TLDCON 2017
Almaty, Kazakhstan

The Avalanche takedown

Benedict Addis
Shadowserver Foundation and Registrar of Last Resort

About Benedict

- Former technical officer, UK National Cybercrime Unit
- ICANN security and stability advisory committee (SSAC)
- Shadowserver Foundation volunteer
- Chair of the Registrar of Last Resort (RoLR)

Registrar of Last Resort (RoLR)

RoLR: a special purpose registrar

Quarantine bad domains

- Spam
- Phishing
- Malware distribution
- Botnet command & control
- "Advanced Persistent Threat"

Limited scope

Avalanche

Avalanche: overview

Not a botnet!

Hosting and DNS for criminals, by criminals

~20 malware families

Operating since 2009

Victims in 180 countries

Stolen $100 millions

Avalanche: Геннадий Капканов

Avalanche: malicious domains

EXAMPLE: TINY BANKER
SOURCE: FRAUNHOFER FKIE

. . .
qvehqbeemgfp.com
qvehqbeemgfp.ru
qvehqbeemgfp.su
qwdssurudtpf.biz
qwdssurudtpf.pw
qwdssurudtpf.space
qwdssurudtpf.us
. . .

Avalanche: TLDs

com	155525		xyz	5418		top	8		ua	3	
net	125837		us	2602		kz	7		at	2	
in	59115		uk	2308		mobi	6		au	2	
biz	51172		space	2105		tk	6		website	2	
cn	50206		pk	400		cx	5		am	1	
cc	48588		bid	204		aaa	4		br	1	
ru	44531		club	202		pl	4		desi	1	
pw	38684		eu	137		asia	3		host	1	
me	30430		it	107		bike	3		ml	1	
su	29286		ca	101		nl	3		press	1	
tw	28015		co	101		online	3		py	1	
sg	18300		tech	101		site	3		win	1	
ws	18300		click	100							
org	13447		rent	100							
info	10697										

Avalanche: domain statistics

830,000 possible domains spanning:
64 TLDs, split equally between ccTLD and gTLD
40 registries
located in 30+ countries

The press said "830,000 domains"
BUT only 4,000 domains registered at time of takedown

In .RU: only 82 domains registered out of ~40,000
In .SU: only 22 domains registered out of ~30,000
In .KZ: just seven domains in total

Remediation

Or, why do we want all these bad domains?

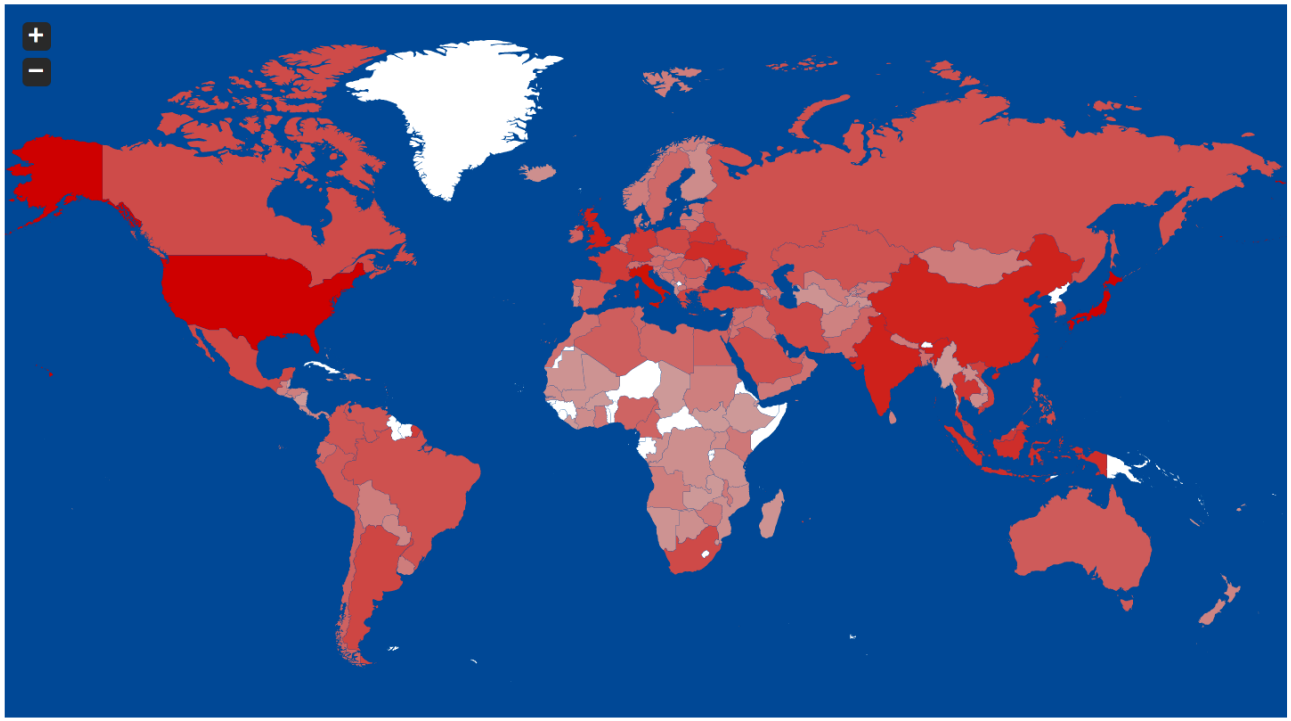
1) Registries point nameservers at the official sinkhole

2) Victim computers connect to sinkhole and are ID'd

3) Data shared free with CERTs, registries and network owners

4) Victims are notified of malware infections

Remediation

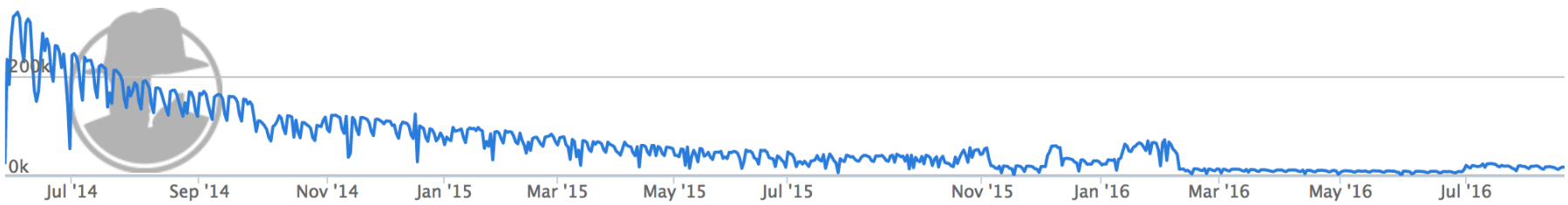


Unique Gameover Zeus IPs Per Day

Unique Infected IPs

Zoom 1m 3m 6m YTD 1y All

From May 30, 2014 To Aug 17, 2016



What can you do?

Request reports:
https://www.shadowserver.org/wiki/pmwiki.php/Involve/GetReportsOnYourNetwork

or…

Search Google for
"Shadowserver get reports"

Questions?

Benedict Addis
bee@rolr.eu