# Cyber Crime Remediation

Tuesday, 22 May 2012

Internet Systems Consortium

# About the Presenter


Merike Kaeo

Director, Data Security and Services

Internet Systems Consortium

merike@isc.org

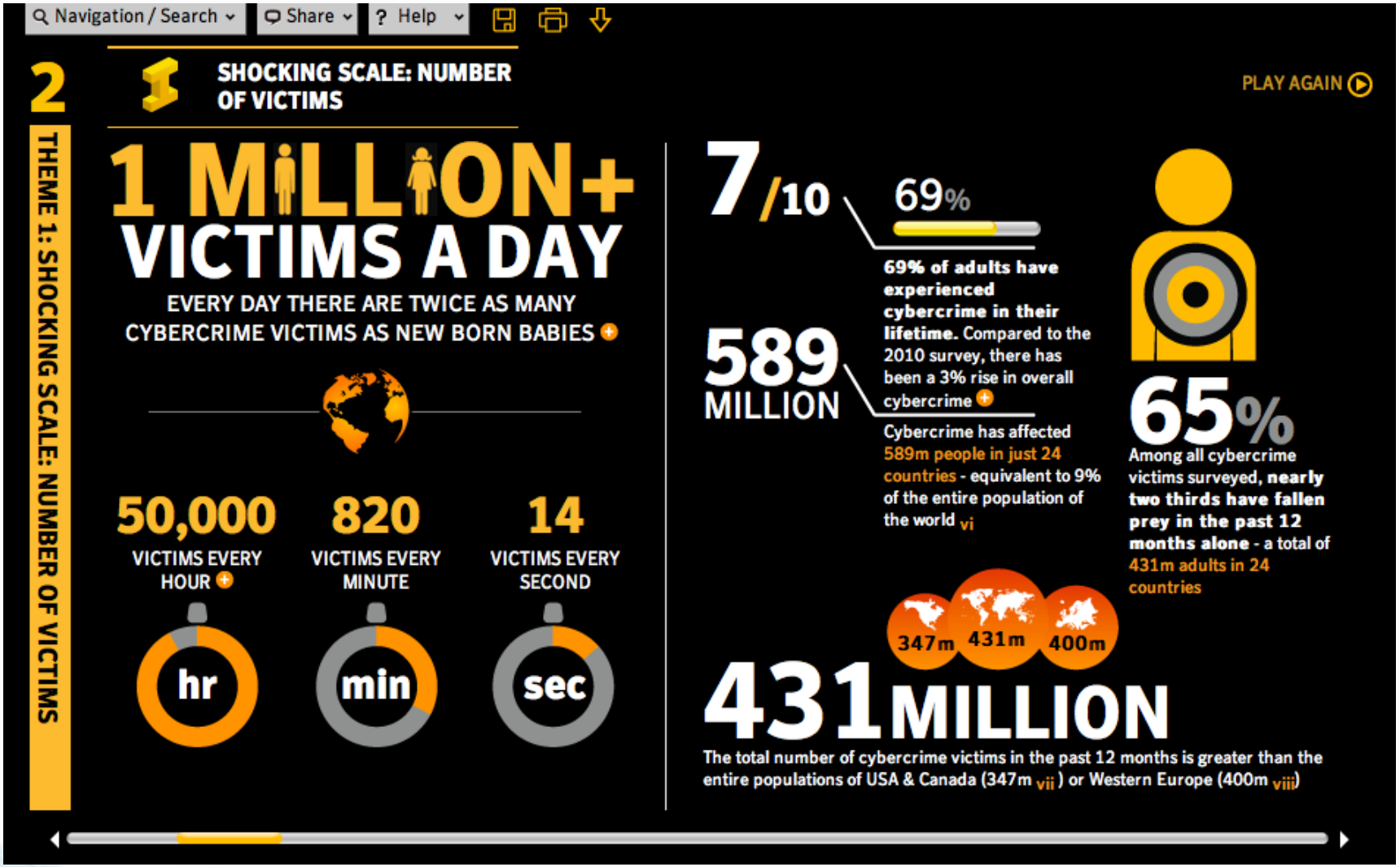
# Agenda

- Malware Remediation Considerations
- DNS Changer Case Study
  - Background Information
  - Current International Remediation Efforts
- Tools and Guidelines for Remediation
  - Exchanging Security Related Information in a Trusted Environment
  - Standards / Codes of Conduct
- Upcoming ISC Events & Trainings
- Q&A Session

# Malware Remediation – Issues

- Who owns the problem?
  - ISP or customer?
  - Which organization within an ISP?
- Who bears the costs?
- What happens if nothing is done?
- Where does regulation fit in?

# Current Realities




( http://www.norton.com/cybercrimereport )

# Whose Move Is It?

Team effort involving entire eco-system of operating system vendors, application providers, on-line content, anti-virus vendors, service providers, professional computer repair organizations, and the ***user of the device.***

# Determining Who Is Affected

- Helpdesk calls
- Service provider telemetry
- Partnerships with Anti-Virus vendors
- Reports from external parties
  - Arbor (http://atlas.arbor.net/)
  - ISC (https://sie.isc.org/)
  - Microsoft (https://postmaster.live.com/snds/)
  - SANS Institute (http://www.dshield.org/about.html)
  - ShadowServer (http://www.shadowserver.org/)
  - Spamhaus (http://www.spamhaus.org/pbl/)
  - Team Cymru (http://www.team-cymru.org/)

# Notification

- Communicating with customers is core to modern customer experience
- Customer persistence and stickiness is important to reducing churn
- Any rational SP strategy to reduce churn will have customer communications tools that include:
  - Email
  - Phone
  - Walled Garden
  - IM
  - Web Alert
  - Home Page Alert
  - SMS
  - TV Screen Alerts

# Notification Considerations

- What mechanism do you use to alert customer of malware susceptibility?
  - Want to get their attention in a timely manner
  - Ensure it comes across as valid
- What information should be included?
  - Details of suspected malware
  - Actionable information such as security checks and remediation tools
  - Contacts for further information
- Track notification vs remediation results

# Questions

# Remediation Case Study

- The "DNS Changer" (aka ‘Ghost Click’) crew that has been hijacking DNS configurations were arrested, infrastructure seized, and a major data center shutdown.
- Law Enforcement Details:
  - http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911


# What does DNS Changer Do?

- Installs malware on PCs and MACs, changes the DNS, and tries to reconfigure the home gateway's DNS.
- Points the DNS configurations to DNS resolvers in specific address blocks and use it for their criminal enterprise.

# Home Routers

- Initial analysis show the following router types might be violated:
  - UTSTARCOM routers from BNSL (India)
  - D-Link
  - Linksys
  - OpenWRT/DD-WRT
  - A-Link
  - Netgear
  - ASUS ZVMODELVZ Web Manager
  - SMC
- No evidence of "changing code," only config
- No evidence of changing the existing password.

# Netblocks Involved

- IP Address Blocks:
  - 85.255.112.0/20
    - (85.255.112.0 through 85.255.127.255 /20)
  - 67.210.0.0/20
    - (67.210.0.0 through 67.210.15.255)
  - 93.188.160.0/21
    - (93.188.160.0 through 93.188.167.255)
  - 77.67.83.0/24
    - (77.67.83.0 through 77.67.83.255)
  - 213.109.64.0/20
    - (213.109.64.0 through 213.109.79.255)
  - 64.28.176.0/20
    - (64.28.176.0 through 64.28.191.255)

# Initial Takedown Remediation

- Trusted DNS resolvers under the control of the investigative team have replaced the criminal's DNS resolvers.
  - All users who might be infected are now going to trusted DNS resolvers.
  - Users might still be infected, but at least they are not going to rogue DNS server or having their DNS service stopped.
  - This "DNS resolver replacement" was done to prevent customer DNS from breaking and having a surge of help desk calls.
- All involved netblocks are advertised as /24s to minimize risk of hijacking by the bad guys.

# Remediation Information

- Logs from the trusted DNS resolvers with the SRC/DST IP addresses, ports, and time stamps are being fed to remediation groups
  - http://www.dcwg.org/cleanup.html
  - ISPs should work with these groups to get feeds to see who in their ASes are infected and help remediate.
- Main site for remediation information is at **http://dcwg.org**
  - Updated news
  - Cleanup details
  - Ongoing efforts

# Are You Infected?

- Global 'are you infected' websites to help in local languages can be found here:
  - http://www.dcwg.org/detect/
- Clearing up some misinformation
  - No software is downloaded
  - No changes are performed on your computer
  - No scanning is done on your computer

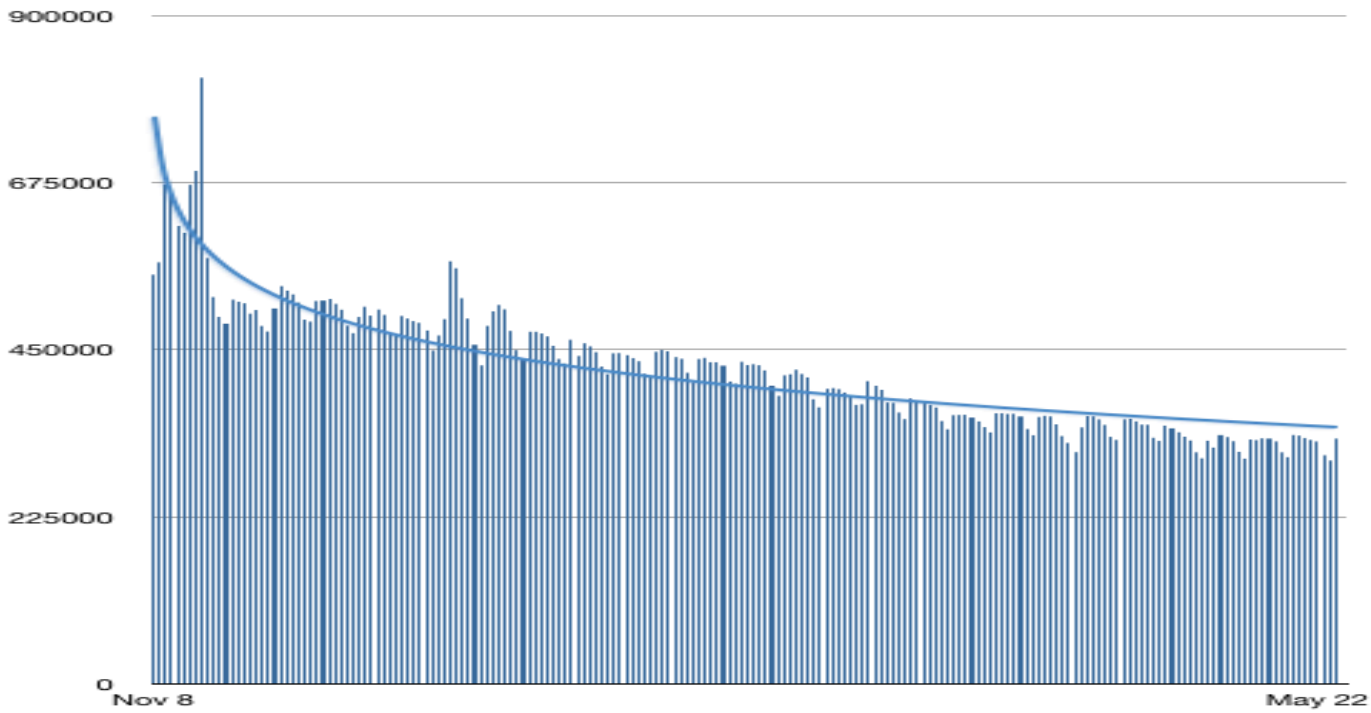
# Tools to Clean Up Infections

- Analysis of the infected computers show that they have multiple infections with boot sector infections.
  - The infections varied over the past five years ranging from the “codex” infections (Zlob) to today’s Alureon.
- Unfortunately, this is not an easy "just use this tool to clean it up."
- The anti-malware community is working on tools.
- http://www.dcwg.org/fix/

# Remediation So Far

- Lukewarm at best
- DoJ notification mistakes are a lesson learned for ENTIRE industry
  - Who you notify and how is not easy when potentially millions of global users involved
- Some global ISP are leaders in helping their customers and overall community
  - dealing with many of cross functional groups and senior management who had to reach agreement
- Lots of FUD but reality is you make mistake, learn, improve, move forward…

# Statistics for .de



# If You Do NOT Help with Remediation

- When the trusted DNS Servers are no longer available
  - The infection remains, and alurion is capable of downloading other plugins beyond just DNS-Changer.
  - Anyone who redirects routes from the involved IP blocks at a regional (non-monitored) level will have a ready supply of DNS victims, and such attacks may not be on ad sales alone. (bank or social or online services URL jacking.)
  - If this address space is later reassigned then the new operator of this space is going to see far more "internet background radiation" than is normal -- so this is a toxic waste dump.

# Positive ISP Lessons Learned

- Some ISPs have gone through learning curve and next time the processes are in place
  - Do you have a process in place?
- Why haven't folks been doing this before?
  - No one to force issue
- Recent trends are to participate in self-regulation efforts
- Senior management type people who need to approve remediation resources are more cognizant of criticality for business
  - Reputation
  - Avoiding down time and user calls

# Still To Figure Out

- What happens after the court order extension for ISC to run the trusted DNS servers?
  - The initial court order had the trusted DNS servers enabled until March 8, 2012
  - This has now been extended to July 9, 2012 to give the industry more time for effective global remediation.
- What happens to non remediated devices after this?
- What are YOUR next steps?

# Questions

# Remediation – Public Private Partnerships

- DNS Changer, like many other large scale malware, is serious, international, and impacts a wide range of the industry.
- No one organization – be it public or private – has the capacity or capabilities to reach out and notify all the infected parties.
- What is needed is a joint Public and Private effort to use existing technology to notify infected parties in real time.

# What Works Now?

- A significant portion of the private industry exchange real time security data from botnets and malware via "bi-lateral" and "multi-lateral" means.
  - Bi-lateral is tedious and runs into scaling issue.
  - Multi-lateral is the industry theme – using tools like the Security Information Exchange (SIE) to fairly distribute information to multiple parties.
- Each party who receives information uses it to notify their customers, alert other organizations, or to adjust their tools to help protect the industry.

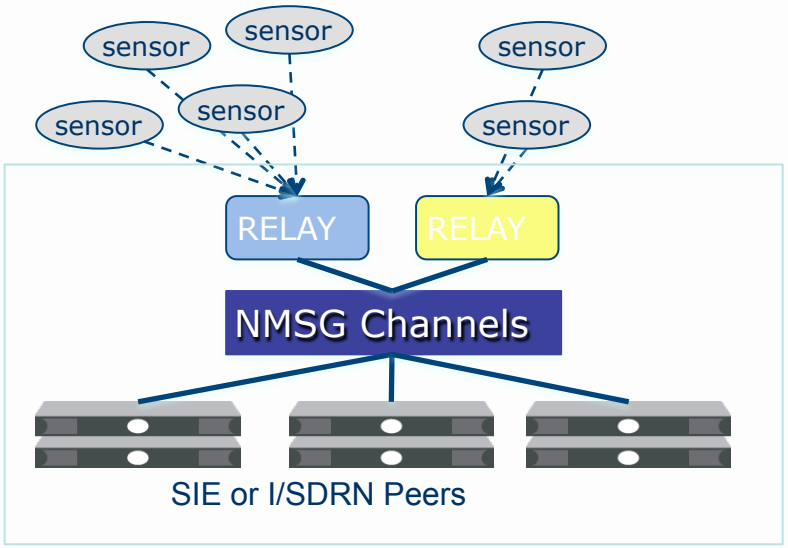
# Security Information Exchange

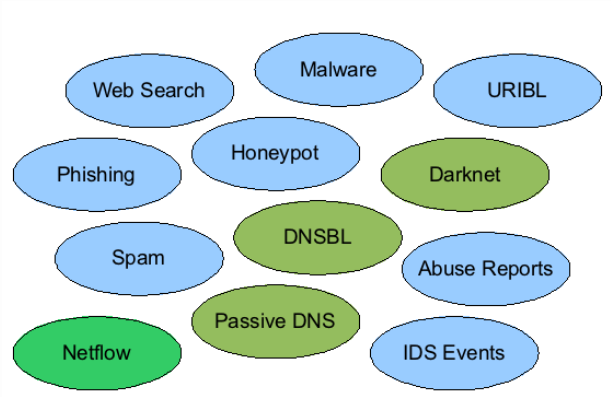
## Building on the Experience of Peering

- ISPs, SPs, and Financial Institutions have been "peering" critical on confidential data for decades.
  - Internet traffic (PAIX, Equinix, LINX)
  - Equity/futures (NY/London SE, NASDAQ)
  - Telco/Meet Me Room (Telehouse, CRG West)
- SIE is building on the SP's experience – by people who have run SPs and other large networks – using that technological and business experience to *short cut perceived obstacles* to security data peering which will *uncover the tangible obstacles*.

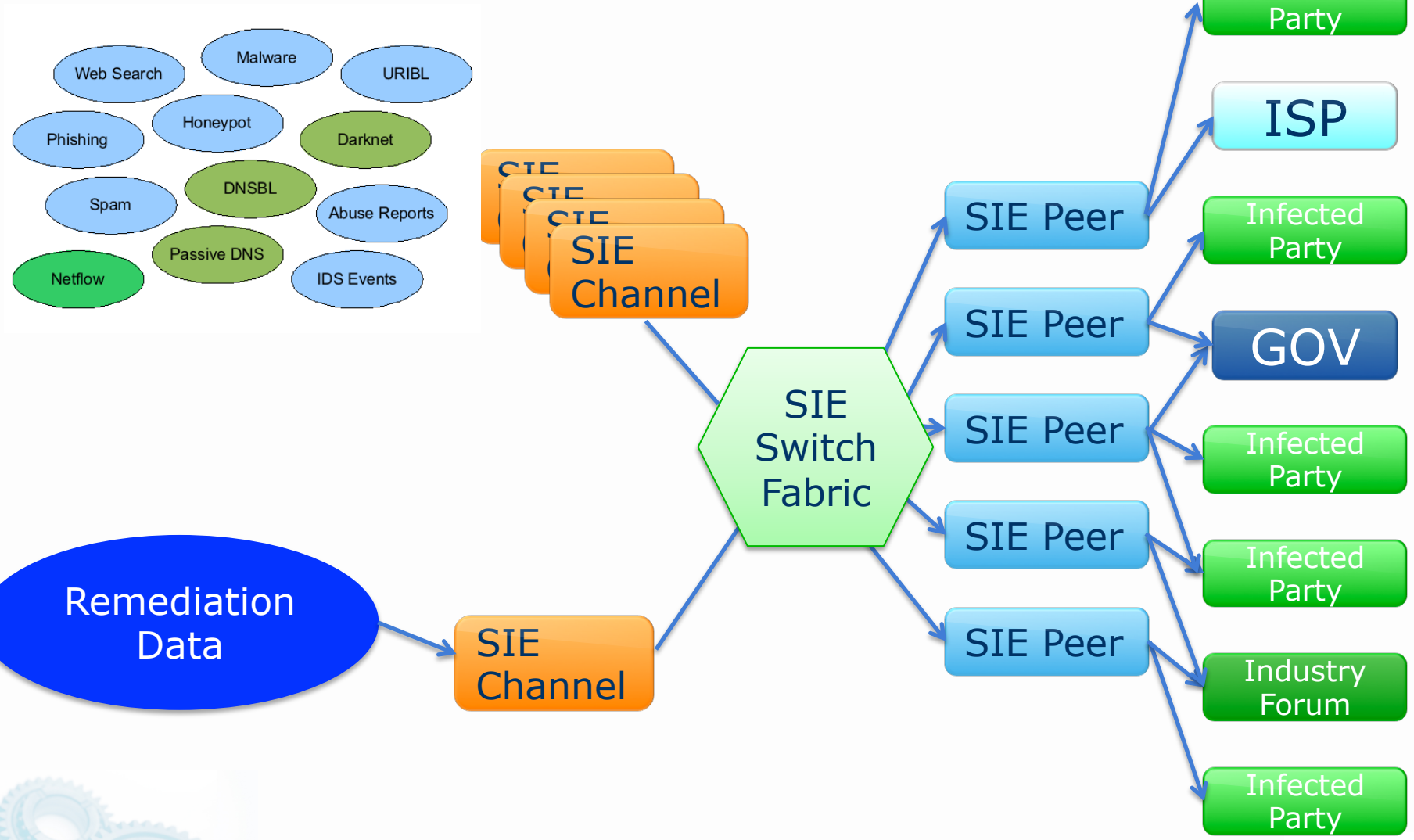
# SIE "Channels"

- SIE used "channels" as the term for peers who are connected to a "port" to subscribe to a data flow.
- There are several types of channels – which are all variants of "private channels":
  - **Community Channels** – multilateral peering, open to any who connect to a port (ISC channels will be converted to Multilateral Community Channels).
  - **Private Channels** – bi-lateral, multi-lateral, and commercial exchange between the SIE constituents.
  - **Incident Channels** – created to provide data during an incident – carries specific distribution rules.



# An Incident SIE Channel



# Who Would Get The Data?

- Access to remediation data from an incident channel depends on who takes ownership of the incident remediation effort
  - Can be organization made up of industry collaborative efforts
  - Can be specific vendor
- Care needs to be taken to not give organizations information that could be misused
  - Infected users for competitive ISPs can be misused by unethical marketing campaigns

# Remediation Guidelines

- Recommendations for the Remediation of Bots in ISP Networks (RFC6561)
  - http://tools.ietf.org/html/rfc6561
- Australia's Code of Conduct
  - http://iia.net.au/images/resources/pdf/iiacybersecuritycode_implementation_dec2010.pdf
- US FCC - CSRIC Working Group 7 (Botnet Remediation Report)
  - http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf

# Questions

# Events and Trainings

www.isc.org/webinars

- Cyber Crime Remediation
  - 22 May 2012
- IPv6 Lessons Learned
  - 12 June 2012

www.isc.org/support/training

- 3-Day IPv6 Fundamentals
  - 4-6 June 2012, Amsterdam
- 2-Day DHCP Workshop
  - 7-8 June 2012, Amsterdam
- 2-Day Intro DNS & BIND
  - 18-19 June 2012, Virginia
- 5-Day Adv DNS & BIND
  - 18-22 June 2012, Virginia
- 2-Day Intro DNS & BIND
  - 2-3 July 2012, Amsterdam
- 5-Day Adv DNS & BIND
  - 2-6 July 2012, Amsterdam

# ISC Resources

- SIE Email Address:
  sie@isc.org

- ISC Knowledge Base:
  **https://deepthought.isc.org**

# Special Offer

Special for today's webinar participants:

***18% discount on any training sessions until 30 September 2012***

Look out for the coupon code in our follow up email after this webinar.

Training information at:

**http://www.isc.org/support/training**

# Questions

# Keeping In Touch

http://www.facebook.com/InternetSystemsConsortium

http://www.linkedin.com/company/internet-systems-consortium

http://twitter.com/ISCdotORG