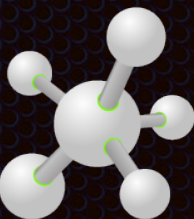


# 2013 - The year in Review

thinkst applied research

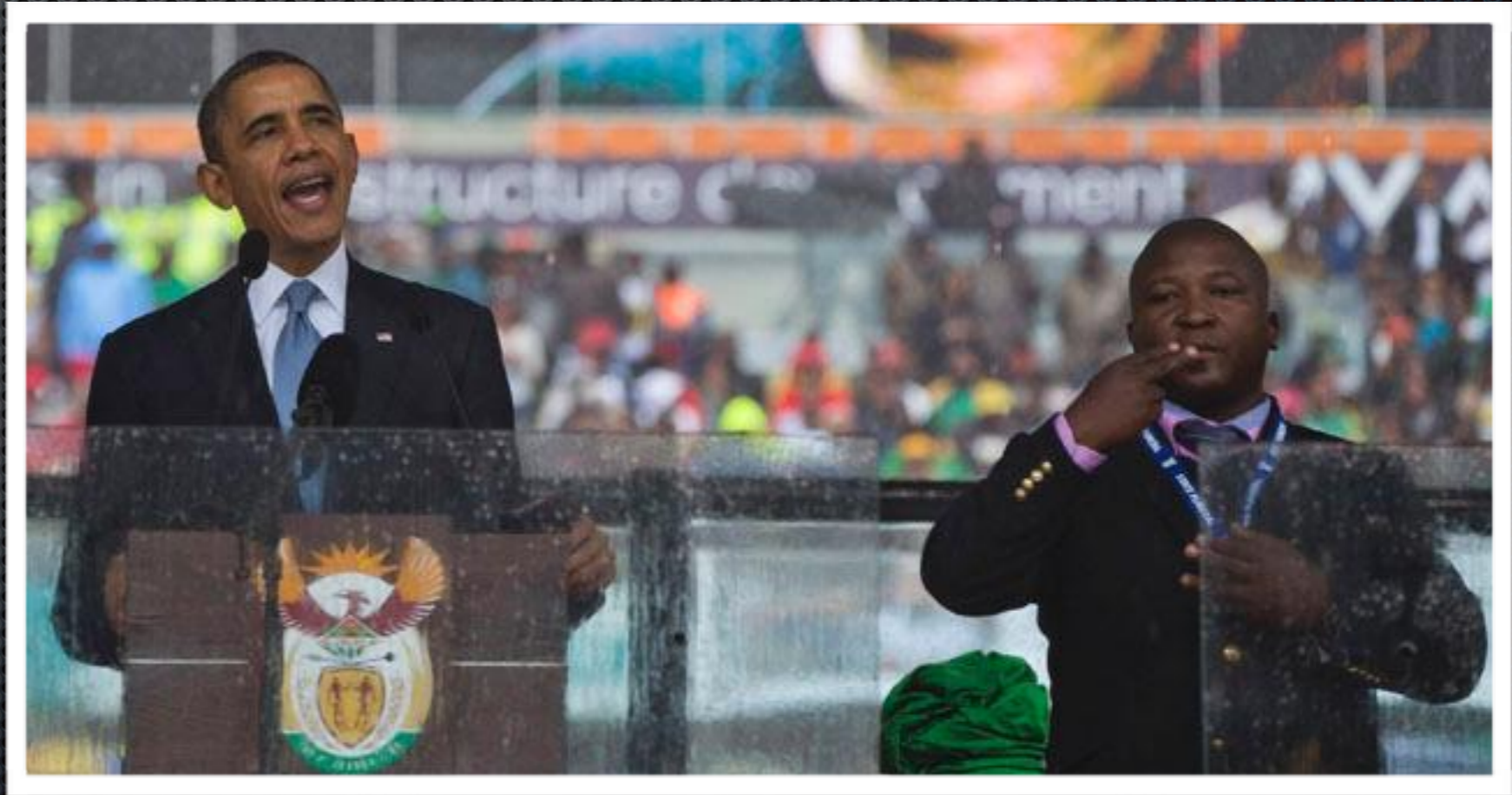
@haroonmeer | @marcoslaviero





Who we are  
(and why does it matter?)







Who we are  
(and why does it matter?)



So... 2013





# 2013

Significant Events

Research Themes

Future Themes ?





# References / Links

- <http://www.theguardian.com/commentisfree/2013/dec/16/fake-mandela-memorial-interpreter-schizophrenia-signing>
- <http://thinkst.com/thinkstscapes>
- <http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html>
- [http://intelreport.mandiant.com/Mandiant\\_APT1\\_Report.pdf](http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf)
- [http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin\\_strategy\\_on\\_mitigating\\_the\\_theft\\_of\\_u.s.\\_trade\\_secrets.pdf](http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf)
- <http://www.aljazeera.com/indepth/opinion/2013/02/201322510446268971.html>
- <http://www.exploit-db.com/papers/25306/HTP5>
- <http://blog.thinkst.com/2013/10/when-we-win-it-is-with-small-things-and.html>
- <http://www.cert.org/flocon/2013/presentations/bellovin-keynote-thinking-security.pdf>
- <https://media.blackhat.com/eu-13/briefings/Gaivoronski/bh-eu-13-hybrid-defense-gaivoronski-slides.pdf>
- <https://zmap.io/>
- <http://blog.erratasec.com/2013/09/masscan-entire-internet-in-3-minutes.html#.UrHC5GQW1Ec>
- <https://dominicspill.com/daisho/Daisho-Troopers13.pdf>
- [https://www.troopers.de/wp-content/uploads/2012/12/TROOPERS13-You\\_wouldnt\\_share\\_a\\_syringe\\_Would\\_you\\_share\\_a\\_USB\\_port-Sergey\\_Bratus%20Series.pdf](https://www.troopers.de/wp-content/uploads/2012/12/TROOPERS13-You_wouldnt_share_a_syringe_Would_you_share_a_USB_port-Sergey_Bratus%20Series.pdf)
- <http://int3.cc/products/usbcondoms>
- <http://conference.hitb.org/hitbsecconf2013ams/materials/D1T1%20-%20Hugo%20Teso%20-%20Aircraft%20Hacking%20-%20Practical%20Aero>
- [http://web.sec.uni-passau.de/papers/2013\\_Braun\\_Gemein\\_Reiser\\_Posegga-Control-Flow\\_Integrity\\_in\\_Web\\_Applications.pdf](http://web.sec.uni-passau.de/papers/2013_Braun_Gemein_Reiser_Posegga-Control-Flow_Integrity_in_Web_Applications.pdf)
- <http://forums.juniper.net/inet/attachments/inet/networkingnow/590/1/bsides%20intrusion%20deception.ppt>
- [http://ritter.vg/blog-deanonymizing\\_amm.html](http://ritter.vg/blog-deanonymizing_amm.html)
- <http://blog.kaspersky.com/roundup-2013/>
- <http://www.slideshare.net/zanelackey/attackdriven-defense>
- <https://ruxconbreakpoint.com/assets/slides/building%20antibodies%2060%20min.pdf>
- <http://www.icir.org/vern/papers/covert-dns-usec13.pdf>
- <http://geer.tinho.net/geer.nro.6xi13.txt>



# OMG!!! CHINA

International New York Times Business Day  
**Technology**

---

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

---

## Hackers in China Attacked The Times for Last 4 Months



**MANDIANT**

APT1  
Exposing One of China's Cyber Espionage Units





## APT1

Exposing One of China's Cyber Espionage Units

### 3 Broad Sections:

- Unit 61398
- APT1
- Conclusion



MANDIANT

**APT1**

Exposing One of China's Cyber Espionage Units

ADMINISTRATION STRATEGY  
ON MITIGATING THE  
THEFT OF U.S. TRADE SECRETS



FEBRUARY 2013



“The secretary of state, Hillary Rodham Clinton, said on Thursday that a global effort was needed to establish rules for cyberactivity.”





## APT1

Exposing One of China's Cyber Espionage Units

## 3 Broad Sections:

- Unit 61398
- APT1
- Conclusion



**MANDIANT**

## APT1

Exposing One of China's Cyber Espionage Units

# Hacking incidents and the rise of the new Chinese bogeyman

Many are beginning to realise that the military digital complex can be more profitable than its industrial complex.

## 3 Broad Sections:

- ✦ Unit 61398
- ✦ APT1
- ✦ Conclusion

thinkst  
applied research



[info@thinkst.com](mailto:info@thinkst.com)  
[research@thinkst.com](mailto:research@thinkst.com)  
<http://www.thinkst.com>

Client: Haroon Meer

ThinkScapes Ad-hoc Information Update 2013 / AH1

China Did It





## Hacking incidents and the rise of the new Chinese bogeyman

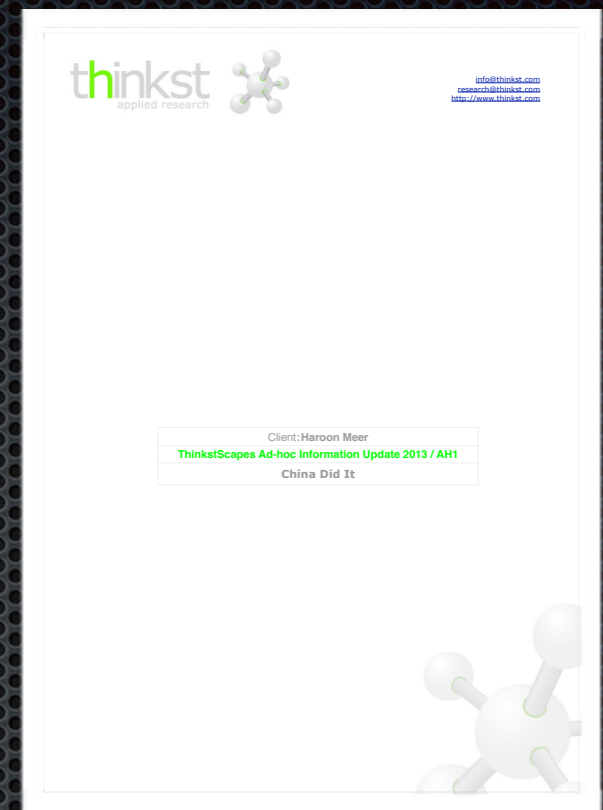
Many are beginning to realise that the military digital complex can be more profitable than its industrial complex.

The new policy document pushed through by the White House includes the promise of "Enhanced Domestic Law Enforcement Operations" and "Improved Domestic Legislations" as two of its five strategic action items.

The penny drops. First comes the bogeyman, and then comes the protection we need:

**more legislation and more law enforcement.**





There is little cost to posting analysis online, especially where the conclusions pass a basic smell test or reinforce preconceived ideas. But there are many types of analysis including recounts of hacks, malware analysis by both professionals and amateurs, intelligence analysis in tracking down attackers, statistics and metrics and general punditry. Each has different burdens of proof, depending on the conclusions drawn and the value assigned to the results.

***The APT1 report was portrayed as conclusive evidence of Chinese military espionage, but instead it is more akin to an intelligence estimate, in which separate threads are woven together into a form acceptable to the analyst, but alternatives have not been excluded.***

Mandiant provide no confidence interval for their estimate, except to state “beyond reasonable doubt”!





**NMAP PROJECT**



**linode**



- HTP vs. MIT
- Rival group on SwiftIRC
- SwiftIRC has Linode Servers
- Linode uses name.com for DNS
- Linode + old code
- Access to Nmap, Nagios, Sucuri, Hak5 (and the machine i still use to irc)



- Rational actor myth
- Determination & Patience
- Incident Response
- Detection
- Supply Chain Problems







- Dismissal
- Sysadmin danger!
- USB : Unlimited Secrets Bus
- US-centric Clouds



PS | AS






# On the fringes



## UPDATE 3-Saab wins Brazil jet deal after NSA spying sours Boeing bid

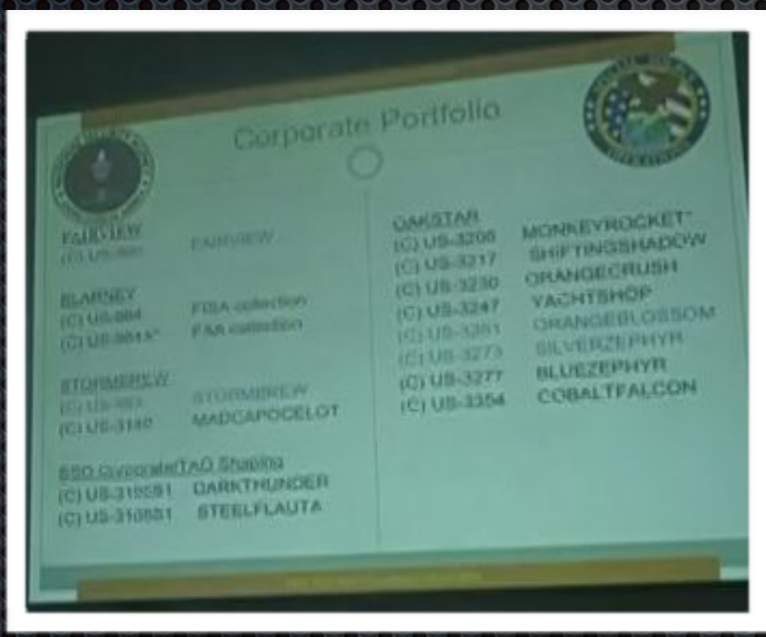
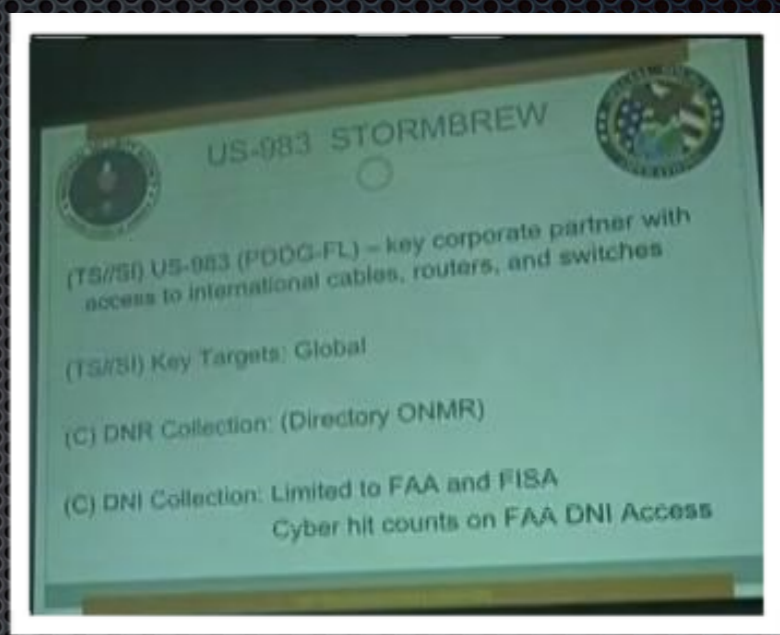
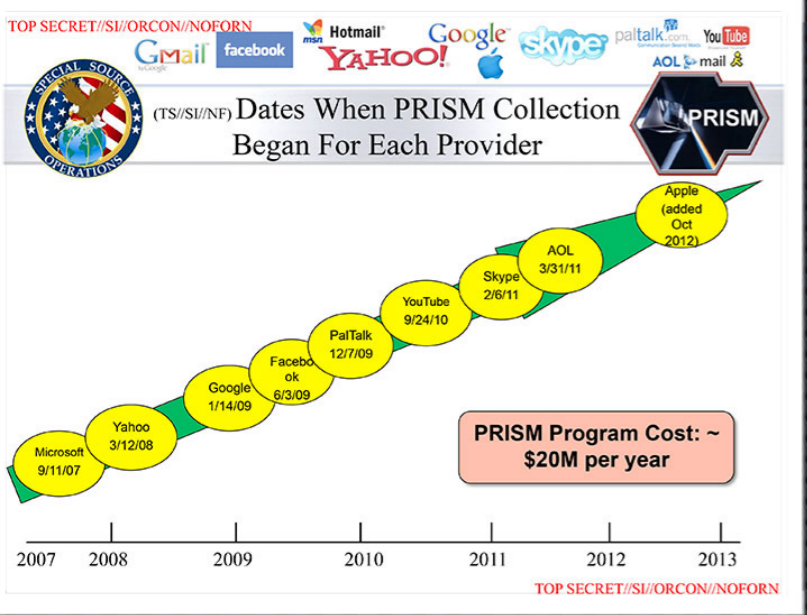
Wed Dec 18, 2013 6:20pm EST

5 COMMENTS |    Share this   Email  Print

By Alonso Soto and Brian Winter

Dec 18 (Reuters) - [Brazil](#) awarded a \$4.5 billion contract to Saab AB on Wednesday to replace its aging fleet of fighter jets, a surprise coup for the Swedish company after news of





BLARNEY AT A GLANCE

Why: started in 1978 to provide FISA authorized access to communications of foreign establishments, agents of foreign powers, and terrorists

External Customers (Who)	Information Requirements (What)	Collection Access and Techniques (How)
<ul style="list-style-type: none"> <li>Department of State</li> <li>Central Intelligence Agency</li> <li>United States UN Mission</li> <li>White House</li> <li>Defense Intelligence Agency</li> <li>National Counterterrorism Center</li> <li>2<sup>nd</sup> Party-GBR, NZL, CAN, AUS</li> <li>Office of Director of National Intelligence</li> <li>Joint Chiefs of Staff</li> <li>Department of Homeland Security</li> <li>Office of Secretary of Defense</li> <li>North Atlantic Treaty Organization</li> <li>Military Commands (Army, EUCOM)</li> </ul>	<ul style="list-style-type: none"> <li>Counter Proliferation</li> <li>Counter Terrorism</li> <li>Diplomatic</li> <li>Economic</li> <li>Military</li> <li>Political / Intentions of Nations</li> </ul>	<ul style="list-style-type: none"> <li>DNI Strong Selectors</li> <li>DNR Strong Selectors</li> <li>DNI Circuits</li> <li>DNR Circuits</li> <li>Mobile Wireless</li> </ul>
	Partnerships (Where)	Legal Authorities (Approvals)
	<ul style="list-style-type: none"> <li>NSA – SSO, TAO, NTOC, CTA, AAP</li> <li>CIA</li> <li>FBI – Headquarters, NY and DC</li> <li>FBI – Engineering Research Facility</li> <li>DOJ</li> <li>Commercial Providers</li> </ul>	<ul style="list-style-type: none"> <li>NSA FISA</li> <li>CT FBI FISA</li> <li>FISA Amendments Act (FAA)</li> <li>CI FBI FISA</li> <li>BR FISA</li> <li>PR/TT FISA</li> </ul>



[www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html](http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html)

## Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm



REUTERS



# Revealed: how US and UK spy agencies defeat internet privacy and security

The documents show that the agency has already achieved another of the goals laid out in the budget request: to influence the international standards upon which encryption systems rely.

Independent security experts have long suspected that the NSA has been introducing weaknesses into security standards, a fact confirmed for the first time by another secret document. It shows the agency worked covertly to get its own version of a draft security standard issued by the US National Institute of Standards and Technology approved for worldwide use in 2006.

"Eventually, NSA became the sole editor," the document states.



## Cryptographic Standards Statement

September 10, 2013

Recent news reports have questioned the cryptographic standards development process at NIST. We want to assure the IT cybersecurity community that the transparent, public process used to rigorously vet our standards is still in place.

NIST would not deliberately weaken a cryptographic standard. We will continue in our mission to work with the cryptographic community to create the strongest possible encryption standards for the U.S. government and industry at large.

There has been some confusion about the standards development process and the role of different organizations in it. NIST's mandate is to develop standards and guidelines to protect the U.S. government and private industry. Other groups also voluntarily participate in the process.

**reopened the public comment period**

NIST has a long history of working with the NSA and other agencies. The NSA also participates in the NIST cryptography development process because of its recognized expertise. NIST is also required by statute to consult with the NSA.

Recognizing community concern regarding some specific standards, we reopened the public comment period for Special Publication 800-90A and draft Special Publications 800-90B and 800-90C to give the public a second opportunity to view and comment on the standards.

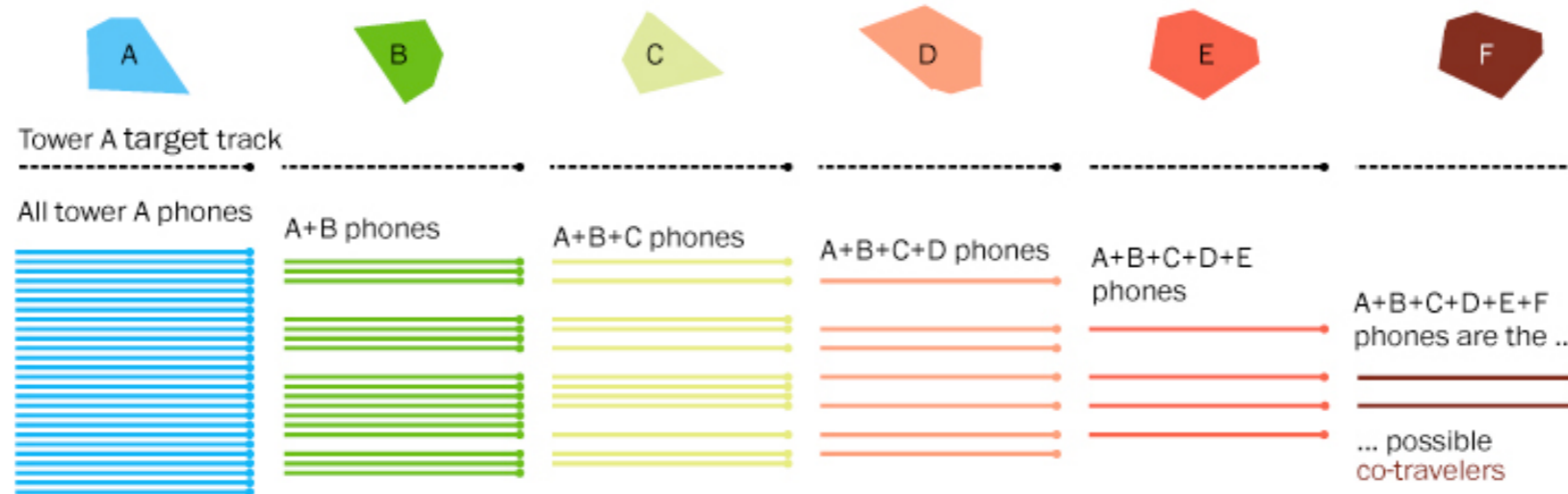
If vulnerabilities are found in these or any other NIST standards, we will work with the cryptographic community to address them as quickly as possible.



By tracking all phones within a cell tower area along with the target phone, co-travelers can be isolated.



As the target phone moves from tower to tower, fewer and fewer potential co-travelers remain.





# Year of the Phish ?



**The New York Times**   
@nytimes

The New York Times Web site is experiencing technical difficulties. We are working on fully restoring the site.

11:23 PM - 27 Aug 2013

481 RETWEETS 59 FAVORITES



**The Associated Press**   
@AP



Following

Breaking: Two Explosions in the White House and Barack Obama is injured

Reply Retweet Favorite More

1,452  
RETWEETS

63  
FAVORITES



12:07 PM - 23 Apr 13

Dow Jones Industrial Average (INDEXDJX: DJI)

**14,692.50** +125.33 (0.86%)

Range 14,554.29 - 14,720.34  
52 week 12,035.09 - 14,887.51  
Open 14,567.17  
Vol. 79.98M

+1 1.6k

Real-time: 1:32PM EDT  
INDEXDJX real-time data - Disclaimer

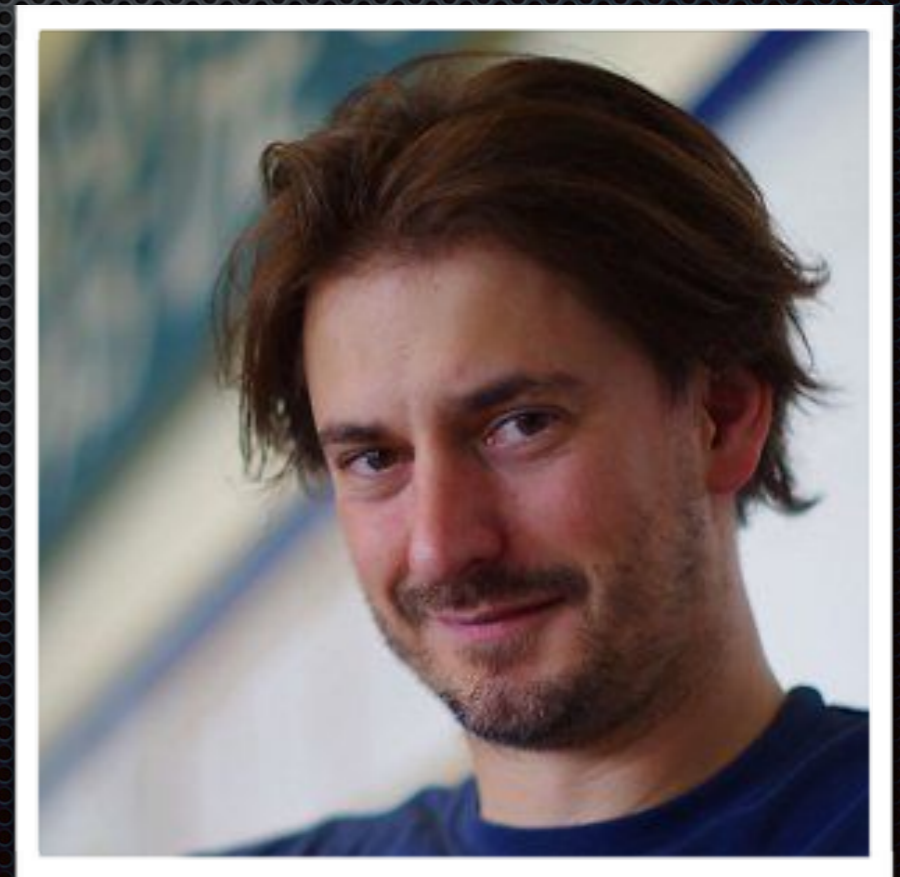
Compare:

Zoom: 1d [3d](#) [1m](#) [3m](#) [6m](#) [YTD](#) [1y](#) [5y](#) [10y](#) [All](#)

Apr 23, 2013 13:32 Price: 14693.04



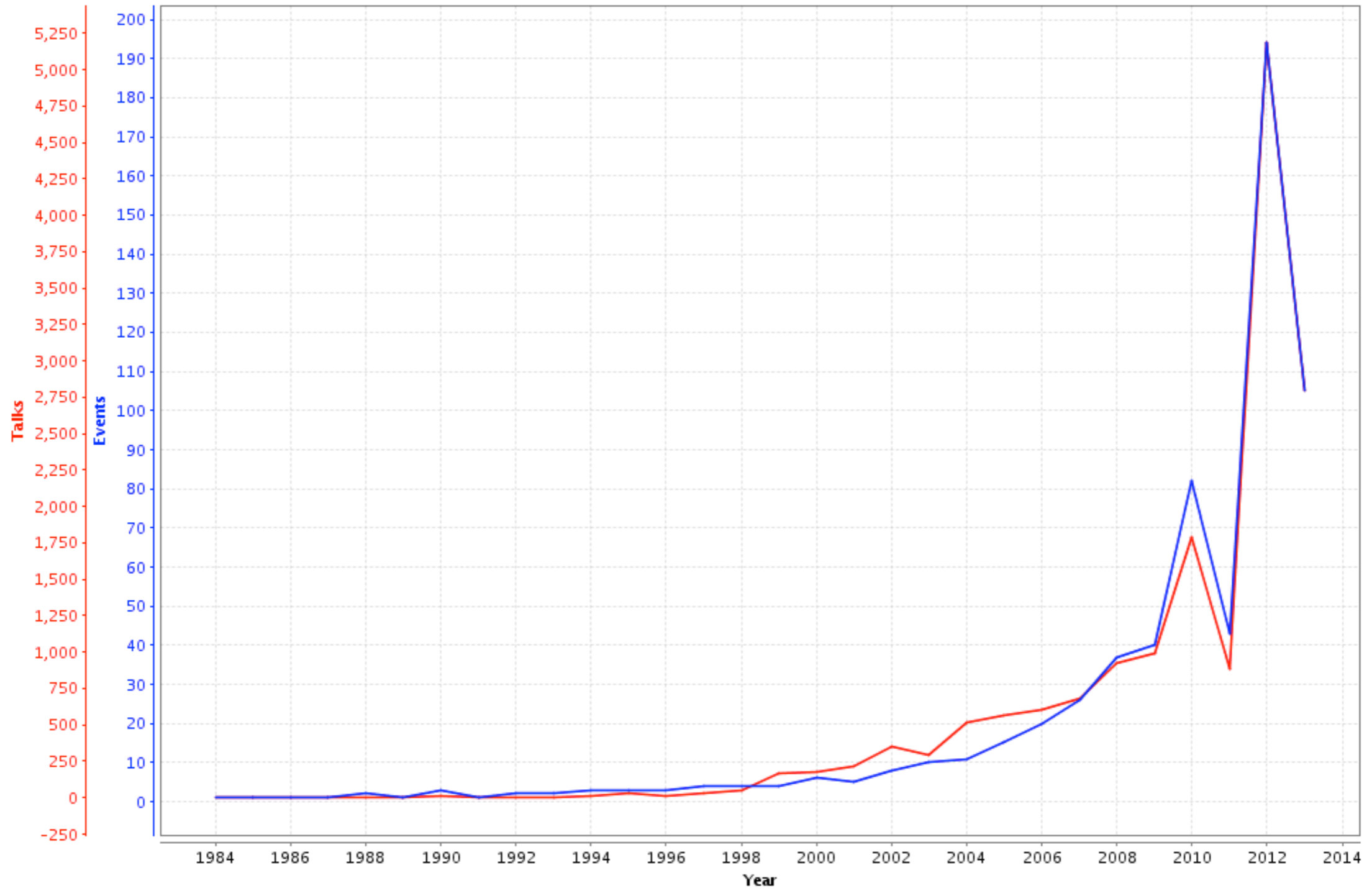




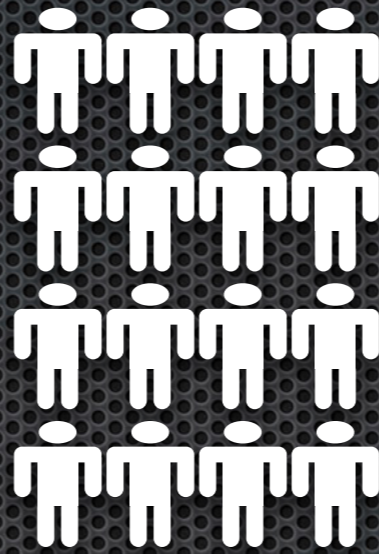


# Let's talk talks (& Research) Trends









# Speakers (BlackHat 1997)



# BlackHat Speakers

2010

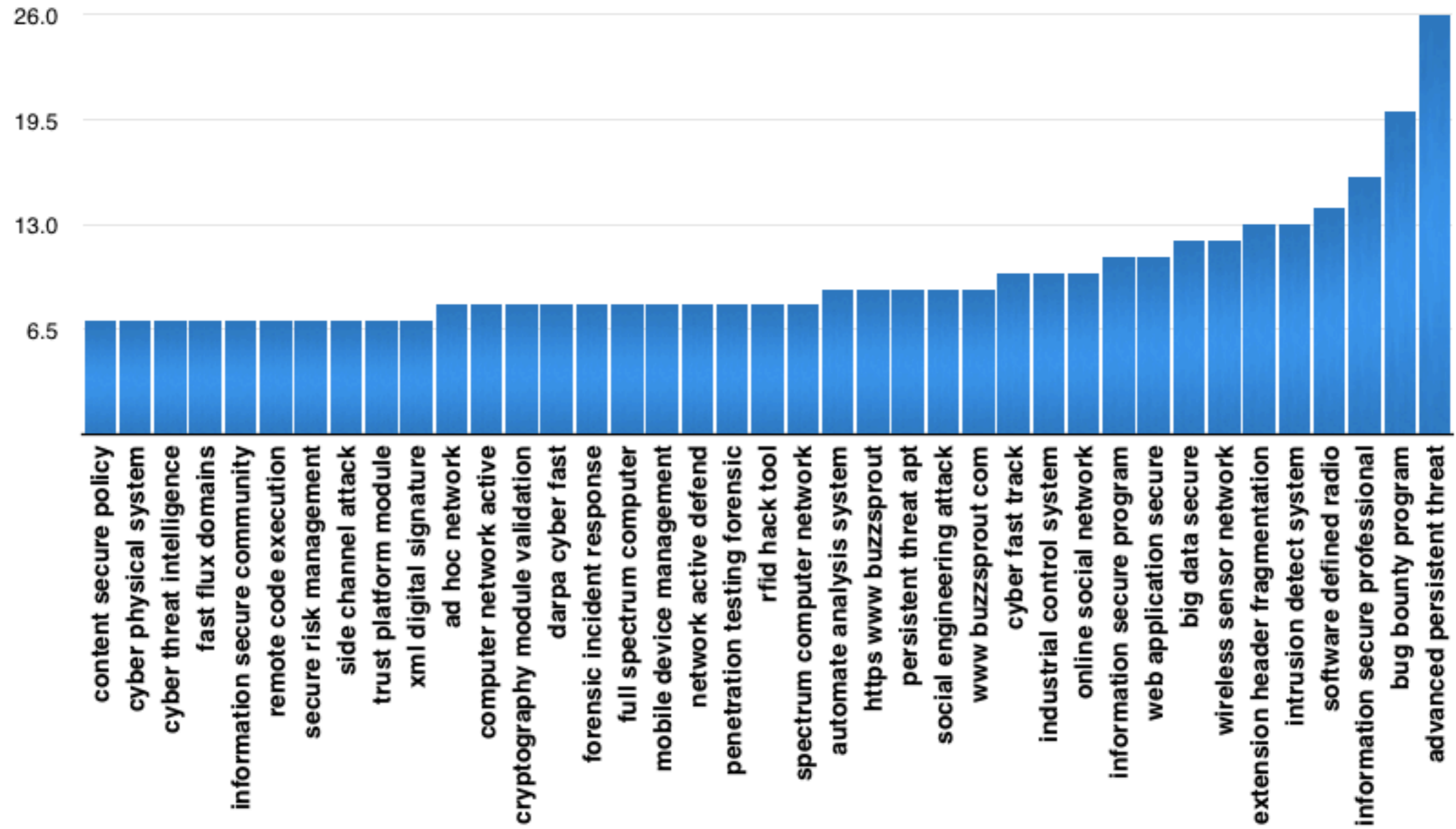


1997





### 3-gram titles and abstracts





Scale

Defense

Metrics

Devices

CyberWar

Active Defense

Bounties

Exploitation





# Thinking Security

Steven M. Bellovin  
Federal Trade Commission/  
Columbia University

These slide are in the public domain.



# Security's Progress

1. There is good research on a new defense
2. Using this defense becomes a recognized "best practice"
3. It is inscribed on assorted auditors' checklists
4. A change in technology or the threat model renders it all but useless
5. It stays on the checklists... (Do you still shred your old punch cards and paper tapes?)

2



# Security Advice

- Pick strong passwords
  - *The Morris-Thompson paper is from 1979, an era of electromechanical terminals and few logins*
- Use a firewall
  - *Smartphones, tablets, and laptops move around*
- Run current antivirus software
  - *It's increasingly ineffective*
- Stay up to date on patches
  - *What about 0-day attacks?*

6



# Flow Rate

- Assume actual traffic of  $P$  packets per second and  $F$  flows/second
  - Implies  $P/F$  packets per flow
- Assume maximum capture rate of  $C$  flows/sec
- What is the relationship of  $F$  and  $C$ ?
- If  $F \gg C$ , we must down-sample and will miss important flows. Ultimate success may depend on technology changes: relative growth of  $F$  and  $C$
- Statistical sampling may mean we'll miss something—and with an intelligent adversary, we may miss what the attackers want us to miss
  - Assumption: the attacker can't manage that. True?

26





**black hat**<sup>®</sup>  
EU 2013

# Hybrid defense: how to protect yourself from polymorphic 0-days

Svetlana Gaivoronski  
PhD student

Dennis Gamayunov  
Senior researcher

Lomonosov Moscow State University



Scale





# Zmap

```
root@supermicro1: ~/masscan
root@supermicro1:~/masscan# bin/masscan 0.0.0.0/0 -p80 --max-rate 30000000 --pfring
/etc/masscan/exclude.txt: excluding 3800 ranges from file

Starting nasscan 1.0 (http://bit.ly/14GZzcT) at 2013-09-14 22:59:14 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 3508758232 hosts [1 port/host]
Rate: 25011.09-kpps, 56.72% done, 0:00:49 remaining, 0-tcps,
```

Scale



# Talk about Talks



Scale

Defense

Metrics

Devices

CyberWar

Active Defense

Bounties

Exploitation



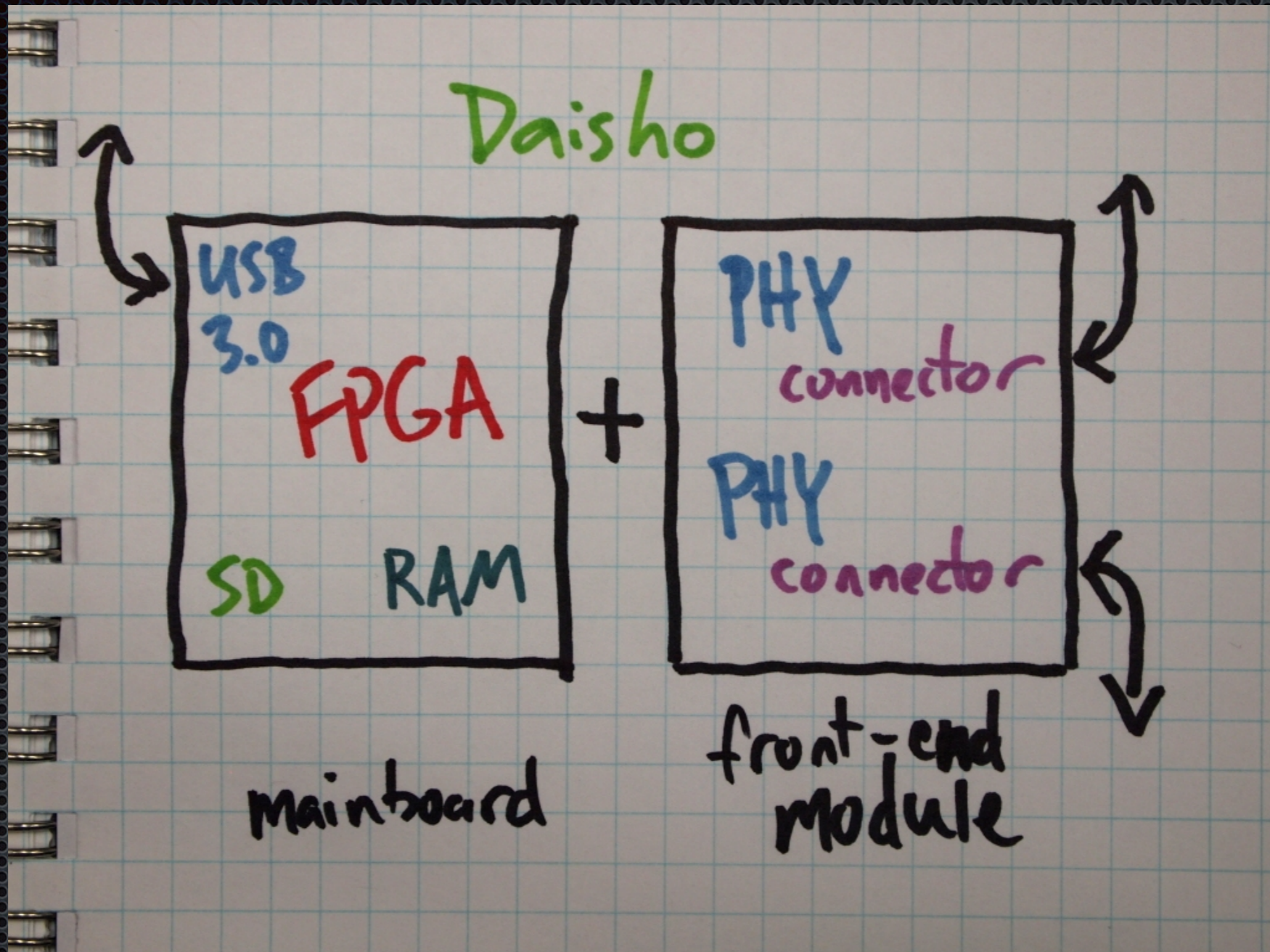


"Security will not get better until tools for practical exploration of the attack surface are made available."  
- Joshua Wright

# Devices







Devices





# Devices



NBC NEWS

Slashdot /.  
News for Nerds. Stuff that matters.

THE VERGE

DiscoveryNews.

examiner.com

EXTREME TECH FAST COMPANY

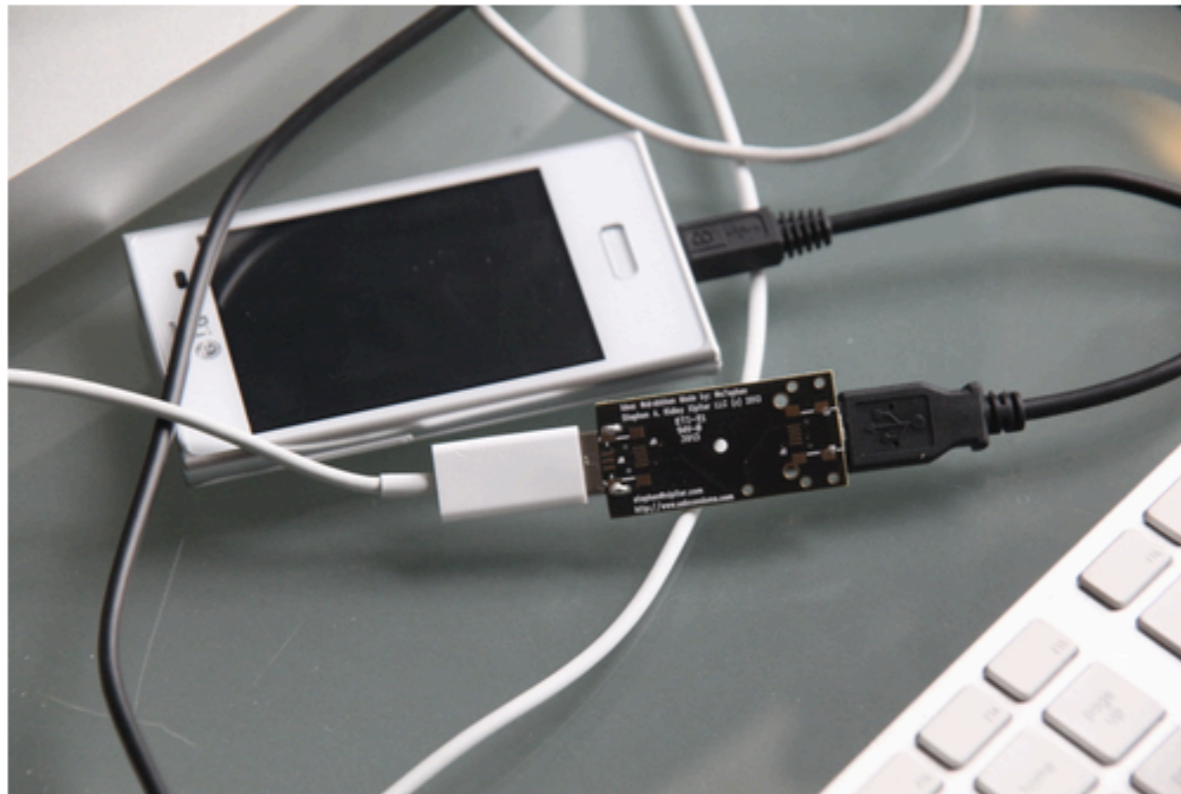
GEEK gizmag

newsy

THE INDEPENDENT

WIRED

VentureBeat



Simplicity.

Security.

The USB Condom protects personal and private data stored on your mobile device, so now you can charge your battery anywhere without fear your data will be stolen, accidentally shared, or infected with a virus! USB Condoms only transfer power, not your data!

# Devices



# Aircraft Hacking (2)

## Attack Overview

### DISCOVERY:

» ADS-B

### INFO GATHERING:

» ACARS

### EXPLOITATION:

» Via ACARS  
» Against on-board systems vulns.

### POST-EXPLOITATION:

» Party hard!

Devices





# Car Hacking



Devices



Scale

Defense

Metrics

Devices

CyberWar

Active Defense

Bounties

Exploitation





- Control-Flow integrity in Web Applications
- Sorry Your Princess is in Another Castle: Intrusion Deception to Protect the Web

Active Defense



Scale

Defense

Metrics

Devices

CyberWar

Active Defense

Bounties

Exploitation





- ✦ Reflection in Managed Languages: James Foreshaw
- ✦ Breaking XML DigSig: James Foreshaw
- ✦ UEFI Attacks
- ✦ Android Attacks
- ✦ De-Anonymizing Alt.Anonymous.Messages

# Exploitation



# MOBILE MALWARE IN 2013

TROJAN-DOWNLOADER

7% ↓

OTHER

15%

TROJAN

16% ♁

TROJAN-SMS

36%

BACKDOOR

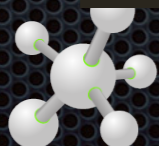
26%

104421 SAMPLES WERE DISCOVERED

98% WERE ANDROID MALWARE SAMPLES

[twitter.com/Kaspersky](https://twitter.com/Kaspersky)

<http://kas.pr/re2013>





- ✦ Reflection in Managed Languages: James Foreshaw
- ✦ Breaking XML DigSig: James Foreshaw
- ✦ UEFI Attacks
- ✦ Android Attacks
- ✦ De-Anonymizing Alt.Anonymous.Messages

# Exploitation



Scale

Defense

Metrics

Devices

CyberWar

Active Defense

Bounties

Exploitation





- ✦ A Password is Not Enough: Why disk encryption is broken and how we might fix it
- ✦ Finding DNS tunnels through information theory (“Practical Comprehensive Bounds on Surreptitious Communication over DNS”)
- ✦ Attack Driven Defense
- ✦ Phishing as training “Building Antibodies – The Phishing program at Twitter”

# Defense





Advanced Persistent Tapestries



## Historically defense has:

- Focused on the perimeter
- Deployed security products that don't address real attack scenarios
- Treated vulnerability enumeration (or worse, compliance) as “pentesting”



Fundamentally we have three goals:

- 1) Raise cost to attackers
- 2) Increase the odds of detecting compromise
- 3) Iterate defenses based on real attack patterns



Attack simulations should be done to learn how attackers are likely to **achieve goals** against your organization

NOT to show compromise is possible  
(spoiler alert: it is.)



## Instrument detection mechanisms around key areas of the attack chain:

- Initial compromise
  - Defensive rootkitting
- Persistence/C2
  - Host level
  - Organizational level
- Lateral Movement
  - Network/systems discovery
  - Information discovery





- ✦ A Password is Not Enough: Why disk encryption is broken and how we might fix it
- ✦ Finding DNS tunnels through information theory (“Practical Comprehensive Bounds on Surreptitious Communication over DNS”)
- ✦ Attack Driven Defense
- ✦ Phishing as training “Building Antibodies – The Phishing program at Twitter”

# Defense



# Phishing is a big deal.

**These are some organizations that have been owned recently via phishing:**

Google

Facebook

LinkedIn

Associated Press

BBC

CNN

The Onion

Sony

Sky News

The White House

Palantir

HotMail

MySpace

WordPress

Zappos

Gawker

HB Gary

Arizona Sheriffs

Department

The FBI

Washington Post





<http://phish5.com>





Scale

Defense

Metrics

Devices

CyberWar

Active Defense

Bounties

Exploitation






- ✦ Extremely prominent researchers shout them down, but the programs allow up-n-coming folks to get started.
- ✦ Google started paying for open source bugs and fixes.
- ✦ Microsoft now pays out for mitigation bypasses.
- ✦ Bugcrowd
- ✦ “An Empirical Study of Vulnerability Rewards Programs” shows that for the cost of roughly 1 security engineer, programs returned about 25% of all significant bugs.



# [Rising|Falling] Trends



- 
- ✦ BYOD
  - ✦ Hacktivism
  - ✦ SCADA
  - ✦ Mobile (we hope)
  - ✦ StrikeBack

- 
- ✦ LE Hacks
  - ✦ Big Data?
  - ✦ OPSEC
  - ✦ Drones
  - ✦ Sensors
  - ✦ AV Hacks
  - ✦ Privacy
  - ✦ Home Spun Security



# Dan Geer (Trends in CyberSec)

- Trend #10: Complexity in the supply chain
  - Security is non-composable
- Trend #12: Attack surface growth versus skill growth
  - we are expanding the society-wide attack surface faster than we are expanding our





# Dan Geer (Trends in CyberSec)

“Where there are so many questions and so few answers, such deep needs and such shallow appreciation of trend directions, the greatest risk is the risk of simplistic solutions carried forward by charismatic fools”



- <http://www.theguardian.com/commentisfree/2013/dec/16/fake-mandela-memorial-interpreter-schizophrenia-signing>
- <http://thinkst.com/thinkstscapes>
- <http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html>
- [http://intelreport.mandiant.com/Mandiant\\_APT1\\_Report.pdf](http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf)
- [http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin\\_strategy\\_on\\_mitigating\\_the\\_theft\\_of\\_u.s.\\_trade\\_secrets.pdf](http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf)
- <http://www.aljazeera.com/indepth/opinion/2013/02/201322510446268971.html>
- <http://www.exploit-db.com/papers/25306/HTP5>
- <http://blog.thinkst.com/2013/10/when-we-win-it-is-with-small-things-and.html>
- <http://www.cert.org/flocon/2013/presentations/bellovin-keynote-thinking-security.pdf>
- <https://media.blackhat.com/eu-13/briefings/Gaivoronski/bh-eu-13-hybrid-defense-gaivoronski-slides.pdf>
- <https://zmap.io/>
- <http://blog.erratasec.com/2013/09/masscan-entire-internet-in-3-minutes.html#.UrHC5GQW1Ec>
- <https://dominicspill.com/daisho/Daisho-Troopers13.pdf>
- [https://www.troopers.de/wp-content/uploads/2012/12/TROOPERS13-You\\_wouldnt\\_share\\_a\\_syringe\\_Would\\_you\\_share\\_a\\_USB\\_port-Sergey\\_Bratus\\_+Travis\\_Goodspeed.pdf](https://www.troopers.de/wp-content/uploads/2012/12/TROOPERS13-You_wouldnt_share_a_syringe_Would_you_share_a_USB_port-Sergey_Bratus_+Travis_Goodspeed.pdf)
- <http://int3.cc/products/usbcondoms>
- <http://conference.hitb.org/hitbsecconf2013ams/materials/D1T1%20-%20Hugo%20Teso%20-%20Aircraft%20Hacking%20-%20Practical%20Aero%20Series.pdf>
- <http://blog.ioactive.com/2013/08/car-hacking-content.html>
- [http://web.sec.uni-passau.de/papers/2013\\_Braun\\_Gemein\\_Reiser\\_Posegga-Control-Flow\\_Integrity\\_in\\_Web\\_Applications.pdf](http://web.sec.uni-passau.de/papers/2013_Braun_Gemein_Reiser_Posegga-Control-Flow_Integrity_in_Web_Applications.pdf)
- <http://forums.juniper.net/jnet/attachments/jnet/networkingnow/590/1/bsides%20intrusion%20deception.ppt>
- [http://ritter.vg/blog-deanonymizing\\_amm.html](http://ritter.vg/blog-deanonymizing_amm.html)
- <http://blog.kaspersky.com/roundup-2013/>
- <http://www.slideshare.net/zanelackey/attackdriven-defense>
- <https://ruxconbreakpoint.com/assets/slides/building%20antibodies%2060%20min.pdf>
- <http://www.icir.org/vern/papers/covert-dns-usec13.pdf>
- <http://geer.tinho.net/geer.nro.6xi13.txt>



<http://thinkst.com/thinkstscapes>

@haroonmeer | @marcoslaviero

