RSA CONFERENCE 2013

TAKING DOWN THE WORLD'S LARGEST BOTNETS

Ali Mesdaq
FireEye, Inc.

Security in knowledge

Session ID: CLE-W03

Session Classification: Advanced

Credit

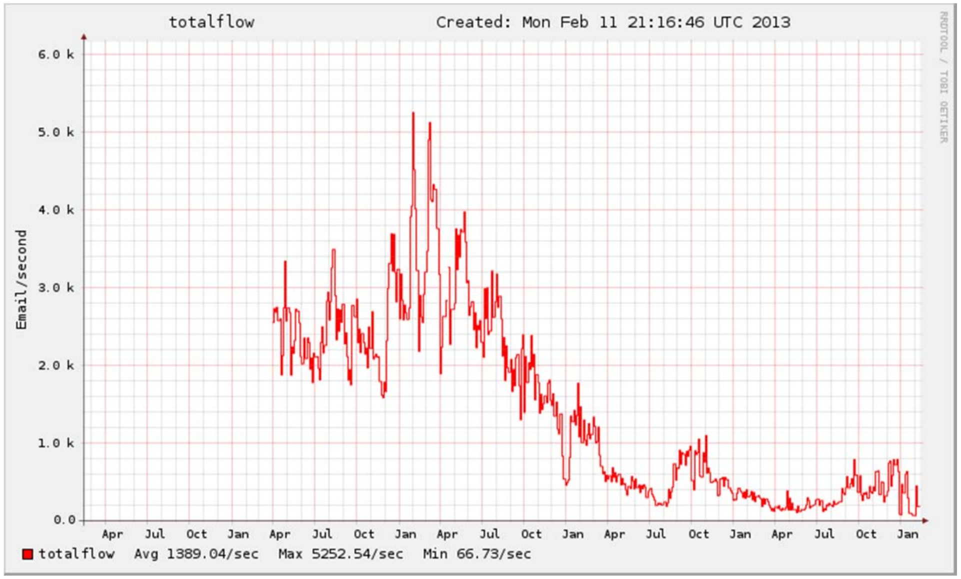
- Atif Mushtaq > Ali Mesdaq
- Real FireEye veteran
- Specialized in Botnets and CnC communication
- Extensive and detail blogs
- Forgive me for mistakes
- If your botnet was taken down it was him not me!

DREAMING OF A JUNK-FREE MAILBOX

Most of you might be surprised to know that global spam levels have dropped more than 92% during last 4 years or so. Thanks to the research community's efforts against spammers. But we need to maintain this pressure until we reach a point where the bad guys start thinking that becoming a spammer is not worth the risk.

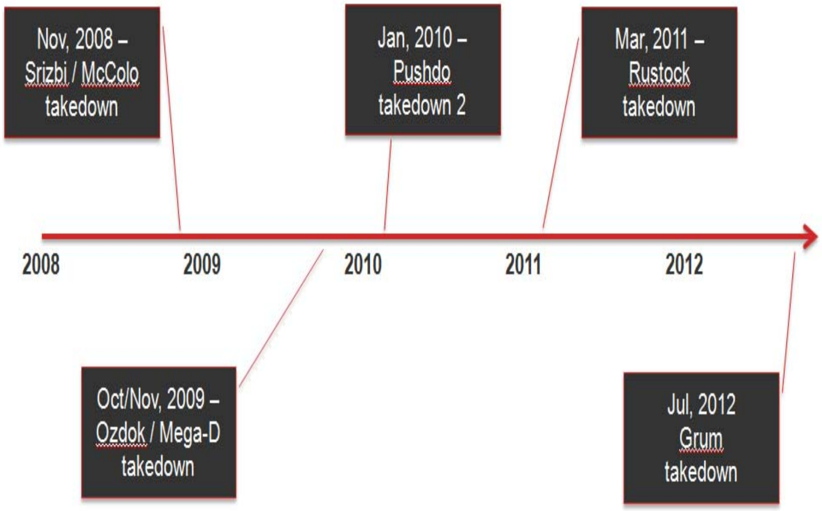
Can we dream of a junk-free mailbox? Guess what—it's just a few takedowns away.

World Wide spam levels for the last four years



Source: Spamhaus

Botnet take downs that made a huge dent in the global spam levels



Nov, 2008 – Srizbi / McColo takedown

Jan, 2010 – Pushdo takedown 2

Mar, 2011 – Rustock takedown

Oct/Nov, 2009 – Ozdok / Mega-D takedown

Jul, 2012 Grum takedown

KILLING 75% OF GLOBAL SPAM IN ONE DAY

McColo Corporation was a shell corporation that leased out it's IP space and bandwidth for nefarious actions. It was formed by a 19 year old Russian citizen nicknamed "Kolya McColo. McColo had headquarters in the "**Market Post Tower" San Jose**, **CA**. In august 2008 FireEye found that McColo Corporation was hosting Command and Control servers of all the major Spam botnets. McColo Corp was later shut down, resulting in two thirds reduction in global spam volume.

McColo Headquarter at "Market Post Tower" San Jose, CA

Mega-D

- Aliases: Ozdok
- At its peak responsible for 32% of spam world wide
- Botnet suspected size of 500,000

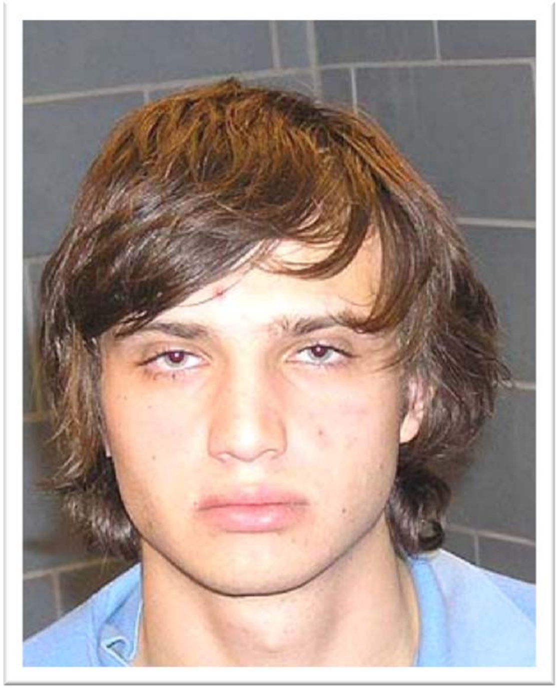
KILLING THE MEGA-D

In November 2010, a Russian citizen Oleg Nikolaenko was arrested in Las Vegas by the FBI and charged with violations of the CAN-SPAM Act of 2003. Nikolaenko later found to be the master mind behind the Mega-D botnet. Mega-d was a botnet that FireEye took-down back in 2009. Nikolaenko was indicted on November 16 at the District Court of Wisconsin and later faced up to five years in prison.

A snippet from FBI's official report

" …Based on Nikoleanko's entry documents, he was expected to stay in the United States until November 11, 2009. However, airline records reveal that Nikoleanko left early. Based on the timing of the FireEye attack on the Mega-D botnet, I believe that Nikoleanko left the U.S. early to repair the damage caused by FireEye. FireEye disabled the Mega-D botnet by disabling its command and control structure, which had an immediate effect on the amount of spam generated by the botnet."

FBI Report Dated February 12, 2010



DDos on FireEye

- Time to celebrate?
- Retaliation for Mega-D suspected
- One of the DDos'ing machines was a customers computer in South Korea
- Determined we have a local copy of the malware generating the Ddos
- With server side exploit we were armed for offensive measures
- FBI coordination and resistance

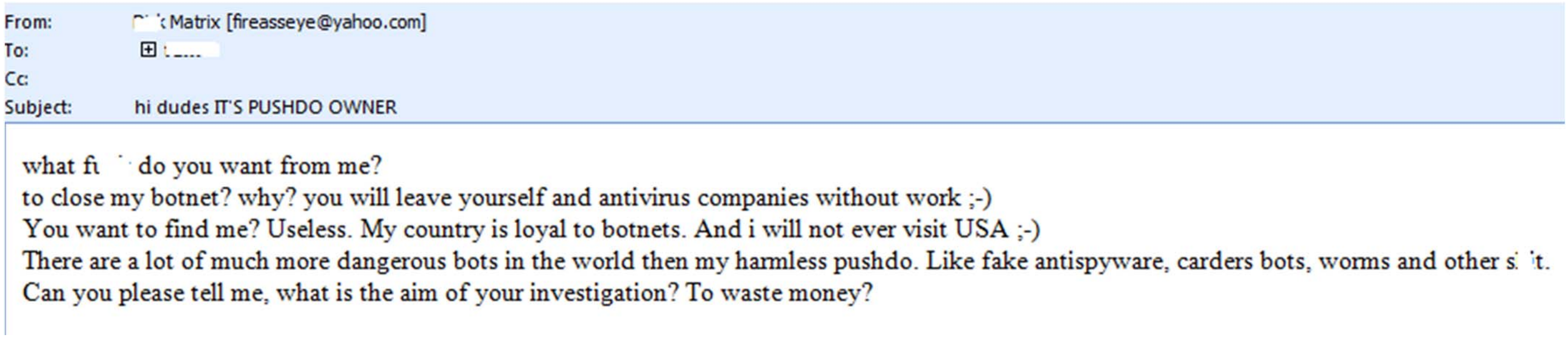
Pushdo

- Aliases: Cutwail
- Peak spam volume 46.5%
- 1.5 – 2 million infected machines
- Known as “0bulk Psyche Evolution”
- For rent botnet
- Advertised services on spambot.biz
- At least 8 different spam groups were using this botnet to deliver junk mail

Pushdo, with Love from Russia

It’s an open secret that almost all the major spam botnets are operated from Russia. Spam in Russia is a serious business, my later conversations with Pushdo bot herder revealed that he is running his botnet just like a conventional software company. He has a office in Moscow and a staff of around ten. This includes developers, guys responsible for developing new evasion techniques, etc.. He said he himself concentrates on business side. His annual profit last year was around $ 450, 000

Pushdo bot herder sent an email to FireEye after we took down his botnet.



From: k Matrix [fireasseye@yahoo.com]
To: ⊞
Cc:
Subject: hi dudes IT'S PUSHDO OWNER

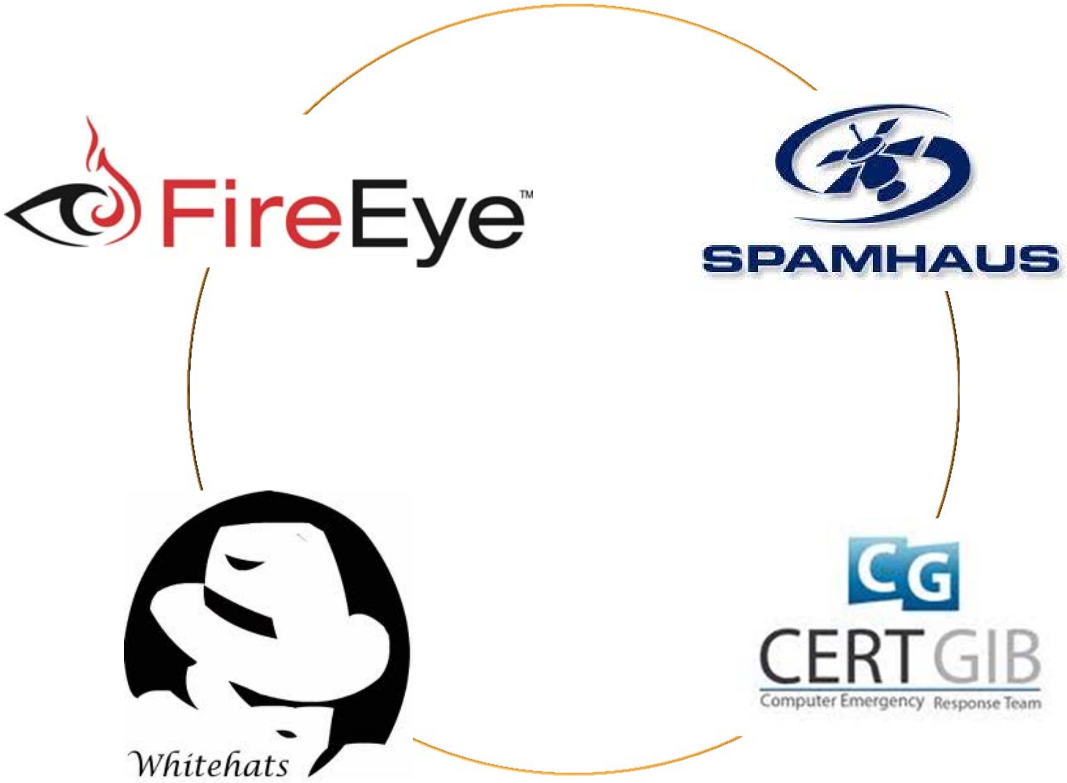
what fu do you want from me?
to close my botnet? why? you will leave yourself and antivirus companies without work ;-)
You want to find me? Useless. My country is loyal to botnets. And i will not ever visit USA ;-)
There are a lot of much more dangerous bots in the world then my harmless pushdo. Like fake antispyware, carders bots, worms and other s t.
Can you please tell me, what is the aim of your investigation? To waste money?

Grum

- Aliases: Tedroo, Reddyb
- Spam levels 18% at takedown and peaked at 26%
- Infected machines 560,000 – 840,000
- Operations: Pharma Spam mainly

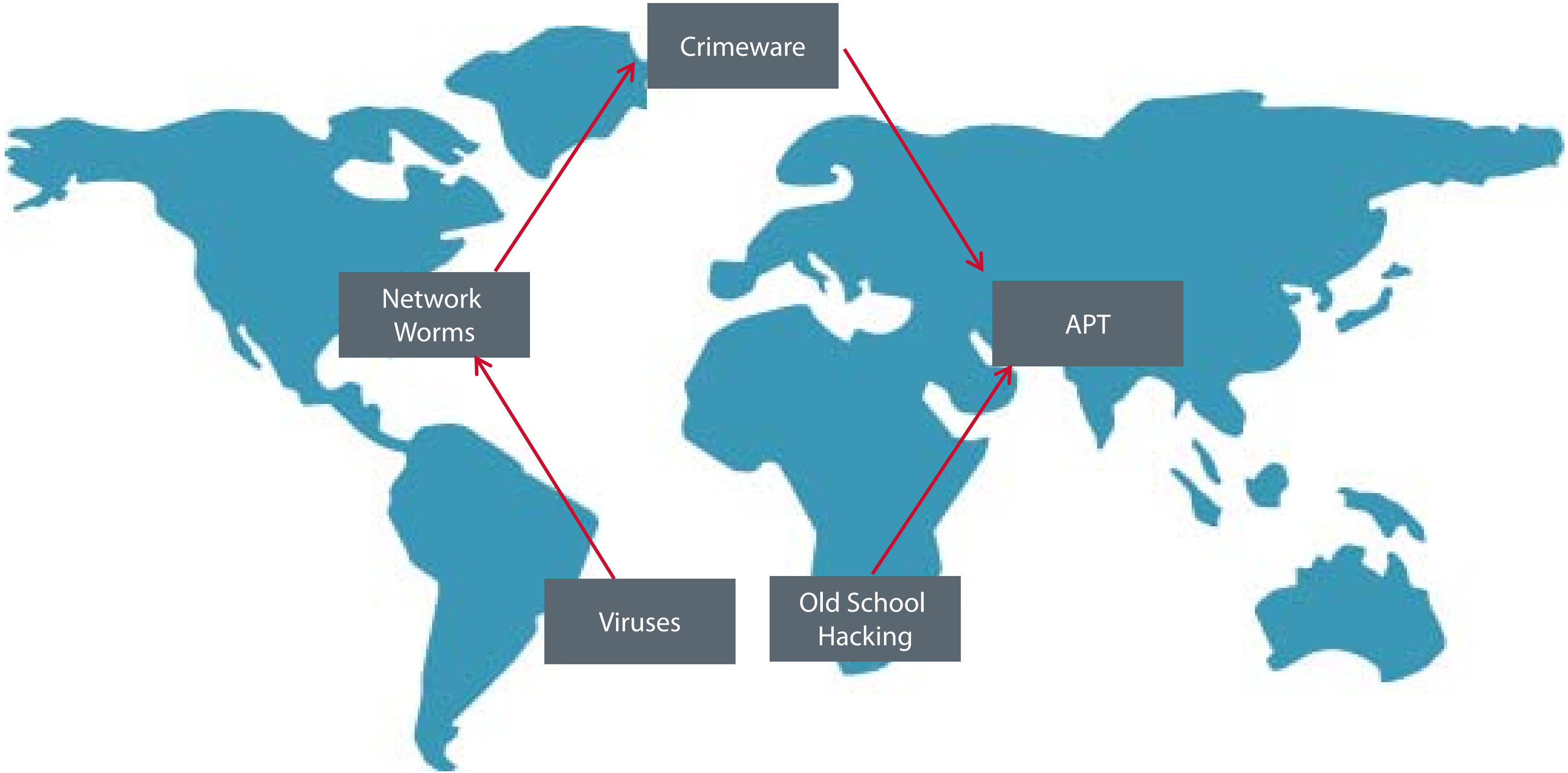
GRUM TAKEDOWN, GOOD vs EVIL

I strongly believe in botnet take-downs that are driven by the community. Organizations like Spamhaus and CERT-GIB played a major role in taking down Grum command and control servers. Without them it would have been very difficult for me to take down servers located in countries like Russia and Ukraine.



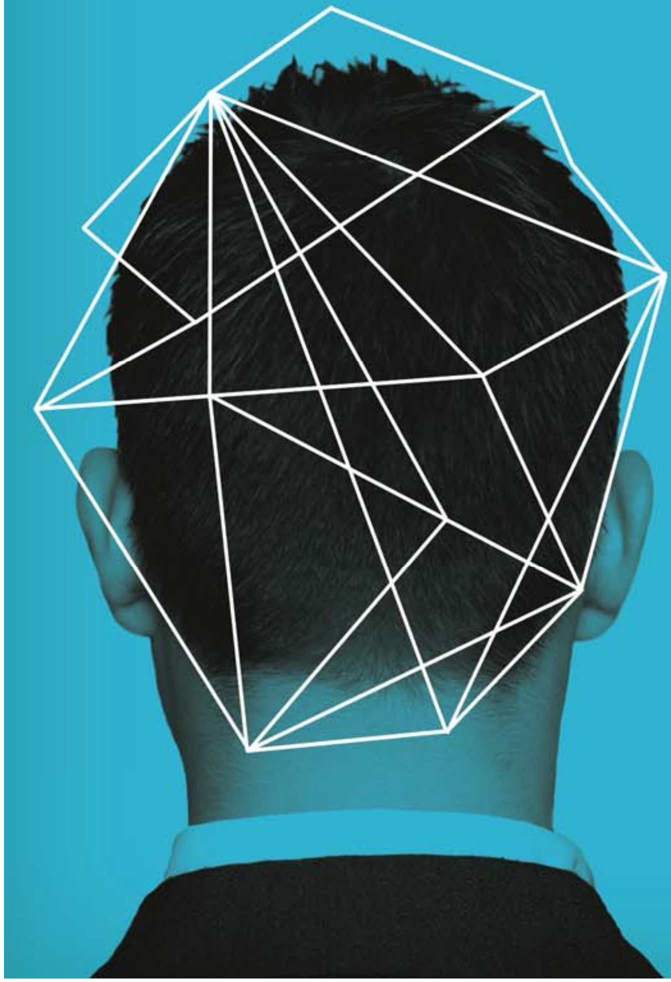
FUTURE OF CYBERWARFARE

The time has come for us to decide how we are going to fight this war in the next decade. Is it going to be just the 'Software (malware)' Vs 'Software (anti-malware)' battle where both guys behind malware and anti-malware are making lots of money and end-users are losing on both ends?



RSA®CONFERENCE2013

Thank You



FireEye™