Keynote

Udo Helmbrecht
Executive Director, ENISA

Workshop on Botnet Detection, Measurement, Disinfection & Defence

Cologne, Germany, 10 March 2011

Overview

- Background – ENISA's related work
- Assessing and addressing the botnet threat
- Bird's eye view of ENISA's report and key recommendations

ENISA

- The European Network and Information Security Agency
  - Gives expert advice on NIS issues to national authorities and EU institutions
  - Acts as a forum for sharing good NIS practices
  - Facilitates information exchange and collaboration between EU institutions, national authorities and businesses on NIS issues.
  - Set up in 2004
  - Around 60 staff.
- ENISA has an advisory role (not operational) and the focus is on prevention and preparedness.

EP3R

- EP3R is the European Public-Private Partnership for Resilience.
  - EP3R builds on National PPPs to address Pan-European dimensions of Critical EU Infrastructure; E.g. cross border dependencies, cascading failures.
- Objectives of EP3R
  - Reduce the need for regulation through industry self-regulation
  - Discuss public policy priorities, objectives and measures;
  - Information sharing and stock taking of good policy and industrial practices

EP3R

- ENISA is supporting the establishment of 3 working groups:
  - WG1 : Identification of Cross-Border and Cross-Sectoral ICT Security and Resilience Interdependencies
  - WG2 : Pan European Security and Resilience Baseline Requirements
  - WG3 : Coordination and Cooperation Strategies for Preventing and Responding to Large Scale Disruptions (Focuses on **Exercises** and **Botnets**)
    - ENISA report: Botnets, Measurement, Disinfection and Defence will feed the recommendations

Pan-European Exercises: Objectives

- Increase understanding on how cyber incidents are handled by Member States
- Test communication points and procedures between participating MSs
- Build trust among participants; help towards establishing mutual support procedures
- Highlight interdependencies between MS across Europe
- Taking an important step towards creating a CIIP community

Format & Participation

- Table top exercise
- In 2010 only public authorities/bodies of M
  - agencies, CERTs, ministries, law enforcement bodies
- Participation
  - 70 organisations and 150 experts
  - 22 countries players and 8 countries observers
  - 320 injects (simulated adverse effects)
- Conducted – 4th of November 2010

Draft Findings

- Incident handling in Member States varies a lot
  - Roles & responsibilities, operating procedures, information sharing
- Lack of pan-European preparedness measures to test
  - No common/baseline operating procedures for responding to and recovery from attacks/incidents
- Different directories are used for information sharing and mutual response
  - No need to create one, new pan-European directory of contacts
  - Existing ones are sufficient but need regular update

ASSESSING AND ADDRESSING THE BOTNET THREAT

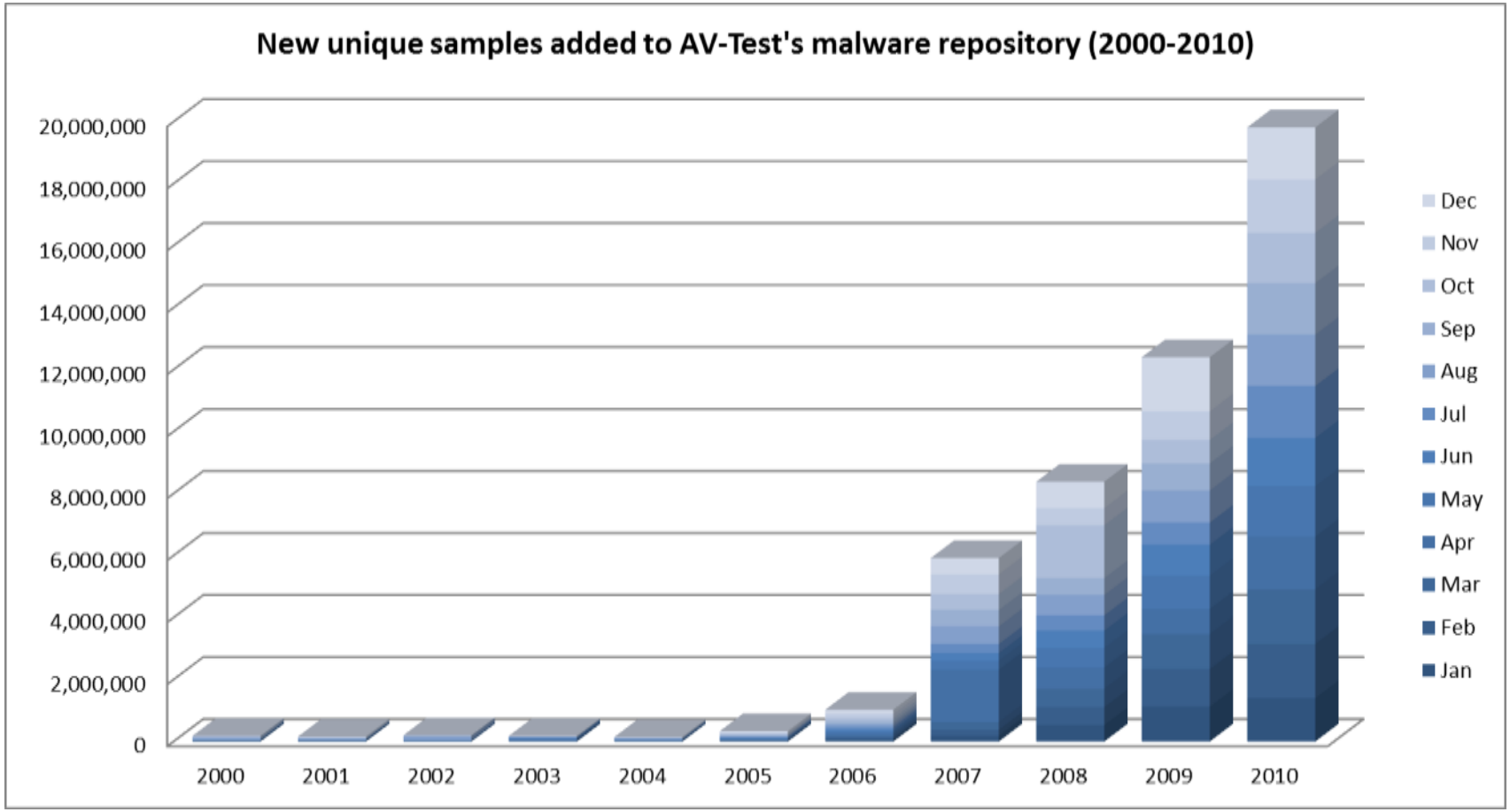
Root causes

- Ease and low cost of infecting a user's PC with malware.
- End users don't feel responsible
- The profit which can be gained by running a botnet (vs the effectiveness of defensive measures).
- Inability to bring cybercriminals to justice.

Malware Trends

Threats	2007	2009	Forecast
Zero-day exploits	↑	↑	→
Drive-by downloads	—	↑	↑
Trojan horses	↑	↑	↑
Viruses	↓	↓	→
Worms	↓	↓	→
Spyware	↑	↑	→
DDoS attacks	→	↑	↑
Unsolicited e-mail	↑	↑	↑
Bot networks	→	↑	↑
Identity theft	↑	↑	↑

Source: BSI 2009



Source, AV-Test

FIGURE 14. The 25 locations with the most bot cleanings in 2Q10

Rank	Country/Region	Computers with Bot Cleanings (1Q10)	Computers with Bot Cleanings (2Q10)	Bot Cleanings Per 1,000 MSRT Executions (Bot CCM)
1	United States	2,163,216	2,148,169	5.2
2	Brazil	511,002	550,426	5.2
3	Spain	485,603	381,948	12.4
4	Korea	422,663	354,906	14.6
5	Mexico	364,554	331,434	11.4
6	France	344,743	271,478	4.0
7	United Kingdom	251,406	243,817	2.7
8	China	227,470	230,037	1.0
9	Russia	181,341	199,229	4.3
10	Germany	200,016	156,975	1.4
11	Italy	191,588	130,888	2.6
12	Turkey	91,262	98,411	4.7
13	Canada	96,834	87,379	1.4
14	Netherlands	115,349	77,466	2.5
15	Colombia	76,610	71,493	5.8
16	Portugal	83,379	68,903	5.7
17	Australia	72,903	66,576	2.8
18	Poland	87,926	62,704	3.9
19	Taiwan	52,915	54,347	3.4
20	Japan	63,202	52,827	0.6
21	Argentina	38,229	43,162	3.8
22	Saudi Arabia	33,283	40,793	5.5
23	Belgium	51,689	39,508	3.4
24	Chile	37,705	39,245	5.1
25	India	37,895	38,954	1.0

The need to assess the threat level

- **Deciding on investments (100's of millions of Euros):** in security measures. For governments as well as for businesses.
- **Defining the political agenda:** Botnets are a major threat to society to be engaged on governmental level.
- **Reporting and journalism**: By providing information to the public, awareness of security issues is raised.

Incentives for exaggeration

- Funding
- Media attention
- Not appearing to be “easy prey” for attackers
- Not giving away your defensive capabilities.

Currently many estimates are inaccurate

- Presentation without mentioning of concrete methodology
- Measurements not easily reproducable
- Measurable characteristics influenced by effects of Internet structure
  - Numbers are over-estimated through “churn” – reuse of IP addresses so that the same bot shows up several times
  - But also sometimes underestimated through NAT (Network Address Translation) – meaning that several bots appear behind the same IP address

Edit View History Bookmarks Tools Help

http://www.smh.com.au/technology/security/a-quarter-of-us-pcs-infected-with-malwa

Google

st Visited Getting Started Latest Headlines 25 percent of US comp...

quarter of US PCs infected ...

AM Saturday Jul 17, 2010 | 644 online now See today's paper

SMH | Domain | Drive | MyCareer | RSVP | Newsletters

smh.com.au

he Sydney Morning Herald

echnology

ews Biz-Tech Security Enterprise Sci-Tech Blogs Digital Life Compare & Save

u are here: Home » Technology » Security » Article

Search here... Technology

A quarter of US PCs infected with malware: OECD

June 2, 2008

Advertisement

oin the conversation

u're the only person reading this
w. Tell your friends

mment on Twitter .

Ads by Google

Telecom Sparkle Germany

Discover where we are, our Network and our Offices in your Country !

One in ten websites 'is infected with malware' - Times Online .

File Edit View History Bookmarks Tools Help

http://technology.timesonline.

Most Visited Getting Started Latest Headlines 25 percent of US com

One in ten websites 'is infecte...

1

THE TIMES | THE SUNDAY TIMES | TIMES+

THE TIMES
THE SUNDAY TIMES

Archive Article Please enjoy this article from The Times & The Sunday Tim

From Times Online

May 14, 2007

One in ten websites 'is infected with malware'

Jonathan Richards

About one in ten websites is infected with malicious software that

US Edition Companies Hardware Software Mobile Security Researc

Zero Day

Ryan Naraine and Dancho Danchev

Mobile
RSS
Email Alerts

145 Comments Share Print Facebook Twitter Recommend 36 Votes

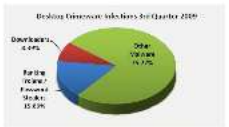
Home / News & Blogs / Zero Day

Report: 48% of 22 million scanned computers infected with malware

By Dancho Danchev | January 27, 2010, 2:42pm PST

Summary

The recently released APWG report shows that 48% of the 22 million scanned computers are infected with malware. Over a million and a half are infected with crimeware/banker trojans.



The recently released APWG Phishing Activity Trends Report for Q3 of 2009, details record highs in multiple phishing vectors, but also offers an interesting observation on desktop crimeware infections.

According to the report, the overall number of infected computers (page 10) used in the sample decreased compared to previous quarters, however, 48.35% of the 22,754,847 scanned computers remain infected with malware.

Most Visited Getting Sta

Malware worldwide gro

home | reviews news

cnet news

Latest News CNET River BETA Webware Crave Business Tech Green Tech Wireless

Home > News > Security

Security

September 29, 2009 11:51 AM PDT

Malware worldwide grows 15 percent in September

by Lance Whitney

Font size Print E-mail Share 42 comments

111 retweet Share 40

A rise in malware has caused the number of infected PCs worldwide to increase 15 percent just from August to September, says a report released Tuesday from antivirus vendor Panda Security.

267 diggs

Across the globe, the average number of PCs hit by malware now stands around 59 percent, an all-time

Join CNET

Sign in or jo
your softwe

cnet Recently Viewed Products My Lists TechTracker

Unsecured Economies – A Trillion Dollar Headwind

Thursday, January 29, 2009 at 5:53pm by David DeWalt

At Davos this week, I've had the opportunity to speak with world leaders about the most pressing issues of the day. Among the issues we've been discussing is the true cost of cybercrime, and the incredible drag it's creating on the global economy. To underscore that point, we just announced the results of the first research to look into how the global economic downturn is affecting corporate data loss.

There are a couple of factors that have created a perfect storm for the challenges we're seeing. Some have been in the making for quite some time, others are more recent.

For those who have read The World is Flat, by Thomas Friedman, you understand the forces that are driving companies to store higher percentages of critical data offshore. With cheaper labor forces, you've got an extended supply chain that creates new challenges. With the world flattening, it's created a perfect storm for data loss.

We continue to see major data breaches, such as Heartland, that are causing major damage to stock values and corporate reputations. We're seeing a dramatic change in the landscape with IPv6, triple-play to the home, and connected devices. Now, basically anything with an IP address can be attacked by the

True story

- The first speaker told the audience there were hundreds of thousands of Storm infected nodes.
- A speaker in a panel on emerging threats referred back to the earlier speaker and said "millions of Storm infections“
- The lunch keynote speaker repeated the previous speaker's comment about Storm and said there were "tens of millions."
- Guess which number the press reported?

ENISA Report - Botnets: Measurement, Detection and Disinfection

- Provide a tool for policy makers to decide where to prioritise action.
  - Comprehensive survey and analysis of botnet measurement/detection and countermeasures
  - Best practice in botnet measurement based on real impact.
  - Best practice in countermeasures
- Ongoing information sharing among expert group on key questions and problems in the fight against botnets

Approach

- Assess measurement and defence methods and approaches according to a feature set.
- Invite group of international experts to provide input
- Let experts explain relevant methods against botnet
- Let experts discuss on important topics / tough questions

Group Composition

- National and pan European Internet Service Providers: 3
- Antivirus Software Developers and Security Solutions Providers: 21
- Operating System Providers: 4
- Application and Network Providers and Developers: 2
- Web 2.0 and Social Network Site Providers: 1
- Academia: 4
- CERTs: 14
- Online User Communities and Consumer Protection Associations: 3
- Regulators and Policy Makers: 7
- Law Enforcement Agencies: 3
- Pan European Associations of Providers: 4

Deliverables

- Botnets: Detection, measurement, disinfection and defence – best practice and analysis. http://www.enisa.europa.eu/botnets
- Botnets: 10 hard questions – Analysis by ENISA and expert group. http://www.enisa.europa.eu/botnets-10Q
- Legal analysis and recommendations. In preparation

Major recommendations

- Addressing the problem from all angles, all stakeholders
- Divided into 3 areas
  - Mitigate existing Botnets
  - Prevent new infections
  - Minimise profitability of botnets and cybercrime

Major areas of recommendations

- Mitigate existing botnets – e.g.
  - Target botnets both at C&C and individual bot level
  - Use special position of ISPs / reimbursement models for their efforts (such projects are on the way)
- Prevent new infections
  - Early detection of threats
  - Protect systems/raise user awareness
- Minimise profitability of botnets and cybercrime
  - Target assets in cybercriminal value creation chain
  - Improve anti-fraud, prosecute botmasters
  - Support victims in prosecuting criminals

Key message for policy makers

- Application layer vulnerabilities are a big factor in the spread of botnets
  - Ease of installing malware
  - Ease of attacking online services
  - Command and control via web services
- Focus of countermeasures should include web service providers, application software developers, not just ISP's and telecoms

Key messages

- Measurement and detection needs improvement
- Focus on application layer vulnerabilities.
- The global and European botnet threat can only be countered by a close international cooperation between governments, technically-oriented, and legislative institutions

Contact

Prof Udo Helmbrecht
Executive Director

European Network and Information Security Agency

Science and Technology Park of Crete (ITE)

P.O. Box 1309

71001 Heraklion - Crete – Greece

udo.helmbrecht@enisa.europa.eu

www.enisa.europa.eu