Slideshow ^ I< << Slide 1 of 23 >> >I

Abuse Situation Awareness (Introduction)



۵

[Amman Cyber Drill/000-AbuseSA][edit]

Slideshow ^ I< << Slide 2 of 23 >> >I

The Problem?



G

[Amman Cyber Drill/001-The Problem][edit]

Slideshow ^ I< << Slide 3 of 23 >> >I

Lari Huttunen



education MA in Linguistics and Computer Science

past University of Helsinki, Finnish Police

present Codenomicon

Real contact@clarifiednetworks.com

[Usual Suspect][edit] [Amman Cyber Drill/010-The Presenter][edit]

Slideshow ^ I< << Slide 4 of 23 >> >I

Sub Topics for Today

- Abuse Feed Ecosystem
- AbuseHelper
- VSRoom, Virtual Situation Room

[Amman Cyber Drill/020-The Presenter][edit]

Slideshow ^ I< << Slide 5 of 23 >> >I

Abuse Feed Ecosystem

Feeders

Organizations, which gather intelligence on malicious activity and identities.

Proxies

CSIRT teams, which collect this information from various sources and report it to the cleaners.

Cleaners

Organisations, whose customers or networks are victims of cyber crime.

[Abuse Feed Ecosystem][edit]

[Amman Cyber Drill/030-Abuse Feed Ecosystem][edit]

Slideshow ^ I< << Slide 6 of 23 >> >I

Feeders

hobbyist

Various projects with varying motivations, such as ZONE-H or Malc0de.

non-profit

Organizations such as ShadowServer, abuse.ch, Dragon Research Group or SpamHaus.

commercial

Feed providers, such as Arbor Networks, SpamHaus Technology or Team Cymru.

[Amman Cyber Drill/035-Feeders][edit]

Slideshow ^ I< << Slide 7 of 23 >> >I

Proxies

government

National CERT teams, such as CERT-FI, CERT-EE, CERT-BE, CERT-IS, CERT-AT or CERT-EU.

academic

Various university network CSIRT teams, such as FUNET CERT in Finland.

industry

ISP or corporate CSIRT teams, which report to their constituency, such as their corporate customers.

[Amman Cyber Drill/042-Feeders][edit]

Slideshow ^ I< << Slide 8 of 23 >> >I

Cleaners

- Various CSIRT teams, whose networks or customers are victims of cybercrime.
- The biggest challenge for them usually is connecting the dots between an ip address and a timestamp in an abuse report and the customer.
- Another challenge is prioritization of abuse reports into different categories.
- AbuseHelper can help in this. 😕

[Amman Cyber Drill/045-Cleaners][edit]

Slideshow ^ I< << Slide 9 of 23 >> >I

And Now teh Mad Tech ;)



۵

[Amman Cyber Drill/047-Teh Technology][edit]

Slideshow ^ I< << Slide 10 of 23 >> >I

Everybody's Different, Nobody's Perfect



[Everybody is Different - Nobody is Perfect][edit]

abuse feeds

vary in format, formalism and transports.

data

varies in integrity, availability and duplication.

time

timespans, update frequencies, time and date formats.

ontology

provided details, schemas, terminology

Slideshow ^ I< << Slide 11 of 23 >> >I

AbuseHelper

abusehelper.lobby.me	Chats	
abusehelper.lobby.me abus	- Jobby me@conference.clarifiednetworks.com	BOOKMARK Participants (4)
/v-descs/virus w32 virut.shtml, cc=IR, "source port"=1067, regis	.243. 159 is a inkely participant of Virut botner, uri= <u>ntp://www.lss</u> ip=84.47.245.159, bgp_prefix=84.47.240.0/21, longitude=53.0, a stry=ripencc, "as name [*] ="MABNA Gostaresh Ertebatat Mabna (N C", latitude=32.0, allocated=2004-10-15, type="botnet drone", ged"	sn=42601, roomgraph IABNA)", bip_cc=IR statsbot
/v-descs/virus w32 virut.shtml, cc=IR, "source port"=1060, regis	8.67.201 is a likely participant of Virut botnet", url= <u>http://www.f-sec</u> ip=2.186.67.201, bgp_prefix=2.184.0.0/13, longitude=46.2919, a stry=ripencc, "as name"="DCI-AS Information Technology Compa C", latitude=38.08, allocated=2010-10-18, type="botnet drone", ge	sn=12880, Invite v any (ITC)",
/v-descs/virus w32 virut.shtml, cc=IL, "source port"=3934, regis	31.40.220 is a likely participant of Virut botnet", url= <u>http://www.f-se</u> ip=79.181.40.220, bgp_prefix=79.181.0.0/18, longitude=34.8417 stry=ripencc, "as name"="BEZEQ-INTERNATIONAL-AS Bezeqint 7:04:10 UTC", latitude=32.1472, allocated=2007-06-14, type="bc	, asn=8551, Internet
<u>/v-descs/virus_w32_virut.shtml</u> , cc=EG, "source port"=1051, reg	I.145.44 is a likely participant of Virut botnet", url= <u>http://www.f-sec</u> ip=41.44.145.44, bgp_prefix=41.44.144.0/20, longitude=30.0, as jisty=afrinic, "as name"="TE-AS TE-AS", time="2012-07-10 17:0- 1-05, type="botnet drone", geoip_cc=EG	n=8452,
/v-descs/virus w32 virut.shtml, cc=IL, "source port"=1678, regis	6.173.40 is a likely participant of Virut botnet", url= <u>http://www.f-sc</u> ip=46.116.173.40, bgp_prefix=46.116.0.0/15, longitude=34.8142, stry=ripencc, "as name"=NV-ASN 013 NetVision Ltd.", time="201 6, allocated=2010-05-12, type="botnet drone", geoip_cc=lL	asn=1680,
<u>/v-descs/virus_w32_virut.shtml</u> , cc=IL, "source port"=3941, regis	35.40.199 is a likely participant of Virut botnet", url= <u>http://www.f-sg</u> ip=109.65.40.199, bgp_prefix=109.65.0.0/18, longitude=34.8367 stry=ripencc, "as name"="BEZEQ-INTERNATIONAL-AS Bezegint 7:06:52 UTC", latitude=32.1658, allocated=2009-08-10, type="bc	, asn=8551, Internet
<u>/v-descs/virus_w32_virut.shtml</u> , asn=12880, cc=IR, "source port"	01.119.81 is a likely participant of Virut botnet", url= <u>http://www.f-se</u> ip=80.191.119.81, bgp_prefix=80.191.96.0/19, longitude=52.538 "=1042, registry=ripencc, "as name"="DCI-AS Information Techn 7-10 17:08:12 UTC", latitude=29.6036, allocated=2002-07-23, typ	8, blogy
/v-descs/virus w32 virut.shtml, cc=IR, "source port"=1938, regis	0.180.43 is a likely participant of Virut botnet", url= <u>http://www.f-sec</u> ip=31.59.180.43, bgp_prefix=31.59.176.0/20, longitude=53.0, as stry=ripencc, "as name"=/RASANA kria Rasana Tadbir", itime="2/ llocated=2011-01-28, type="botnet drone", geoip_cc=IR	n=31549,
<u>■ ◎ - ☆ -</u>		

G

[Amman Cyber Drill/099-AbuseHelper][edit]

Slideshow ^ I< << Slide 12 of 23 >> >I

AbuseHelper - Design Goals

The initial implementation was a collaboration between CERT-EE and Clarified Networks, with the help of CERT-FI.

why

To enable you to systematically deal with abuse in your country.

botnet inspired

AbuseHelper is an XMPP-driven technology, a benign botnet to fight malicious botnets.

streaming architecture

Data is collected from various sources over various transports and fed through a processing pipeline to the final recipient of an actionable abuse report.

[Amman Cyber Drill/100-AbuseHelper][edit]

Slideshow ^ I< << Slide 13 of 23 >> >I

G

AbuseHelper - Bot Classes



[Amman Cyber Drill/110-Bot Classes][edit]

Slideshow ^ I< << Slide 14 of 23 >> >I

G

AbuseHelper - Example Botnet



[Amman Cyber Drill/120-Botnet][edit]

Slideshow ^ I< << Slide 15 of 23 >> >I

VSRoom, Virtual Situation Room



[Amman Cyber Drill/200-VSRoom][edit]

Slideshow ^ I < << Slide 16 of 23 >> >I

VSRoom - Design Goals

- Provide a generic browser-based user interface for visualizing XMPP event driven data.
 - Implemented in Javascript and HTML5.
 - Distinct views, view-specific and global parameters.
 - The user interface is a Javascript bot, which requests data from a historian bot.
- Enable the users to share their findings with their colleagues via VSRoom URLs.
 - Provide actionable visualizations and the ability to drill down to the level of a single abuse event.
- Visualize pre-processed and filtered data in the order of tens of thousands of events instead of millions.

[Amman Cyber Drill/210-VSRoom-Design-Goals][edit]

Slideshow ^ I< << Slide 17 of 23 >> >I

G

VSRoom - Basic Views



[Amman Cyber Drill/220-Teh-Views][edit]

Slideshow ^ I< << Slide 18 of 23 >> >I

VSRoom - Map



G

[Amman Cyber Drill/230-Map][edit]

Slideshow ^ I< << Slide 19 of 23 >> >I

VSRoom - Categorilla



۵

[Amman Cyber Drill/240-Categorilla][edit]

Slideshow ^ I< << Slide 20 of 23 >> >I

VSRoom - List

New view	Last 1 month		geoip_cc=JO	Share
count *	сс	asn	type	
442	JO	8376	botnet drone	
190	JO	48832	botnet drone	
164	JO	8697	botnet drone	
13	JO	42912	botnet drone	
11	JO	35656	botnet drone	
4	JO	9038	botnet drone	
3	JO	8697	ssh brute-force	
3	JO	50670	botnet drone	
3	JO	44466	botnet drone	
2	JO	9038	ssh brute-force	
2	JO	8934	defacement	
1	JO	47887	ssh brute-force	
1	OC	47887	defacement	
Settings	Jordanian Abuse Even	ts	Remo	ve

۵

[Amman Cyber Drill/250-List][edit]

Slideshow ^ I< << Slide 21 of 23 >> >I

On to the Demo, Let's Go



[Amman Cyber Drill/300-Teh Demo][edit]

Slideshow ^ I< << Slide 22 of 23 >> >I

G

Questions?



[Amman Cyber Drill/303-Questions][edit]

Slideshow ^ I< << Slide 23 of 23 >> >I

Thank You!

reminder

CERT-FI was able to amp up their abuse handling capabilities 100x through automation.

[Amman Cyber Drill/999-Cest-Fini][edit]

Title

Abuse Situation Awareness (Introduction)

Author

Lari Huttunen

CategorySlideShow

Amman Cyber Drill (last edited 2012-07-10 05:05:36 by ?svimes)