# Forum on DNS Abuse

*June 25, 2012*

*Moderator:*

*Ondrej Filip,  CEO CZ.NIC*

No. 44 • 24-29 JUNE 2012

ICANN PRAGUE

One World

One Internet

# Introduction

No. 44 • 24-29 JUNE 2012

ICANN PRAGUE

One World

One Internet

# Martin Peterka
# Operations Manager
# CZ.NIC

No. 44 • 24-29 JUNE 2012

ICANN PRAGUE

# CZ.NIC & security

CZ.NIC z.s.p.o. / http://www.nic.cz

Martin Peterka / martin.peterka@nic.cz
Operations director

25. 6. 2012, ICANN 44 | Prague

cz.
nic | CZ DOMAIN REGISTRY

# Agenda

- About CZ.NIC
- Our security teams
- Solved incidents
- Our proactive tools

# About CZ.NIC

- Special interest association of legal entities
- Founded in 1998 by leading ISPs
- Currently 103 members – growing (open membership)
- 50+ employees
- Core business – domain registry .cz
- MoU with Czech government and NSA
- Part of State's critical infrastructure
- Non profit, Neutrality
- Variety of other activities

cz nic | CZ DOMAIN REGISTRY

# CZ.NIC-CSIRT

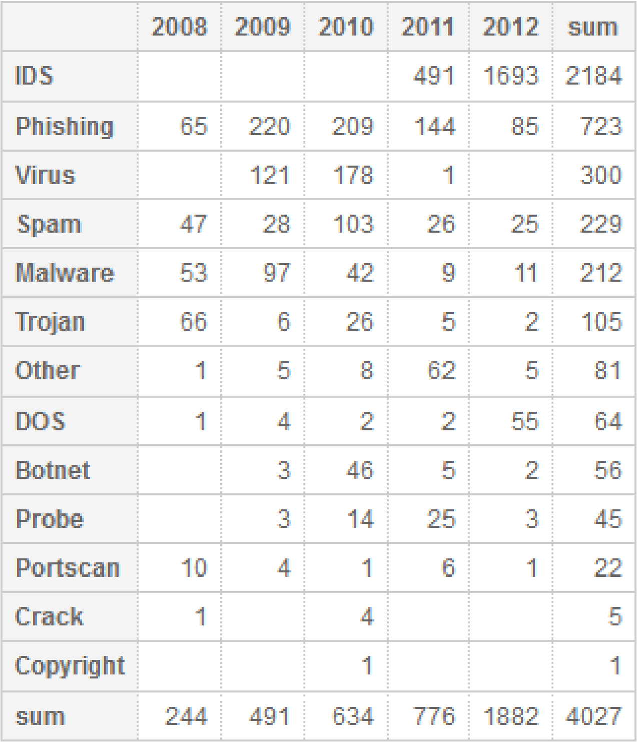
- incident handling within AS25192 and incident relating to nameservers for .cz and 0.2.4.e164.arpa
  - no incidents, just our own network
- We are entitled to deactivate a domain if is used in a fashion that endangers the national or international computer security
  - harmful content (especially viruses, malware) are distributed
  - the content of a different service is masqueraded (eg phishing),
  - domain becomes a control centre of interlinked hardware network distributing the harmful content (especially botnet)
- Deactivation for 1 month, even repeatedly

# CSIRT.CZ

- National, last resort CSIRT – no executive power
- Operation since 1 Jan 2011
  - Day-by-day operation and transfer of agenda from CESNET
- Full operation since Jun 2011
- Mainly incident handling/reporting – very successful
- But also a pro-active steps – detection of open unsecured DNS resolvers – cooperation with Security Information Service (BIS)
- Community meetings
- Cooperation – Terena, FIRST, ENISA, team CYMRU
- „accredited“ by TERENA TI (10/2011)

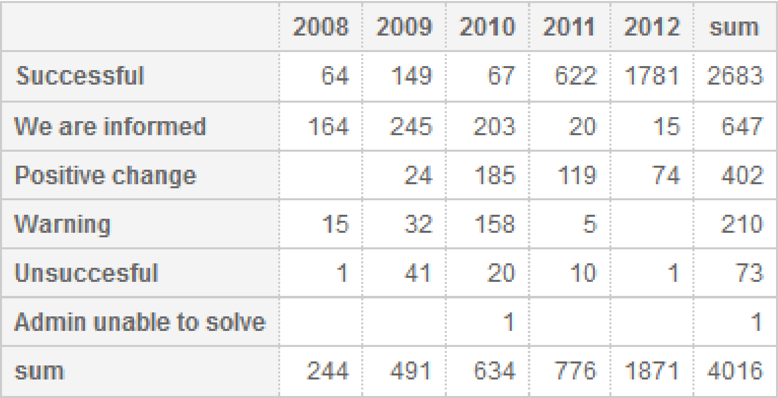
# CSIRT.CZ - statistics

Number of incidents by type (open and closed cases)



| | 2008 | 2009 | 2010 | 2011 | 2012 | sum |
|---|---|---|---|---|---|---|
| IDS | | | | 491 | 1693 | 2184 |
| Phishing | 65 | 220 | 209 | 144 | 85 | 723 |
| Virus | | 121 | 178 | 1 | | 300 |
| Spam | 47 | 28 | 103 | 26 | 25 | 229 |
| Malware | 53 | 97 | 42 | 9 | 11 | 212 |
| Trojan | 66 | 6 | 26 | 5 | 2 | 105 |
| Other | 1 | 5 | 8 | 62 | 5 | 81 |
| DOS | 1 | 4 | 2 | 2 | 55 | 64 |
| Botnet | | 3 | 46 | 5 | 2 | 56 |
| Probe | | 3 | 14 | 25 | 3 | 45 |
| Portscan | 10 | 4 | 1 | 6 | 1 | 22 |
| Crack | 1 | | 4 | | | 5 |
| Copyright | | | 1 | | | 1 |
| sum | 244 | 491 | 634 | 776 | 1882 | 4027 |

Incident resolution states (only closed cases)



| | 2008 | 2009 | 2010 | 2011 | 2012 | sum |
|---|---|---|---|---|---|---|
| Successful | 64 | 149 | 67 | 622 | 1781 | 2683 |
| We are informed | 164 | 245 | 203 | 20 | 15 | 647 |
| Positive change | | 24 | 185 | 119 | 74 | 402 |
| Warning | 15 | 32 | 158 | 5 | | 210 |
| Unsuccesful | 1 | 41 | 20 | 10 | 1 | 73 |
| Admin unable to solve | | | 1 | | | 1 |
| sum | 244 | 491 | 634 | 776 | 1871 | 4016 |

CSIRT.CZ
powered by CZ.NIC

# Incidents

- Examples of 2 incidents
- DNS amplification DDOS (June 2012)
  - Solved by CSIRT.CZ
- Phishing sites (2010)
  - Solved by CZ.NIC-CSIRT

# DNS amplification DDOS

- 2012, solved by CSIRT.CZ
- Attack to the Latvian bank
- Thousands open relay DNS server from all over the world
  - Most of them from USA, 172 from Czech Republic
- Our team solved it at the request of CERT NIC.LV
- Procedure
  - Sort IP’s
  - Find information (companies, admins)
  - Ask for correction
- Cca 50% DNS fixed
- Still in progress

# Phishing attack

- 2010, solved by CZ.NIC-CSIRT
- Target – IRS
- Trojan horse at pages
- During 5 days registered 150 domains
  - Different registrars
  - Different nameservers
  - Fast flux
  - Paid by stolen credit cards
- All domains were deactivated for 1 month
- Immediate response, cooperation with registrars

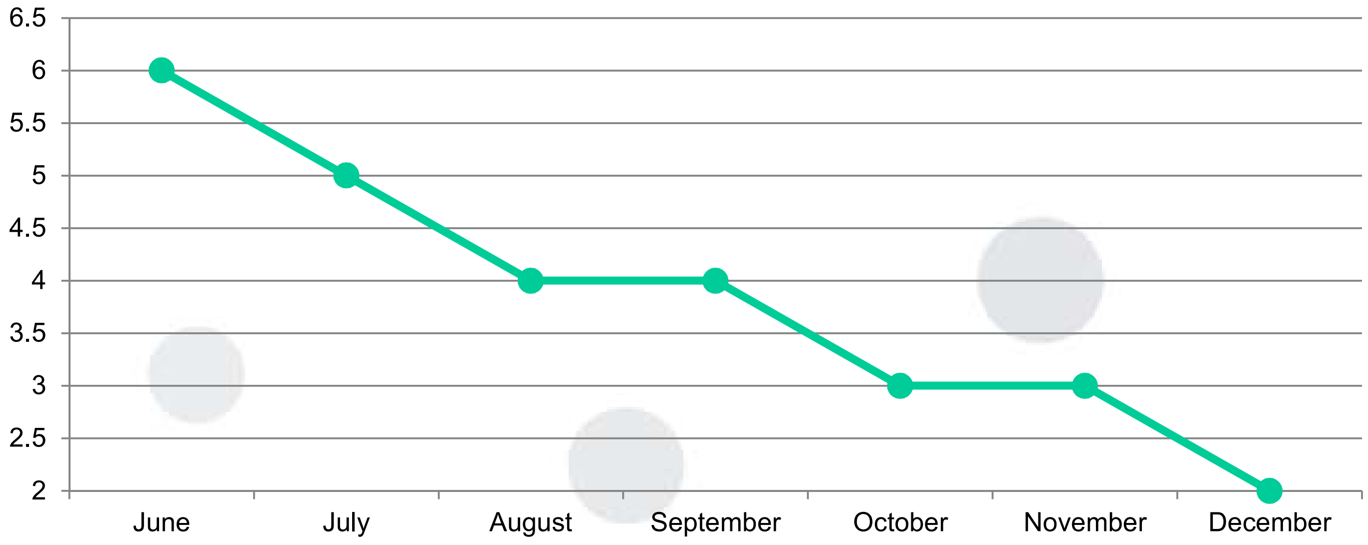
# Lesson learned – we need to be proactive

- Developing of MDM - Malicious Domain Manager
  - In cooperation with CZ.NIC.LABS
- Takes data from public sources
  - Malwarepatrol, Phishtank, Zeus Tracker Abuse.ch, ...
  - Focused on malware, phishing, domains as C&C botnets, etc.
- Selects sites/sources within .cz domain
- Searches for contact information
- Is connected to the ticket system
  - allows controlled communication with the administrators of the sites
- Started in June 2011

# MDM - results

- Since June 2011 cleaned
  - 11 649 pages in
  - 2 299 domains

**% of phishing pages within .cz June-Dec 2011**
**Source : http://www.phishtank.com/**



**https://git.nic.cz/redmine/projects/mdm**

# ?

# Questions ?

# Thank you!

Martin Peterka / *martin.peterka@nic.cz*
http://www.nic.cz

One World

One Internet

## Branko Stamenković
## Head of the Special Public Prosecutor's Office for High-Tech Crime of Serbia

No. 44 • 24-29 JUNE 2012

ICANN PRAGUE

One World

One Internet

# Christopher Landi and Christopher Malone Cyber Crimes Center U.S. Department of Homeland Security

No. 44 • 24-29 JUNE 2012

ICANN PRAGUE

# Investigative Methodology: IP Address

- Agent obtains suspect IP address
- Agent conducts IP address check using WhoIs, APNIC, ARIN, Domain Tools, etc.
- Agent obtains ISP information; generates subpoena for subscriber information – may take 14 – 30 days for response from provider
- If ISP/record holder information is incorrect, additional research; generate new subpoena
- Agent obtains subscriber information, which may or may not be the same as target information

# Investigative Methodology: IP Address

- Agent conducts investigative activities to determine target, including:
  - Surveillance
  - Checks of additional records
  - U/C activities
  - Addl' traditional investigative techniques
- Delays in obtaining accurate IP information can delay following steps in investigation/enforcement actions

# Domain Name Seizures

The following measures are implemented to make every effort to ensure no legitimate activity is disrupted through the seizure of domain names:

- Identify the full Uniform Resource Locator (URL) hosting the illegal content
- Identify the specific area of the URL where the illegal content or contraband content is hosted; i.e. sub domain (third level domain), sub folder.  (It should be noted that the terms URL(s) and website(s) are used interchangeably)
- If the illegal content is hosted on a sub folder( e.g., ***website.com/illegalcontent***) where the illegal content is hosted in the ***illegalcontent*** sub folder off of the URL ***website.com***, the following steps will be taken

# Domain Name Seizures

- Verify the content at URL ***website.com/illegalcontent***, as stated above

- Capture the contents of the website to preserve/evidentiary value

- Identify the listed registrant of ***website.com*** through open source tools available on the Internet (e.g: WhoIs, APNIC, Domain Tools, etc.)

- Identify and verify the content hosted at the URL ***website.com***

- Identify any potential legitimate activity associated with ***website.com***

- If no legitimate activity or other associations can be identified, the domain ***website.com*** may be marked for seizure

# Domain Name Seizures

If the illegal content is hosted on a sub domain (third level domain - e.g., ***illegalcontent.website.com***), the following steps will be taken:

a. Verify the content at URL ***illegalcontent.website.com***

b. Capture the contents of the site to preserve the structure and content of the site at the time of access

c. Identify the listed registrant of ***website.com*** through open source tools available on the Internet

*Generally, it is not possible to identify the registrant of the third level domain through open source tools. The registrant of the second level domain has control over issuing third level domains linked to their second level domain and would have to update the registrant records to reflect any third level domain that was controlled by someone else. **No seizures occur without some form of legal process**.

One World

One Internet

# Questions

# Thank You

No. 44 • 24 - 29 JUNE 2012

ICANN PRAGUE

# Forum on DNS Abuse

*June 25, 2012*

*Moderator:*

*Ondrej Filip,  CEO CZ.NIC*

No. 44 • 24-29 JUNE 2012

ICANN PRAGUE

One World

One Internet

# Introduction

No. 44 • 24-29 JUNE 2012

ICANN PRAGUE

One World

One Internet

# Martin Peterka
# Operations Manager
# CZ.NIC

No. 44 • 24-29 JUNE 2012

ICANN PRAGUE

# CZ.NIC & security

CZ.NIC z.s.p.o. / http://www.nic.cz

Martin Peterka / martin.peterka@nic.cz
Operations director

25. 6. 2012, ICANN 44 | Prague

cz.
nic | CZ DOMAIN REGISTRY

# Agenda

- About CZ.NIC
- Our security teams
- Solved incidents
- Our proactive tools

# About CZ.NIC

- Special interest association of legal entities
- Founded in 1998 by leading ISPs
- Currently 103 members – growing (open membership)
- 50+ employees
- Core business – domain registry .cz
- MoU with Czech government and NSA
- Part of State's critical infrastructure
- Non profit, Neutrality
- Variety of other activities

# CZ.NIC-CSIRT

- incident handling within AS25192 and incident relating to nameservers for .cz and 0.2.4.e164.arpa
  - no incidents, just our own network
- We are entitled to deactivate a domain if is used in a fashion that endangers the national or international computer security
  - harmful content (especially viruses, malware) are distributed
  - the content of a different service is masqueraded (eg phishing),
  - domain becomes a control centre of interlinked hardware network distributing the harmful content (especially botnet)
- Deactivation for 1 month, even repeatedly

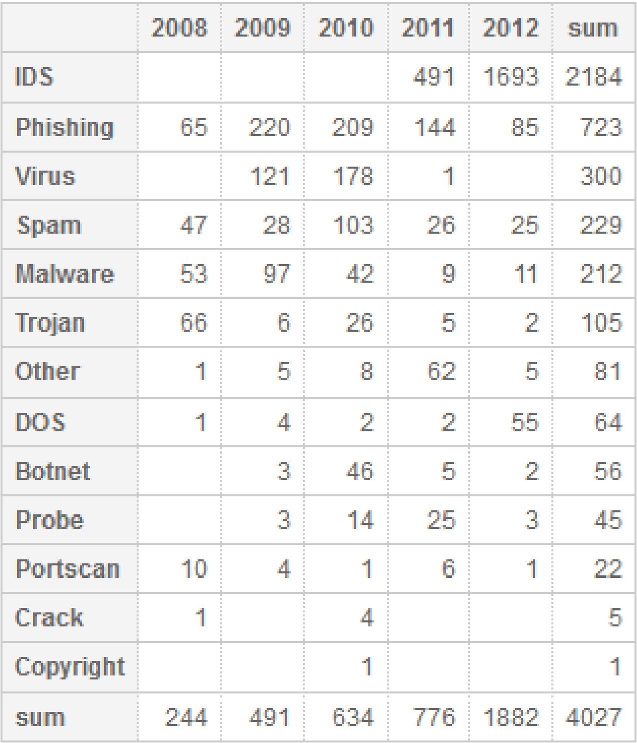
# CSIRT.CZ

CSIRT.CZ
powered by CZ.NIC

- National, last resort CSIRT – no executive power
- Operation since 1 Jan 2011
  - Day-by-day operation and transfer of agenda from CESNET
- Full operation since Jun 2011
- Mainly incident handling/reporting – very successful
- But also a pro-active steps – detection of open unsecured DNS resolvers – cooperation with Security Information Service (BIS)
- Community meetings
- Cooperation – Terena, FIRST, ENISA, team CYMRU
- „accredited“ by TERENA TI (10/2011)

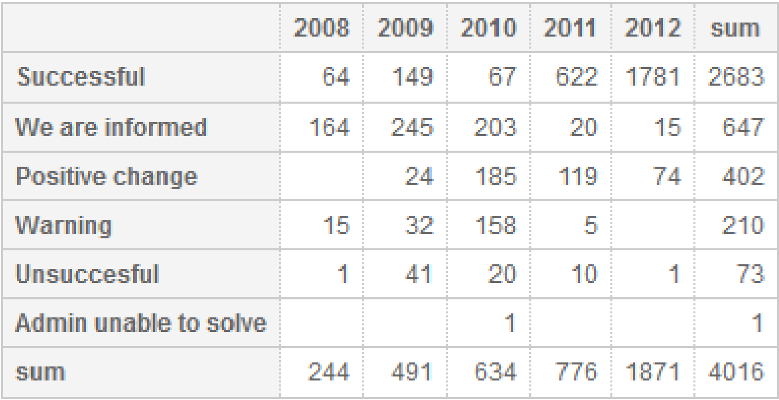
# CSIRT.CZ - statistics

Number of incidents by type (open and closed cases)



| | 2008 | 2009 | 2010 | 2011 | 2012 | sum |
|---|---|---|---|---|---|---|
| IDS | | | | 491 | 1693 | 2184 |
| Phishing | 65 | 220 | 209 | 144 | 85 | 723 |
| Virus | | 121 | 178 | 1 | | 300 |
| Spam | 47 | 28 | 103 | 26 | 25 | 229 |
| Malware | 53 | 97 | 42 | 9 | 11 | 212 |
| Trojan | 66 | 6 | 26 | 5 | 2 | 105 |
| Other | 1 | 5 | 8 | 62 | 5 | 81 |
| DOS | 1 | 4 | 2 | 2 | 55 | 64 |
| Botnet | | 3 | 46 | 5 | 2 | 56 |
| Probe | | 3 | 14 | 25 | 3 | 45 |
| Portscan | 10 | 4 | 1 | 6 | 1 | 22 |
| Crack | 1 | | 4 | | | 5 |
| Copyright | | | 1 | | | 1 |
| sum | 244 | 491 | 634 | 776 | 1882 | 4027 |

Incident resolution states (only closed cases)



| | 2008 | 2009 | 2010 | 2011 | 2012 | sum |
|---|---|---|---|---|---|---|
| Successful | 64 | 149 | 67 | 622 | 1781 | 2683 |
| We are informed | 164 | 245 | 203 | 20 | 15 | 647 |
| Positive change | | 24 | 185 | 119 | 74 | 402 |
| Warning | 15 | 32 | 158 | 5 | | 210 |
| Unsuccesful | 1 | 41 | 20 | 10 | 1 | 73 |
| Admin unable to solve | | | 1 | | | 1 |
| sum | 244 | 491 | 634 | 776 | 1871 | 4016 |

CSIRT.CZ
powered by CZ.NIC

# Incidents

- Examples of 2 incidents
- DNS amplification DDOS (June 2012)
  - Solved by CSIRT.CZ
- Phishing sites (2010)
  - Solved by CZ.NIC-CSIRT

# DNS amplification DDOS

- 2012, solved by CSIRT.CZ
- Attack to the Latvian bank
- Thousands open relay DNS server from all over the world
  - Most of them from USA, 172 from Czech Republic
- Our team solved it at the request of CERT NIC.LV
- Procedure
  - Sort IP’s
  - Find information (companies, admins)
  - Ask for correction
- Cca 50% DNS fixed
- Still in progress

CSIRT.CZ
powered by CZ.NIC

# Phishing attack

- 2010, solved by CZ.NIC-CSIRT
- Target – IRS
- Trojan horse at pages
- During 5 days registered 150 domains
  - Different registrars
  - Different nameservers
  - Fast flux
  - Paid by stolen credit cards
- All domains were deactivated for 1 month
- Immediate response, cooperation with registrars

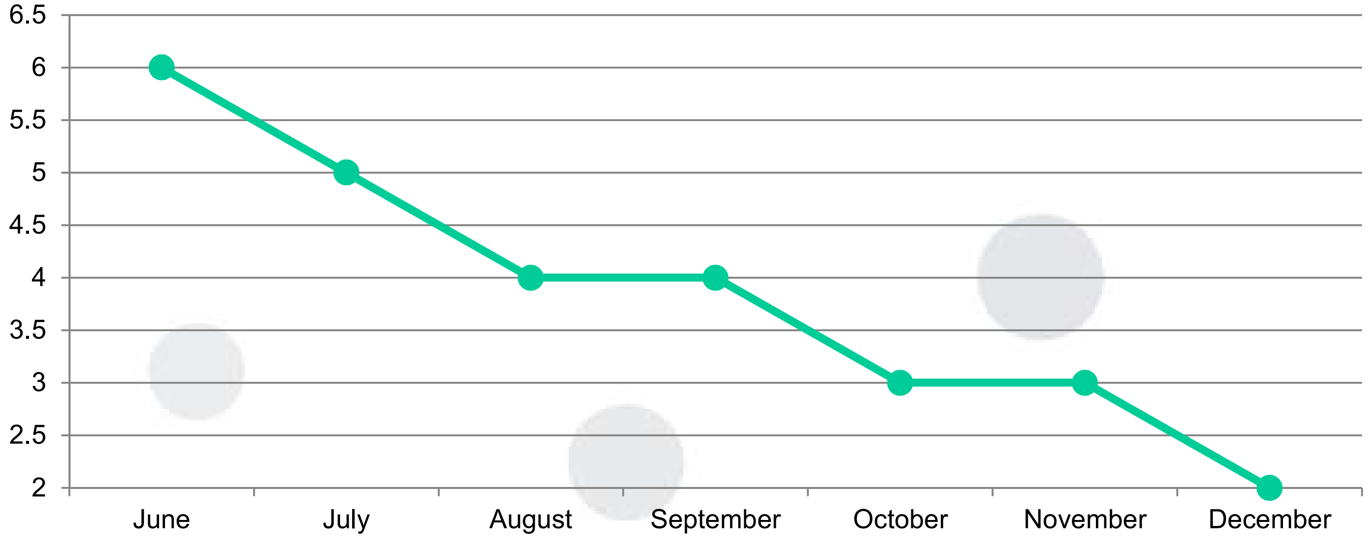
# Lesson learned – we need to be proactive

- Developing of MDM - Malicious Domain Manager
  - In cooperation with CZ.NIC.LABS
- Takes data from public sources
  - Malwarepatrol, Phishtank, Zeus Tracker Abuse.ch, ...
  - Focused on malware, phishing, domains as C&C botnets, etc.
- Selects sites/sources within .cz domain
- Searches for contact information
- Is connected to the ticket system
  - allows controlled communication with the administrators of the sites
- Started in June 2011

# MDM - results

- Since June 2011 cleaned
  - 11 649 pages in
  - 2 299 domains

**% of phishing pages within .cz June-Dec 2011**
**Source : http://www.phishtank.com/**



**https://git.nic.cz/redmine/projects/mdm**

?

## Questions ?

## Thank you!

Martin Peterka / *martin.peterka@nic.cz*
http://www.nic.cz

One World

One Internet

# Branko Stamenković
# Head of the Special Public Prosecutor's Office for High-Tech Crime of Serbia

One World

One Internet

No. 44 • 24-29 JUNE 2012

ICANN PRAGUE

# Christopher Landi and Christopher Malone
# Cyber Crimes Center
# U.S. Department of Homeland Security

# Investigative Methodology: IP Address

- Agent obtains suspect IP address
- Agent conducts IP address check using WhoIs, APNIC, ARIN, Domain Tools, etc.
- Agent obtains ISP information; generates subpoena for subscriber information – may take 14 – 30 days for response from provider
- If ISP/record holder information is incorrect, additional research; generate new subpoena
- Agent obtains subscriber information, which may or may not be the same as target information

# Investigative Methodology: IP Address

- Agent conducts investigative activities to determine target, including:
  - Surveillance
  - Checks of additional records
  - U/C activities
  - Addl' traditional investigative techniques
- Delays in obtaining accurate IP information can delay following steps in investigation/enforcement actions

# Domain Name Seizures

The following measures are implemented to make every effort to ensure no legitimate activity is disrupted through the seizure of domain names:

- Identify the full Uniform Resource Locator (URL) hosting the illegal content
- Identify the specific area of the URL where the illegal content or contraband content is hosted; i.e. sub domain (third level domain), sub folder. (It should be noted that the terms URL(s) and website(s) are used interchangeably)
- If the illegal content is hosted on a sub folder( e.g., ***website.com/illegalcontent***) where the illegal content is hosted in the ***illegalcontent*** sub folder off of the URL ***website.com***, the following steps will be taken

# Domain Name Seizures

- Verify the content at URL ***website.com/illegalcontent***, as stated above

- Capture the contents of the website to preserve/evidentiary value

- Identify the listed registrant of ***website.com*** through open source tools available on the Internet (e.g: WhoIs, APNIC, Domain Tools, etc.)

- Identify and verify the content hosted at the URL ***website.com***

- Identify any potential legitimate activity associated with ***website.com***

- If no legitimate activity or other associations can be identified, the domain ***website.com*** may be marked for seizure

# Domain Name Seizures

If the illegal content is hosted on a sub domain (third level domain - e.g., ***illegalcontent.website.com***), the following steps will be taken:

a. Verify the content at URL ***illegalcontent.website.com***

b. Capture the contents of the site to preserve the structure and content of the site at the time of access

c. Identify the listed registrant of ***website.com*** through open source tools available on the Internet

*Generally, it is not possible to identify the registrant of the third level domain through open source tools. The registrant of the second level domain has control over issuing third level domains linked to their second level domain and would have to update the registrant records to reflect any third level domain that was controlled by someone else. **No seizures occur without some form of legal process**.

One World

One Internet

# Questions

# Thank You

No. 44 • 24 - 29 JUNE 2012

ICANN PRAGUE

# Forum on DNS Abuse

*June 25, 2012*

*Moderator:*

*Ondrej Filip, CEO CZ.NIC*

No. 44 • 24 - 29 JUNE 2012

ICANN PRAGUE

One World

One Internet

# Introduction

No. 44 • 24-29 JUNE 2012

ICANN PRAGUE

One World

One Internet

# Martin Peterka
# Operations Manager
# CZ.NIC

# CZ.NIC & security

CZ.NIC z.s.p.o. / http://www.nic.cz

Martin Peterka / martin.peterka@nic.cz
Operations director

25. 6. 2012, ICANN 44 | Prague

cz.
nic | CZ DOMAIN REGISTRY

# Agenda

- About CZ.NIC
- Our security teams
- Solved incidents
- Our proactive tools

# About CZ.NIC

- Special interest association of legal entities
- Founded in 1998 by leading ISPs
- Currently 103 members – growing (open membership)
- 50+ employees
- Core business – domain registry .cz
- MoU with Czech government and NSA
- Part of State's critical infrastructure
- Non profit, Neutrality
- Variety of other activities

cz nic | CZ DOMAIN REGISTRY

# CZ.NIC-CSIRT

- incident handling within AS25192 and incident relating to nameservers for .cz and 0.2.4.e164.arpa
  - no incidents, just our own network
- We are entitled to deactivate a domain if is used in a fashion that endangers the national or international computer security
  - harmful content (especially viruses, malware) are distributed
  - the content of a different service is masqueraded (eg phishing),
  - domain becomes a control centre of interlinked hardware network distributing the harmful content (especially botnet)
- Deactivation for 1 month, even repeatedly

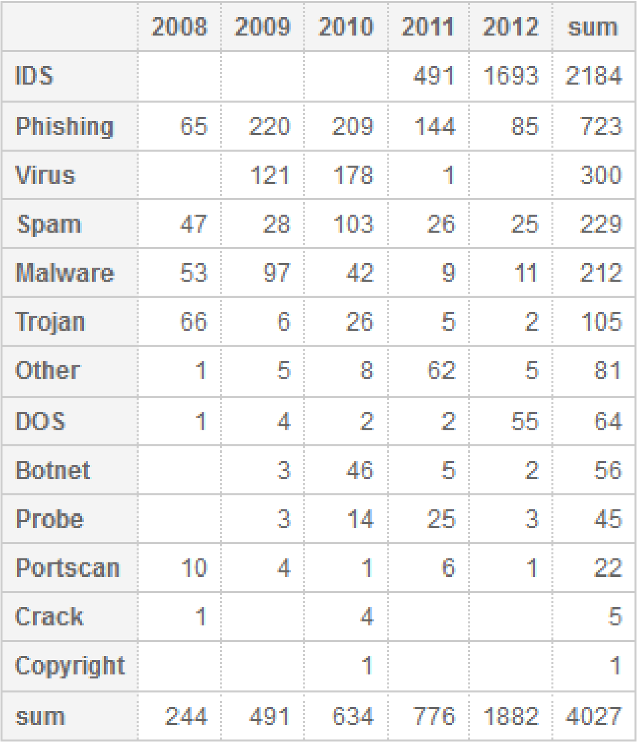
# CSIRT.CZ

CSIRT.CZ
powered by CZ.NIC

- National, last resort CSIRT – no executive power
- Operation since 1 Jan 2011
    - Day-by-day operation and transfer of agenda from CESNET
- Full operation since Jun 2011
- Mainly incident handling/reporting – very successful
- But also a pro-active steps – detection of open unsecured DNS resolvers – cooperation with Security Information Service (BIS)
- Community meetings
- Cooperation – Terena, FIRST, ENISA, team CYMRU
- „accredited“ by TERENA TI (10/2011)

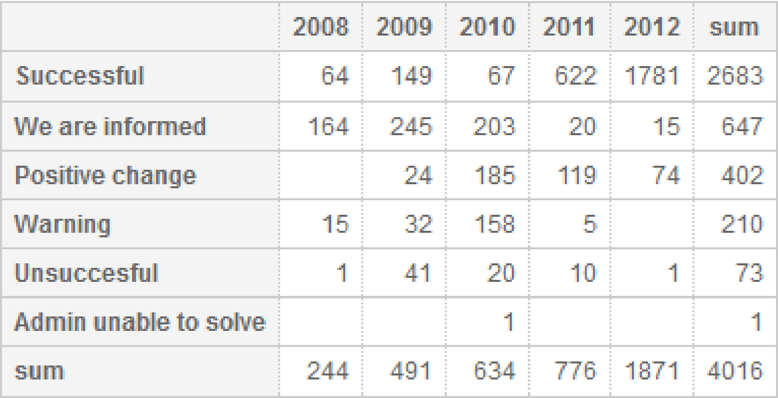
# CSIRT.CZ - statistics

Number of incidents by type (open and closed cases)



| | 2008 | 2009 | 2010 | 2011 | 2012 | sum |
|---|---|---|---|---|---|---|
| IDS | | | | 491 | 1693 | 2184 |
| Phishing | 65 | 220 | 209 | 144 | 85 | 723 |
| Virus | | 121 | 178 | 1 | | 300 |
| Spam | 47 | 28 | 103 | 26 | 25 | 229 |
| Malware | 53 | 97 | 42 | 9 | 11 | 212 |
| Trojan | 66 | 6 | 26 | 5 | 2 | 105 |
| Other | 1 | 5 | 8 | 62 | 5 | 81 |
| DOS | 1 | 4 | 2 | 2 | 55 | 64 |
| Botnet | | 3 | 46 | 5 | 2 | 56 |
| Probe | | 3 | 14 | 25 | 3 | 45 |
| Portscan | 10 | 4 | 1 | 6 | 1 | 22 |
| Crack | 1 | | 4 | | | 5 |
| Copyright | | | 1 | | | 1 |
| sum | 244 | 491 | 634 | 776 | 1882 | 4027 |

Incident resolution states (only closed cases)



| | 2008 | 2009 | 2010 | 2011 | 2012 | sum |
|---|---|---|---|---|---|---|
| Successful | 64 | 149 | 67 | 622 | 1781 | 2683 |
| We are informed | 164 | 245 | 203 | 20 | 15 | 647 |
| Positive change | | 24 | 185 | 119 | 74 | 402 |
| Warning | 15 | 32 | 158 | 5 | | 210 |
| Unsuccesful | 1 | 41 | 20 | 10 | 1 | 73 |
| Admin unable to solve | | | 1 | | | 1 |
| sum | 244 | 491 | 634 | 776 | 1871 | 4016 |

CSIRT.CZ
powered by CZ.NIC

# Incidents

- Examples of 2 incidents
- DNS amplification DDOS (June 2012)
  - Solved by CSIRT.CZ
- Phishing sites (2010)
  - Solved by CZ.NIC-CSIRT

# DNS amplification DDOS

- 2012, solved by CSIRT.CZ
- Attack to the Latvian bank
- Thousands open relay DNS server from all over the world
  - Most of them from USA, 172 from Czech Republic
- Our team solved it at the request of CERT NIC.LV
- Procedure
  - Sort IP’s
  - Find information (companies, admins)
  - Ask for correction
- Cca 50% DNS fixed
- Still in progress

CSIRT.CZ
powered by CZ.NIC

# Phishing attack

- 2010, solved by CZ.NIC-CSIRT
- Target – IRS
- Trojan horse at pages
- During 5 days registered 150 domains
  - Different registrars
  - Different nameservers
  - Fast flux
  - Paid by stolen credit cards
- All domains were deactivated for 1 month
- Immediate response, cooperation with registrars

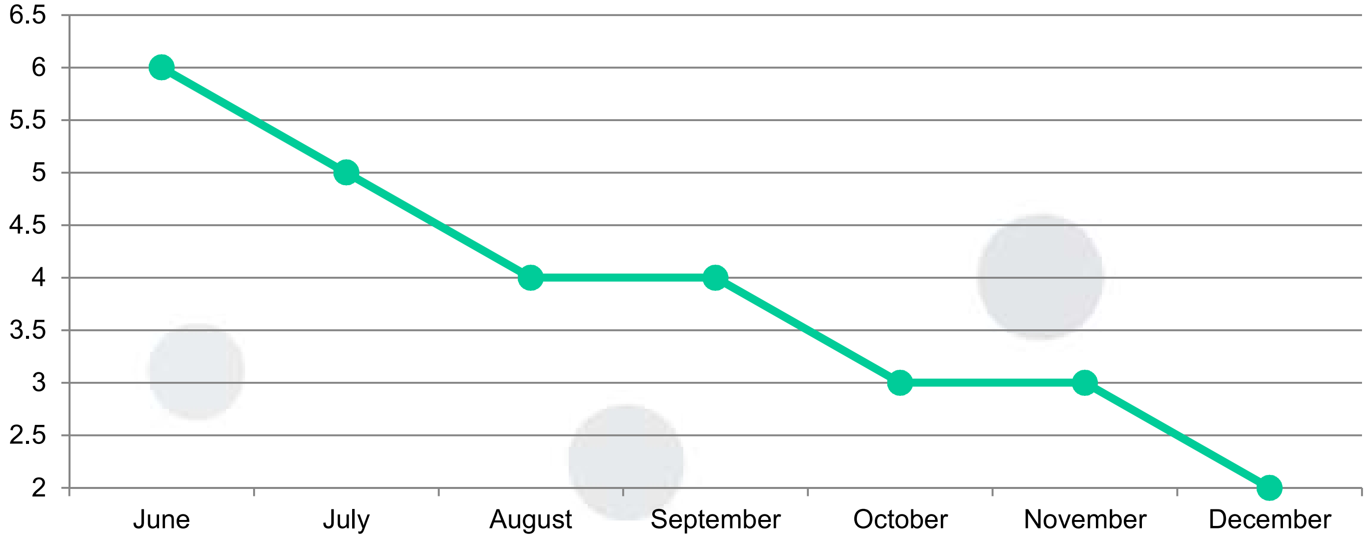
# Lesson learned – we need to be proactive

- Developing of MDM - Malicious Domain Manager
  - In cooperation with CZ.NIC.LABS
- Takes data from public sources
  - Malwarepatrol, Phishtank, Zeus Tracker Abuse.ch, ...
  - Focused on malware, phishing, domains as C&C botnets, etc.
- Selects sites/sources within .cz domain
- Searches for contact information
- Is connected to the ticket system
  - allows controlled communication with the administrators of the sites
- Started in June 2011

# MDM - results

- Since June 2011 cleaned
  - 11 649 pages in
  - 2 299 domains

% of phishing pages within .cz June-Dec 2011
Source : http://www.phishtank.com/



https://git.nic.cz/redmine/projects/mdm

?

# Questions ?

# Thank you!

Martin Peterka / *martin.peterka@nic.cz*
http://www.nic.cz

One World

One Internet

# Branko Stamenković
# Head of the Special Public Prosecutor's Office for High-Tech Crime of Serbia

One World

One Internet

# Christopher Landi and Christopher Malone Cyber Crimes Center U.S. Department of Homeland Security

No. 44 • 24-29 JUNE 2012

ICANN PRAGUE

# Investigative Methodology: IP Address

- Agent obtains suspect IP address
- Agent conducts IP address check using WhoIs, APNIC, ARIN, Domain Tools, etc.
- Agent obtains ISP information; generates subpoena for subscriber information – may take 14 – 30 days for response from provider
- If ISP/record holder information is incorrect, additional research; generate new subpoena
- Agent obtains subscriber information, which may or may not be the same as target information

# Investigative Methodology: IP Address

- Agent conducts investigative activities to determine target, including:
  - Surveillance
  - Checks of additional records
  - U/C activities
  - Addl’ traditional investigative techniques
- Delays in obtaining accurate IP information can delay following steps in investigation/enforcement actions

# Domain Name Seizures

The following measures are implemented to make every effort to ensure no legitimate activity is disrupted through the seizure of domain names:

- Identify the full Uniform Resource Locator (URL) hosting the illegal content
- Identify the specific area of the URL where the illegal content or contraband content is hosted; i.e. sub domain (third level domain), sub folder. (It should be noted that the terms URL(s) and website(s) are used interchangeably)
- If the illegal content is hosted on a sub folder( e.g., ***website.com/illegalcontent***) where the illegal content is hosted in the ***illegalcontent*** sub folder off of the URL ***website.com***, the following steps will be taken

# Domain Name Seizures

- Verify the content at URL ***website.com/illegalcontent***, as stated above

- Capture the contents of the website to preserve/evidentiary value

- Identify the listed registrant of ***website.com*** through open source tools available on the Internet (e.g: WhoIs, APNIC, Domain Tools, etc.)

- Identify and verify the content hosted at the URL ***website.com***

- Identify any potential legitimate activity associated with ***website.com***

- If no legitimate activity or other associations can be identified, the domain ***website.com*** may be marked for seizure

# Domain Name Seizures

If the illegal content is hosted on a sub domain (third level domain - e.g., ***illegalcontent.website.com***), the following steps will be taken:

a. Verify the content at URL ***illegalcontent.website.com***

b. Capture the contents of the site to preserve the structure and content of the site at the time of access

c. Identify the listed registrant of ***website.com*** through open source tools available on the Internet

*Generally, it is not possible to identify the registrant of the third level domain through open source tools. The registrant of the second level domain has control over issuing third level domains linked to their second level domain and would have to update the registrant records to reflect any third level domain that was controlled by someone else. **No seizures occur without some form of legal process**.

One World

One Internet

# Questions

No. 44 • 24-29 JUNE 2012

ICANN PRAGUE

# Thank You

# Forum on DNS Abuse

*June 25, 2012*

*Moderator:*

*Ondrej Filip, CEO CZ.NIC*

No. 44 • 24 - 29 JUNE 2012

ICANN PRAGUE

One World

One Internet

# Introduction

One World

One Internet

## Martin Peterka
## Operations Manager
## CZ.NIC

# CZ.NIC & security

CZ.NIC z.s.p.o. / http://www.nic.cz

Martin Peterka / martin.peterka@nic.cz
Operations director

25. 6. 2012, ICANN 44 | Prague

cz.
nic | CZ DOMAIN REGISTRY

# Agenda

- About CZ.NIC
- Our security teams
- Solved incidents
- Our proactive tools

# About CZ.NIC

- Special interest association of legal entities
- Founded in 1998 by leading ISPs
- Currently 103 members – growing (open membership)
- 50+ employees
- Core business – domain registry .cz
- MoU with Czech government and NSA
- Part of State's critical infrastructure
- Non profit, Neutrality
- Variety of other activities

# CZ.NIC-CSIRT

- incident handling within AS25192 and incident relating to nameservers for .cz and 0.2.4.e164.arpa
  - no incidents, just our own network
- We are entitled to deactivate a domain if is used in a fashion that endangers the national or international computer security
  - harmful content (especially viruses, malware) are distributed
  - the content of a different service is masqueraded (eg phishing),
  - domain becomes a control centre of interlinked hardware network distributing the harmful content (especially botnet)
- Deactivation for 1 month, even repeatedly

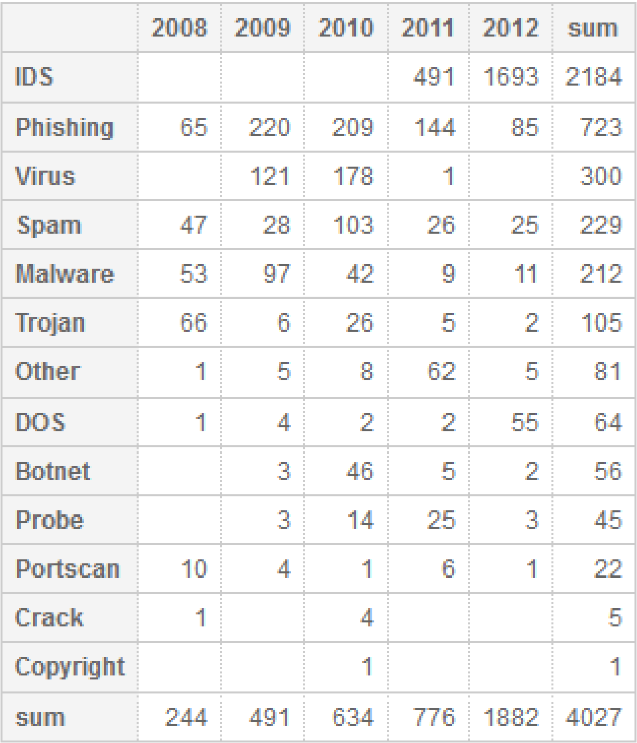
# CSIRT.CZ

CSIRT.CZ
powered by CZ.NIC

- National, last resort CSIRT – no executive power
- Operation since 1 Jan 2011
  - Day-by-day operation and transfer of agenda from CESNET
- Full operation since Jun 2011
- Mainly incident handling/reporting – very successful
- But also a pro-active steps – detection of open unsecured DNS resolvers – cooperation with Security Information Service (BIS)
- Community meetings
- Cooperation – Terena, FIRST, ENISA, team CYMRU
- „accredited“ by TERENA TI (10/2011)

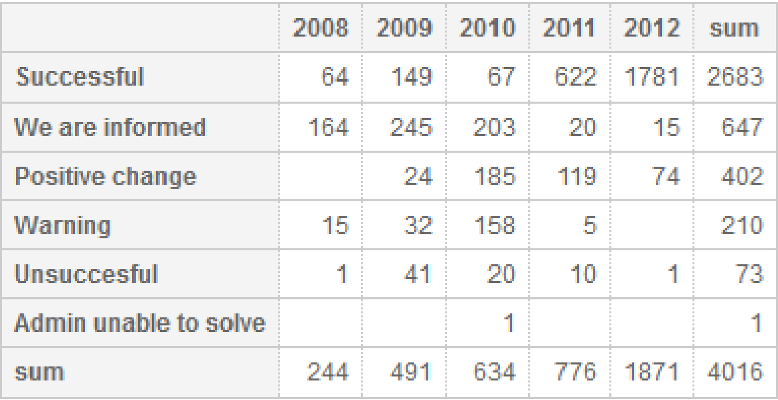
# CSIRT.CZ - statistics

Number of incidents by type (open and closed cases)



| | 2008 | 2009 | 2010 | 2011 | 2012 | sum |
|---|---|---|---|---|---|---|
| IDS | | | | 491 | 1693 | 2184 |
| Phishing | 65 | 220 | 209 | 144 | 85 | 723 |
| Virus | | 121 | 178 | 1 | | 300 |
| Spam | 47 | 28 | 103 | 26 | 25 | 229 |
| Malware | 53 | 97 | 42 | 9 | 11 | 212 |
| Trojan | 66 | 6 | 26 | 5 | 2 | 105 |
| Other | 1 | 5 | 8 | 62 | 5 | 81 |
| DOS | 1 | 4 | 2 | 2 | 55 | 64 |
| Botnet | | 3 | 46 | 5 | 2 | 56 |
| Probe | | 3 | 14 | 25 | 3 | 45 |
| Portscan | 10 | 4 | 1 | 6 | 1 | 22 |
| Crack | 1 | | 4 | | | 5 |
| Copyright | | | 1 | | | 1 |
| sum | 244 | 491 | 634 | 776 | 1882 | 4027 |

Incident resolution states (only closed cases)



| | 2008 | 2009 | 2010 | 2011 | 2012 | sum |
|---|---|---|---|---|---|---|
| Successful | 64 | 149 | 67 | 622 | 1781 | 2683 |
| We are informed | 164 | 245 | 203 | 20 | 15 | 647 |
| Positive change | | 24 | 185 | 119 | 74 | 402 |
| Warning | 15 | 32 | 158 | 5 | | 210 |
| Unsuccesful | 1 | 41 | 20 | 10 | 1 | 73 |
| Admin unable to solve | | | 1 | | | 1 |
| sum | 244 | 491 | 634 | 776 | 1871 | 4016 |

CSIRT.CZ
powered by CZ.NIC

# Incidents

- Examples of 2 incidents
- DNS amplification DDOS (June 2012)
  - Solved by CSIRT.CZ
- Phishing sites (2010)
  - Solved by CZ.NIC-CSIRT

# DNS amplification DDOS

- 2012, solved by CSIRT.CZ
- Attack to the Latvian bank
- Thousands open relay DNS server from all over the world
  - Most of them from USA, 172 from Czech Republic
- Our team solved it at the request of CERT NIC.LV
- Procedure
  - Sort IP’s
  - Find information (companies, admins)
  - Ask for correction
- Cca 50% DNS fixed
- Still in progress

CSIRT.CZ
powered by CZ.NIC

# Phishing attack

- 2010, solved by CZ.NIC-CSIRT
- Target – IRS
- Trojan horse at pages
- During 5 days registered 150 domains
  - Different registrars
  - Different nameservers
  - Fast flux
  - Paid by stolen credit cards
- All domains were deactivated for 1 month
- Immediate response, cooperation with registrars

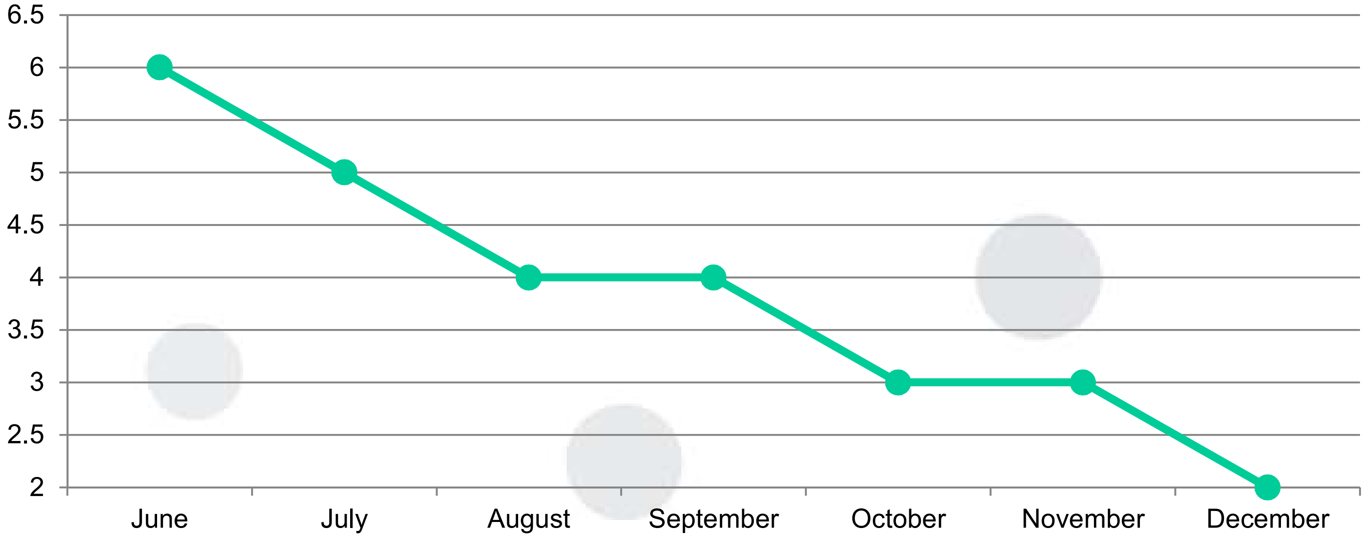
# Lesson learned – we need to be proactive

- Developing of MDM - Malicious Domain Manager
  - In cooperation with CZ.NIC.LABS
- Takes data from public sources
  - Malwarepatrol, Phishtank, Zeus Tracker Abuse.ch, ...
  - Focused on malware, phishing, domains as C&C botnets, etc.
- Selects sites/sources within .cz domain
- Searches for contact information
- Is connected to the ticket system
  - allows controlled communication with the administrators of the sites
- Started in June 2011

# MDM - results

- Since June 2011 cleaned
  - 11 649 pages in
  - 2 299 domains

**% of phishing pages within .cz June-Dec 2011**
**Source : http://www.phishtank.com/**



**https://git.nic.cz/redmine/projects/mdm**

?

## Questions ?

## Thank you!

Martin Peterka / *martin.peterka@nic.cz*
http://www.nic.cz

One World

One Internet

# Branko Stamenković
# Head of the Special Public Prosecutor’s Office for High-Tech Crime of Serbia

One World

One Internet

# Christopher Landi and Christopher Malone
# Cyber Crimes Center
# U.S. Department of Homeland Security

No. 44 • 24-29 JUNE 2012

ICANN PRAGUE

# Investigative Methodology: IP Address

- Agent obtains suspect IP address
- Agent conducts IP address check using WhoIs, APNIC, ARIN, Domain Tools, etc.
- Agent obtains ISP information; generates subpoena for subscriber information – may take 14 – 30 days for response from provider
- If ISP/record holder information is incorrect, additional research; generate new subpoena
- Agent obtains subscriber information, which may or may not be the same as target information

# Investigative Methodology: IP Address

- Agent conducts investigative activities to determine target, including:
  - Surveillance
  - Checks of additional records
  - U/C activities
  - Addl’ traditional investigative techniques
- Delays in obtaining accurate IP information can delay following steps in investigation/enforcement actions

# Domain Name Seizures

The following measures are implemented to make every effort to ensure no legitimate activity is disrupted through the seizure of domain names:

- Identify the full Uniform Resource Locator (URL) hosting the illegal content
- Identify the specific area of the URL where the illegal content or contraband content is hosted; i.e. sub domain (third level domain), sub folder. (It should be noted that the terms URL(s) and website(s) are used interchangeably)
- If the illegal content is hosted on a sub folder( e.g., ***website.com/illegalcontent***) where the illegal content is hosted in the ***illegalcontent*** sub folder off of the URL ***website.com***, the following steps will be taken

# Domain Name Seizures

- Verify the content at URL ***website.com/illegalcontent***, as stated above

- Capture the contents of the website to preserve/evidentiary value

- Identify the listed registrant of ***website.com*** through open source tools available on the Internet (e.g: WhoIs, APNIC, Domain Tools, etc.)

- Identify and verify the content hosted at the URL ***website.com***

- Identify any potential legitimate activity associated with ***website.com***

- If no legitimate activity or other associations can be identified, the domain ***website.com*** may be marked for seizure

# Domain Name Seizures

If the illegal content is hosted on a sub domain (third level domain - e.g., ***illegalcontent.website.com***), the following steps will be taken:

a. Verify the content at URL ***illegalcontent.website.com***

b. Capture the contents of the site to preserve the structure and content of the site at the time of access

c. Identify the listed registrant of ***website.com*** through open source tools available on the Internet

*Generally, it is not possible to identify the registrant of the third level domain through open source tools.  The registrant of the second level domain has control over issuing third level domains linked to their second level domain and would have to update the registrant records to reflect any third level domain that was controlled by someone else.  **No seizures occur without some form of legal process**.

One World

One Internet

# Questions

# Thank You