyber Attacks.

3. Resilience is Essential

- Something will happen.
- Make sure that the effects of the Unknown can be controlled.



Practically relevant solutions for detecting, analyzing, and responding to cyber attacks

Monitoring & Situational Awareness

IDS for heterogeneous Networks
Operational Picture & Situational Awareness
Intrusion Response

Resource-efficient Cryptography

Efficient Key Management
Application Protection Protocols
Network Protection Protocols

cydef@fkie.fraunhofer.de

+49 (228) 9435 - 378

Digital Forensics & Malware Analysis

Malware Analysis
Digital Forensics
Honeypots/Honeynets
Botnet Analysis

Secure Network Architectures

Interoperable Coalition
Architectures
Multi-Level Security
Gateway Concepts
Protected Core Networking
