

2012 is Cyber Security's Turning Point

Barry Greene bgreene@isc.org

Version 1.0

Tuesday, January 10, 2012



Takeaways

- Aggressive Private Industry to Private Industry Collaboration is critical before any successful “public – private partnership”.
- There **are effective Private Industry “Operational Security” Communities** that specialize and succeed.
- Effective Incident Response, Cyber-Risk Management, and Investigations requires active participation and collaboration in these “Operational Security Communities.”
- These communities have rules, expectations, “trust networks,” and paranoia that makes it hard to find and hard to gain access. The investment in Trust does turn into results.

Example of Specializations

- Situational Consultation (Map the Crime Vector): **OPSEC Trust's Main Team**
- Situational Awareness: BTFC, Anti-S, SCADASEC (and others)
- Dissecting Malware: **YASMIL, II** (perhaps MWP)
- Big Back Bone Security and IP Based Remediation: **NSP-SEC**
- Domain Name Takedown: **NX-Domain**
- DNS System Security: **DNS-OARC**
- Anti SPAM, Phishing, and Crime: **MAAWG & APWG**
- Vulnerability Management: **FIRST**
- Many other Confidential Groups specializing into specific areas, issues, incidents, and vulnerabilities.
- Investigative Portals providing focused, confidential investigation: **OPSEC Trust Investigative Teams**



2012 - Optimistically

- Every January we have many throughout the industry predicting cyber-doom and cyber-pessimism.
- 2012 is a year where we're going to see a dramatic change.
- Conficker, McColo, Coreflood, Zeus, Gozi, Waledec, Rustoc, DNS Changer, and many other operations have taught us what is needed to effectively collaborate to succeed.
- We can not turn these lessons into a **Cyber Security Strategy of Action**.



Cyber Strategy of Action

- **Private-to-Private Collaboration with Public participation.** Public policy around the world needs to facilitate the flexibility of private industry to collaboration with each other and with global public partners – moving beyond National constraints.
- **Public – Private Partnership activities need to optimize around private industry flexibility, clarity, and action.** Models like NCFTA are successful because of the interface with aggressive Private-to-Private Collaboration Communities. **We know this works through our results.**



Cyber Strategy of Action

- **Existing Technology for Detecting, Tracking, and Identifying malicious activity is at a level to allow for broad adoption – resulting in new levels of cyber-criminal visibility.** This technology has been validated in enough small and large commercial networks to have a good grasp on the operational cost and impact.
- **Existing Technologies for Remediation have proven to work.** Industry who have deployed remediation are prepared to share the business model impact to foster a sustainable and persistent remediation effort.



Cyber Strategy of Action

- **Action Now is the key to preparing for Cyber-Security Defense.** It is imperative for industry to prepare for critical cyber security incidents. Action now is the best way to prepare and build new security capability/capacity. DCWG, Conficker, and other malware take downs are golden opportunities to build the remediation tools that might save the business in the future.



Effective Collaboration

[bgreene@senki.org](#) ([logout](#))

Main Ops-Trust Group
([change](#)) Ω

[Home](#)

[List member airports](#)

[Nominate new member](#)

[Vouching control panel](#)

[CIDRs of Interest](#)

[AutSys' of Interest](#)

[Domains of Interest](#)

[View mailing lists](#)

[Download PGP key ring](#)

[Visit the Wiki](#)

(Your WikiName must be set)

[Confluence](#) (Experimental)

[Edit contact info](#)

[Change password](#)

Member Information for: [bgreene@senki.org](#)

Full name: Barry Raveendran Greene

Affiliation: @senki.org

PGP Key: [16BF45F3](#)

Entered: 2008-10-11 03:00:04 UTC

Last Activity: 2010-09-01 10:38:38 UTC

Inactive for: 00:00:00

Status: *active*

Timezone info: US Westcoast

SMS info: +1.408.218.4669

I.M. info:

Phone info: +1 408 218 4669

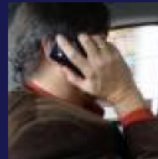
Postal info:

WikiName: BarryRGreene

Home Airport: SFO

Biography: <http://www.linkedin.com/in/barryrgreene>

0x16BF45F3



Has vouched For:

[jose@arbor.net](#)
2010-08-27 21:13:11
[Delete](#)

Know, trust, and work with weekly (sometimes daily)

[ddugal@juniper.net](#)
2010-08-20 16:58:52
[Delete](#)

I've worked with Dave for over two years, with the last year with Dave reporting to me at Juniper. He has been part of Juniper's SIRT Team for a number of year, great incident responder, and insightful investigator.

[derrick.scholl@sun.com](#)
2010-05-24 16:50:04

In 2012, we will have the tools for the good guy to organize and effectively take action (taking lessons from OPSEC Trust's successes)



Cyber Strategy of Action

- **Exercise the Court with Criminal and Civil Action. Laws are driven by cases in the court.** We are consistently working on criminal action, but that is one side of the legal system. Civil action is as important as the criminal action. As seen by Microsoft, damages to a company can be used as a bases for civil action that results in impact against the perceived criminal damage.



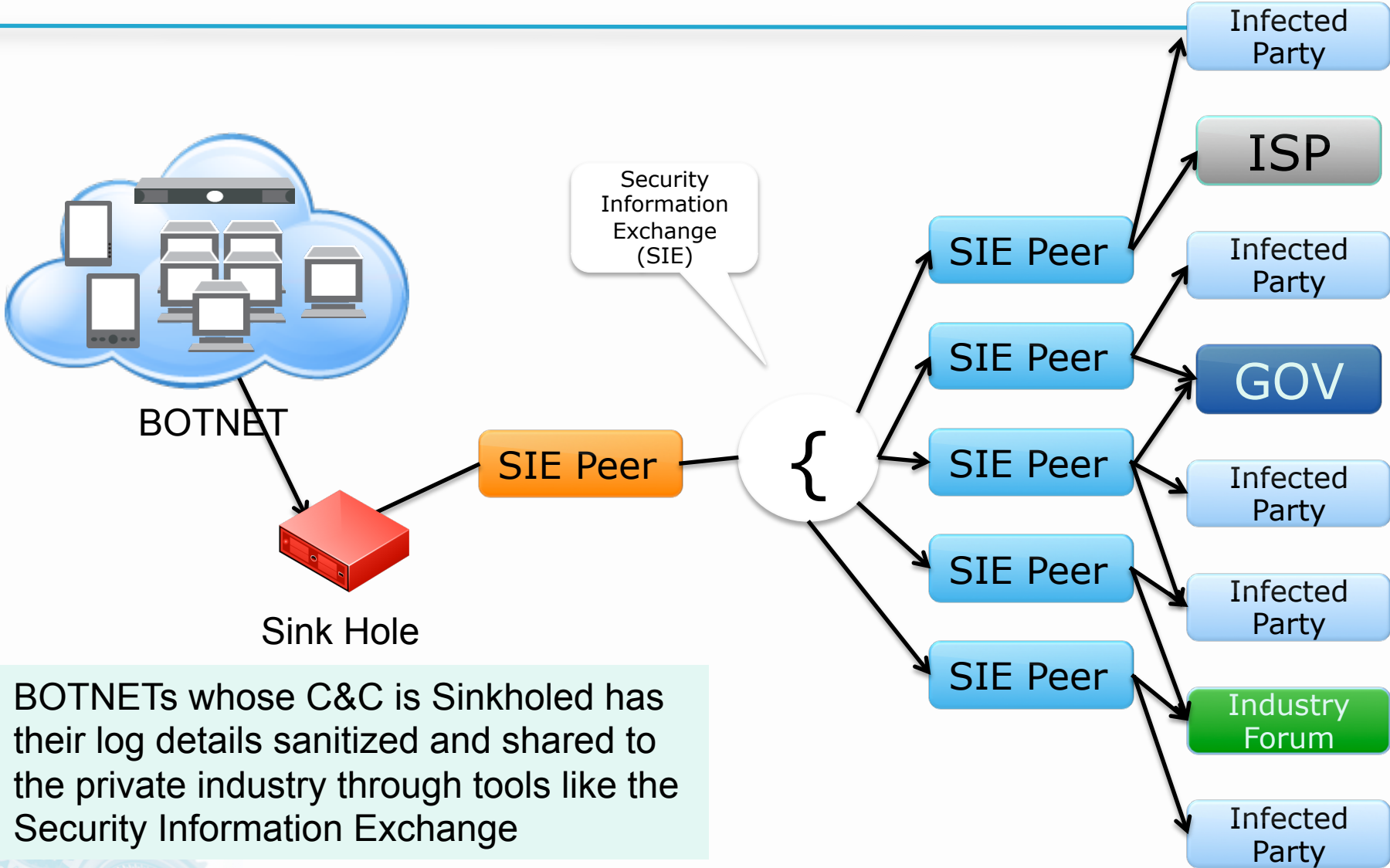
Cyber Strategy of Action

- **Autonomous System (ASN) Sovereignty, Contract Law, and AUPs can be used to embargo peers who are damaging the business.** Each ASN can choose to whom they communicate. While it is a general principle to maintain global connectivity with every ASN in the world, it is by no means a requirement. Problem ASNs have been temporarily “filtered” for the best interest of the Internet. This filtering is done within each ASN.

SRIZBI	36.1%
MEGA-D	20.7%
RUSTOCK	17.6%
PUSHDO	7.1%
BOBAX	5.2%
GRUM	1.5%
WOPLA	1.0%
OTHER SOURCES	10.8%



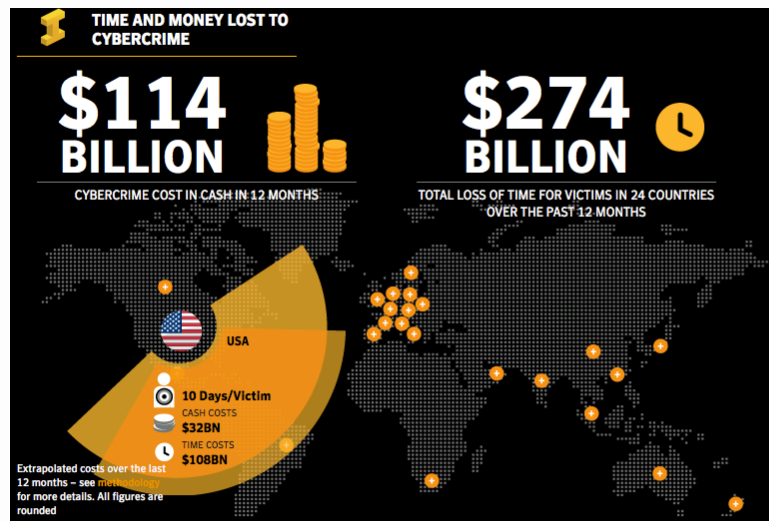
Real Time Security Data Sharing



BOTNETs whose C&C is Sinkholed has their log details sanitized and shared to the private industry through tools like the Security Information Exchange

Cyber Strategy of Action

- **Monetizing Cyber-Security Cost and Risk to the Global Economy will happen in 2012.** Symantec's commissioned study takes expectations to a new level (i.e value of risk can be quantified.) More studies are coming along with the consequence of those studies.



See <http://norton.com/cybercrimereport>.

Take Back the DNS!

Passive DNS – Tool to Find the Badness behind the DNS

bailiwick	oquyclyedi.com.
first seen	2010-11-24 18:09:45 -0000
last seen	2010-11-25 09:52:03 -0000
oquyclyedi.com.	A 213.55.114.132
bailiwick	com.
first seen	2010-11-15 02:47:01 -0000
last seen	2010-11-26 02:07:10 -0000
first seen in zone file	2010-11-15 17:09:22 -0000
last seen in zone file	2010-11-24 17:09:28 -0000
oquyclyedi.com.	NS ns1.gvghi.ru.
oquyclyedi.com.	NS ns2.justecosy.com.
bailiwick	com.
first seen in zone file	2010-11-14 17:09:22 -0000
last seen in zone file	2010-11-14 17:09:22 -0000
oquyclyedi.com.	NS ns3.lerelaisinternet.com.
oquyclyedi.com.	NS ns4.lerelaisinternet.com.
bailiwick	oquyclyedi.com.
first seen	2010-11-16 02:24:21 -0000
last seen	2010-11-25 12:16:08 -0000
oquyclyedi.com.	NS ns1.oquyclyedi.com.
oquyclyedi.com.	NS ns2.oquyclyedi.com.

bailiwick	gvghi.ru.	03:43:04 -0000
first seen	2010-11-18 15:54:49 -0000	13:44:15 -0000
last seen	2010-11-22 03:31:24 -0000	03.66
ns1.gvghi.ru.	A 190.86.101.171	
bailiwick	gvghi.ru.	
first seen	2010-11-11 03:12:45 -0000	
last seen	2010-11-18 15:42:32 -0000	
ns1.gvghi.ru.	A 201.147.145.254	
bailiwick	gvghi.ru.	
first seen	2010-11-23 13:53:07 -0000	
last seen	2010-11-25 11:12:16 -0000	
ns1.gvghi.ru.	A 218.67.78.181	

Rdata results for ANY/213.55.114.132

Found 10000 RRs in 1.65 seconds.

01jwahwdjz.curibeudo.com.	A 213.55.114.132
0ck37mtnfv.hattytysi.com.	A 213.55.114.132
0dnk1o6x6r.drinekage.com.	A 213.55.114.132
0dzt3uw24r.cyrzoekfo.com.	A 213.55.114.132
0gtnu.mas.bayhealthmedicine.ru.	A 213.55.114.132
0hfvvthw23.curibeudo.com.	A 213.55.114.132
0pt7yqdrop.edfasawen.com.	A 213.55.114.132
0q2ufc10tx.curibeudo.com.	A 213.55.114.132
0q1foqmgwa.drinekage.com.	A 213.55.114.132
0tftb1tk5.hattytysi.com.	A 213.55.114.132
0xc1uej10t.synpaybs.com.	A 213.55.114.132
0zu54eln0n.aneznauks.com.	A 213.55.114.132
10004.buvaiklo.com.	A 213.55.114.132
10004.lekpoeha.com.	A 213.55.114.132
10005.nrukixbya.com.	A 213.55.114.132
1000shop.myralfiah.com.	A 213.55.114.132
1001shop.myralfiah.com.	A 213.55.114.132
1003shop.myralfiah.com.	A 213.55.114.132
10061.psyatlin.com.	A 213.55.114.132
10064.adevrecos.com.	A 213.55.114.132
100675.drugeshop.com.	A 213.55.114.132
10089.kieobdole.com.	A 213.55.114.132
1009.muyveqwal.com.	A 213.55.114.132

Rdata results for ANY/218.67.78.181

Found 4700 RRs in 1.12 seconds.

\\s2.tabletpilldrug.net.	A 218.67.78.181
a9y.ru.	A 218.67.78.181
atlanticmedsrx.net.	A 218.67.78.181
enclavedirect.com.	A 218.67.78.181
grandrxpills.com.	A 218.67.78.181
justecosy.com.	A 218.67.78.181
locutionsite.com.	A 218.67.78.181
mail.c3o.ru.	A 218.67.78.181
mail.usualworld.com.	A 218.67.78.181
maternitybuydirect.com.	A 218.67.78.181
medrxpills.net.	A 218.67.78.181
ns1.alternativehealthrx.net.	A 218.67.78.181
ns1.badsguide.com.	A 218.67.78.181
ns1.bafac.ru.	A 218.67.78.181
ns1.bafad.ru.	A 218.67.78.181
ns1.bafaf.ru.	A 218.67.78.181
ns1.bafag.ru.	A 218.67.78.181
ns1.bafaj.ru.	A 218.67.78.181
ns1.bafal.ru.	A 218.67.78.181
ns1.bafap.ru.	A 218.67.78.181
ns1.bafar.ru.	A 218.67.78.181
ns1.bafaw.ru.	A 218.67.78.181

Criminal Domain Names found via the bad A Record

Criminal Domain Names found via the bad Name Server

Summary = Action

- Make 2012 your year of action.
 - **Foster Private-to-Private Collaboration with Public participation.**
 - **Invest in Public – Private Partnership activities like NCFTA**
 - **Action Now is the key to preparing for Cyber-Security Defense**
 - **Reach out and participate in the Operational Security Portals**
 - **Exercise the Court with Criminal and Civil Action.**
 - **Have your service providers each out an empower their *Autonomous System (ASN) Sovereignty.***
 - **Real Time Security Data Sharing**
 - **Monetizing Cyber-Security Cost and Risk to the Global Economy will happen in 2012.**
 - **Take Back the DNS – Get a DNSDB Account**

Start with DNS Changer



[Home](#) [News](#) [Checkup](#) [Cleanup](#) [Victim Rights](#) [For ISPs](#) [About/Contact](#)

What is the DNS Changer Malware?

On November 8, the FBI, the NASA-OIG and Estonian police arrested several cyber criminals in "Operation Ghost Click". The criminals operated under the company name "Rove Digital", and distributed DNS changing viruses, variously known as TDSS, Alureon, TidServ and TDL4 viruses. You can read more about the arrest of the Rove Digital principals [here](#), and in the [FBI Press Release](#).

What does the DNS Changer Malware do?

The botnet operated by Rove Digital altered user DNS settings, pointing victims to malicious DNS in data centers in Estonia, New York, and Chicago. The malicious DNS servers would give fake, malicious answers, altering user searches, and promoting fake and dangerous products. Because every web search starts with DNS, the malware showed users an altered version of the Internet.

How Can I Protect Myself?

This page describes how you can determine if you are infected, and how you can clean infected machines. To check if you're infected, [Click Here](#). If you believe you are infected, [here are instructions](#) on how to clean your computer.

DCWG.ORG

