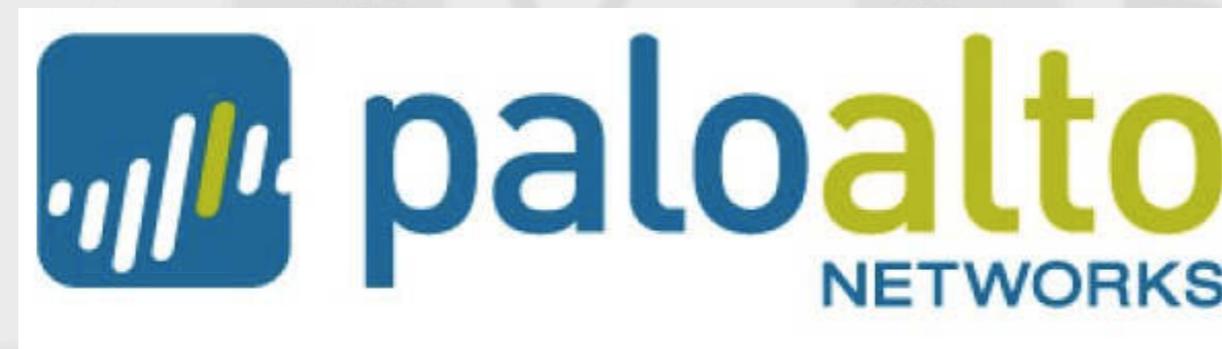




Minneapolis Chapter Palo Alto Networks Fuel Users Group Meeting



milestone systems
SECURITY SIMPLIFIED



7 May 2015

State of Cyber Security



It could be worse!

Source: PBS Sesame Street, Oscar the Grouch

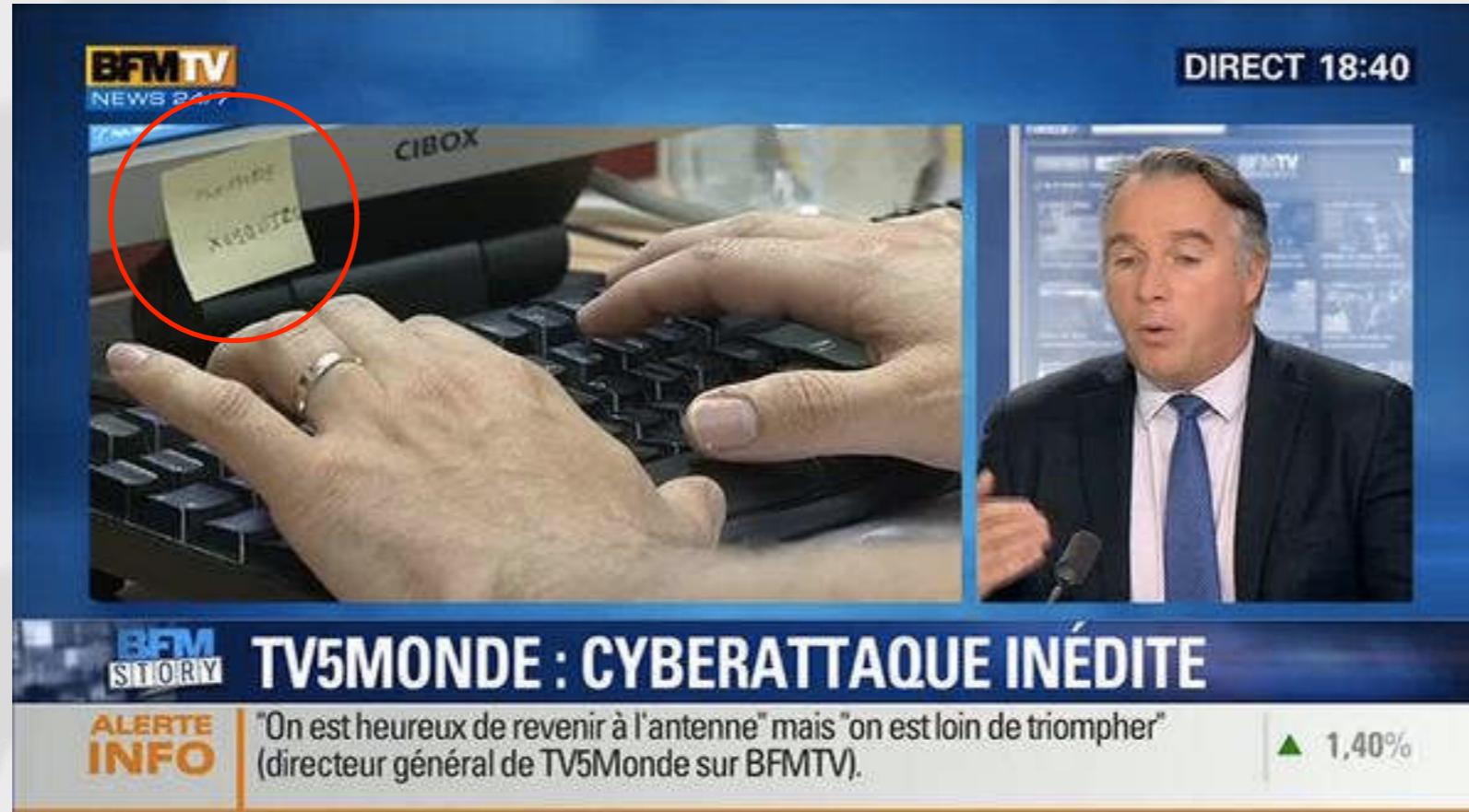
Breaches are inevitable



against a motivated attacker with time and resources

Source: BBC Sherlock Holmes - The Reichenbach Fall
Moriarty stealing the crown jewels

Or with post-it notes



It doesn't take a Super Genius if you publish your post-it note credentials in an interview segment.

Or big sheets of paper in the background



Let's look at some metrics by

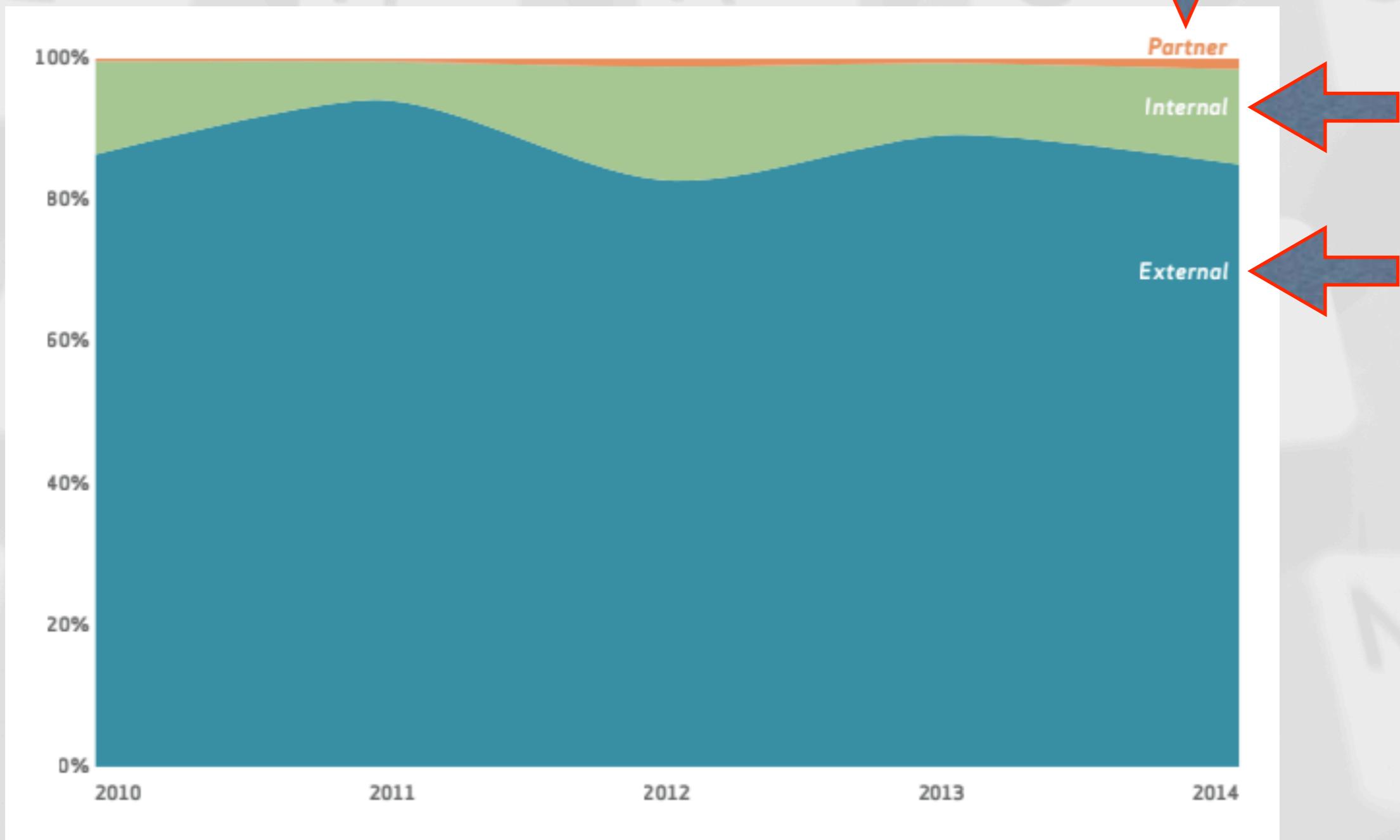


2014 Incidents and Data Loss

INDUSTRY	NUMBER OF SECURITY INCIDENTS				CONFIRMED DATA LOSS			
	TOTAL	SMALL	LARGE	UNKNOWN	TOTAL	SMALL	LARGE	UNKNOWN
Accommodation (72)	368	181	90	97	223	180	10	33
Administrative (56)	205	11	13	181	27	6	4	17
Agriculture (11)	2	0	0	2	2	0	0	2
Construction (23)	3	1	2	0	2	1	1	0
Educational (61)	165	18	17	130	65	11	10	44
Entertainment (71)	27	17	0	10	23	16	0	7
Financial Services (52)	642	44	177	421	277	33	136	108
Healthcare (62)	234	51	38	145	141	31	25	85
Information (51)	1,496	36	34	1,426	95	13	17	65
Management (55)	4	0	2	2	1	0	0	1
Manufacturing (31-33)	525	18	43	464	235	11	10	214
Mining (21)	22	1	12	9	17	0	11	6
Other Services (81)	263	12	2	249	28	8	2	18
Professional (54)	347	27	11	309	146	14	6	126
Public (92)	50,315	19	49,596	700	303	6	241	56
Real Estate (53)	14	2	1	11	10	1	1	8
Retail (44-45)	523	99	30	394	164	95	21	48
Trade (42)	14	10	1	3	6	4	0	2
Transportation (48-49)	44	2	9	33	22	2	6	14
Utilities (22)	73	1	2	70	10	0	0	10
Unknown	24,504	144	1	24,359	325	141	1	183
TOTAL	79,790	694	50,081	29,015	2,122	573	502	1,047

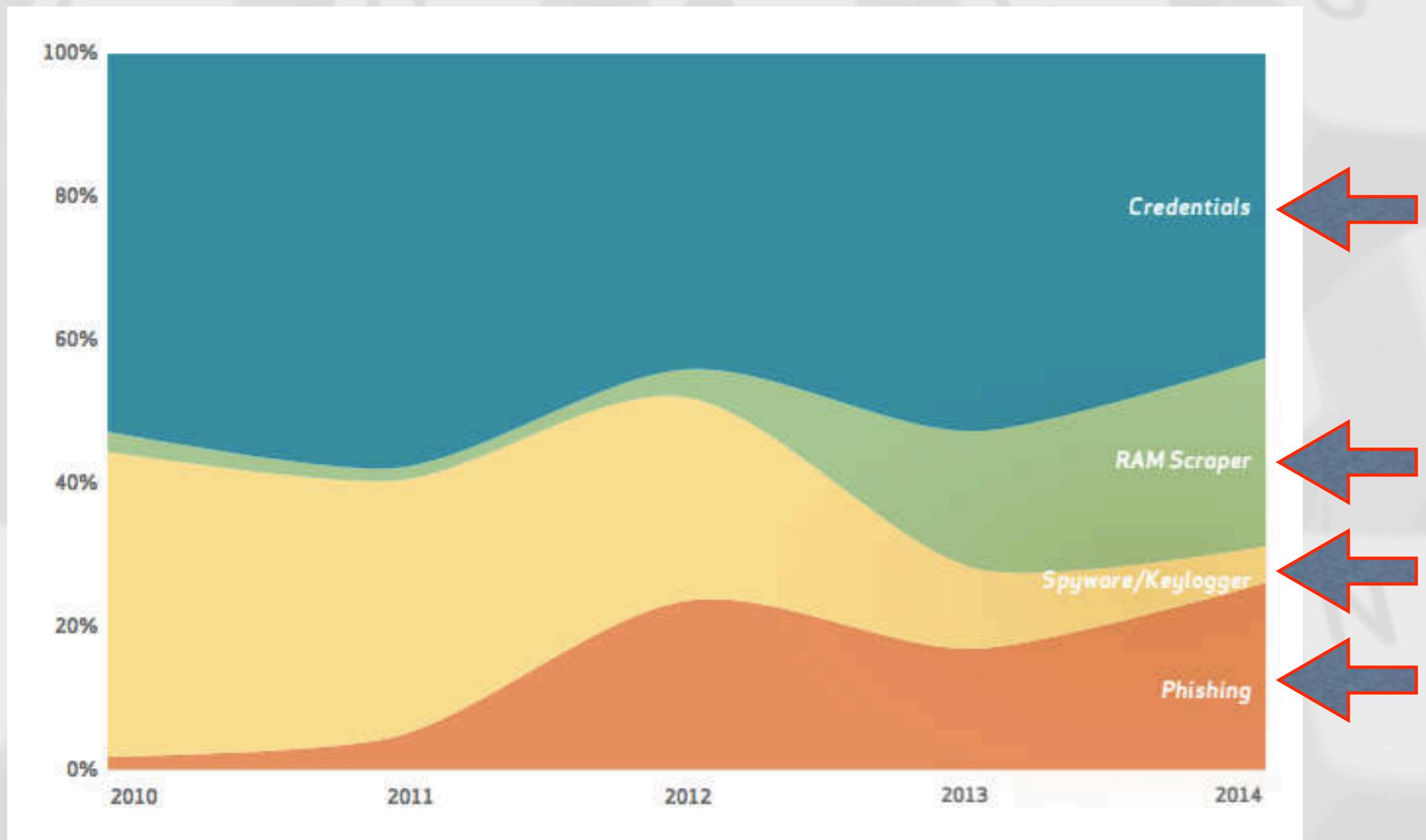
Source:Verizon 2015 Data Breach Investigations Report

2014 Threat Sources



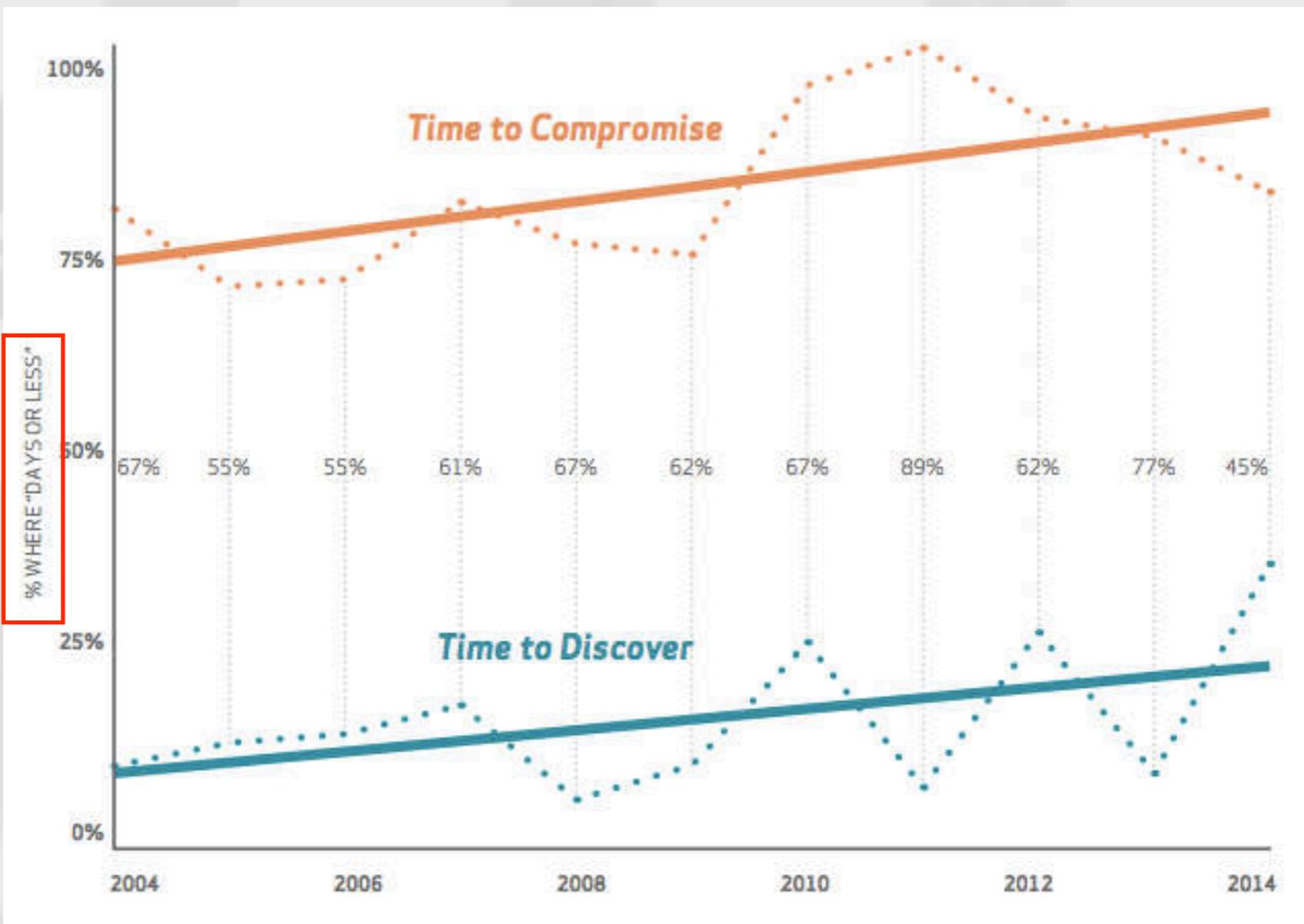
Source: Verizon 2015 Data Breach Investigations Report

2014 Attack Vectors



Source: Verizon 2015 Data Breach Investigations Report

2014 Time to Compromise vs Discover



Source: Verizon 2015 Data Breach Investigations Report

2014 in Summary

Neiman Marcus - **350,000 records**

Hilton, Marriott, Westin and Sheraton - **168 Hotels**

Michaels - **2.6 Mil cards**

Affinity Gaming - **11 Casinos**

New York Attorney General - **22.8 Mil records**

PF Chang - **33 Restaurants**

Community Health Systems - **4.5 Mil patient records**

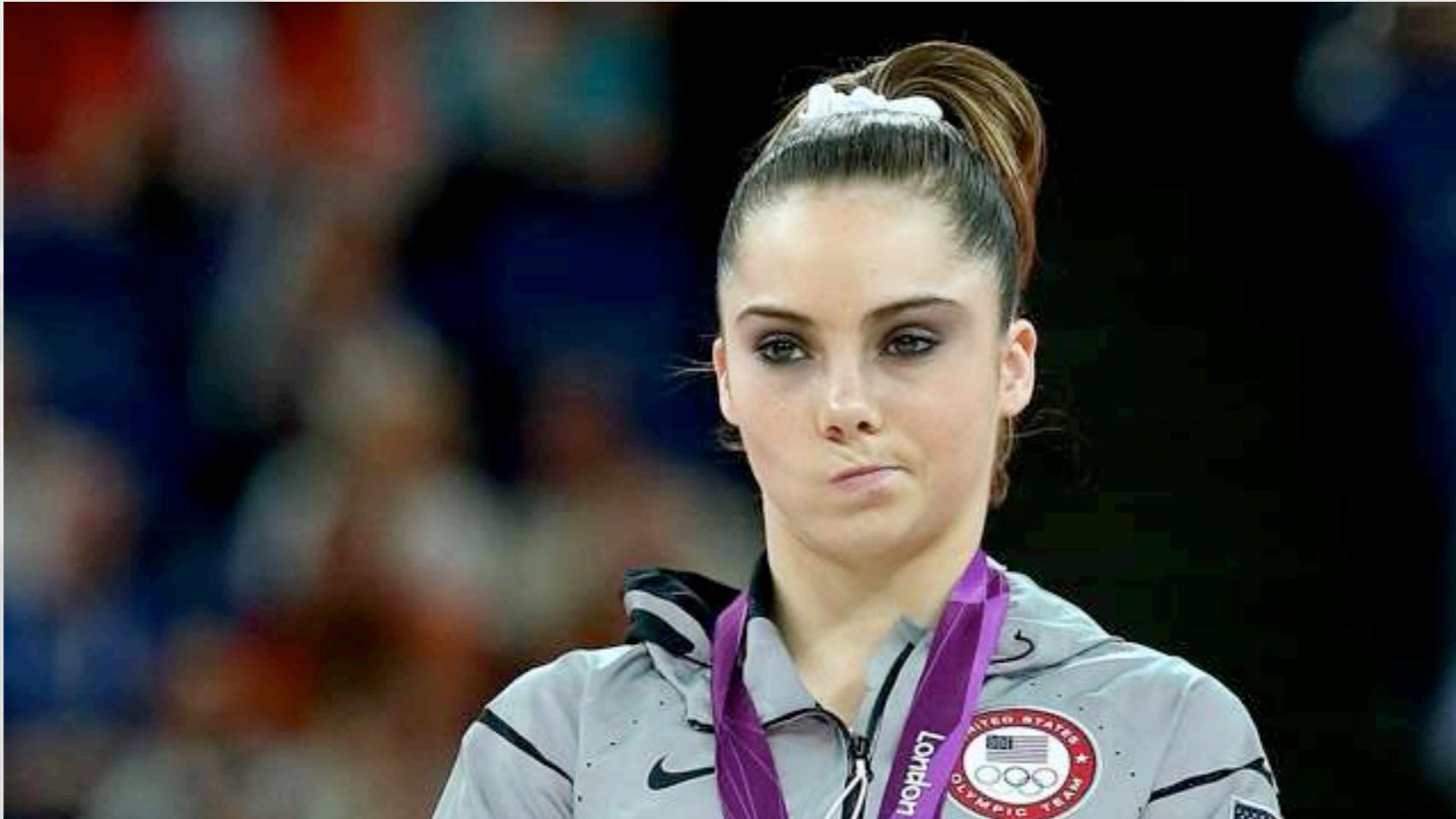
Home Depot - **56 Mil Cards**

Jimmy Johns - **216 stores** (PoS system)

JP Morgan Chase - 76 mil households + 7 mil businesses

... and many, many more.

We really need to get better at this

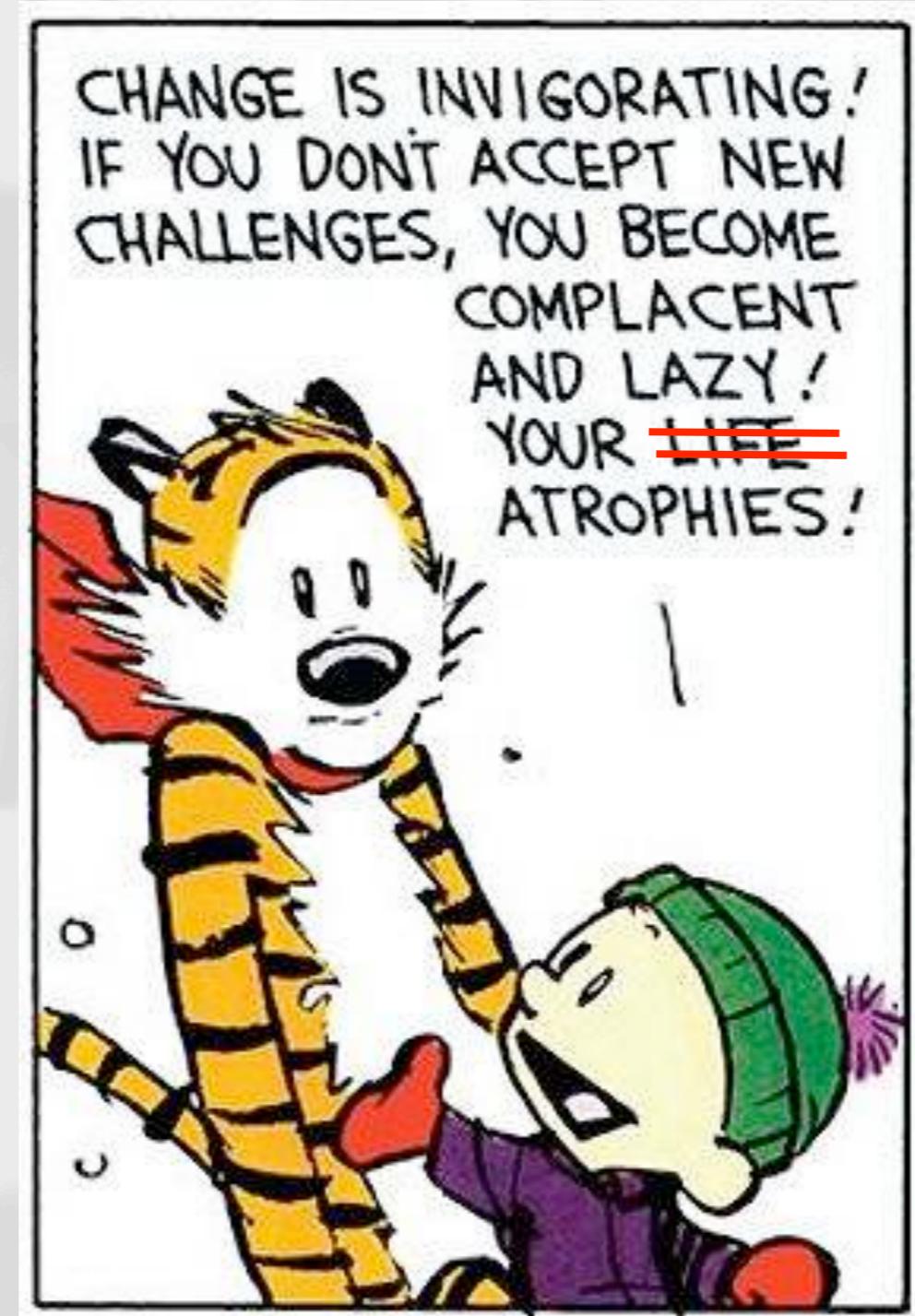


we need to change our approach

Photo: McKayla Maroney, 2012 London Olympics “McKayla Not Impressed”

Change is good, sharing is good.

Network



Source: Calvin and Hobbes by Bill Watterson (1995)

We must learn from each other



Palo Alto Networks
Founding Member



NorSec ISAO

ISAO's per Executive Order "Feb 13, 2015"
Promoting Private Sector Cybersecurity Information Sharing
Per EO 13636 and PPD-21

By sharing what we have an abundance of...



LOGS!!!!

What is Threat Intelligence?

Indicators of Compromise (IoC's)

DNS Hosts
IP Addresses
E-Mail Addresses
URLs
Files (hashes)

+

Relevant Threat Activity

Campaigns
Malware
Known Adversaries

=

Crowd Sourced Actionable Cyber Threat Intelligence
Vetted by experts



NorSec ISAO

Known Adversaries



INDICATORS ▾



ACTIVITY ▾

1010100
1000011

DOCUMENTS ▾



THREATS



TAGS



ADVERSARIES ▾



VICTIMS ▾



WORKFLOW ▾

Filter



Name		Owner	Date Added
Song Yubo		Common Community	02-27-2015
li fei		Common Community	11-18-2014
john.fielder@hotmail.com		Common Community	09-30-2014
tommy.bibber1234321@ddd.com		Common Community	09-30-2014
Li Ning		Common Community	04-18-2014
Hacking Team		Common Community	02-13-2014
Sergey Tarasov		Common Community	01-21-2014
Jack White		Common Community	01-02-2014
rooterit		Common Community	12-20-2013
Wang Zhong Yun		Common Community	12-11-2013

(1 of 2)

10

◀

1

2

▶

Hacking Team

DETAILS

PIVOT

Description:

Hacking Team, also known as HT S.r.l., is a Milan-based purveyor of "offensive technology" to governments around the world.

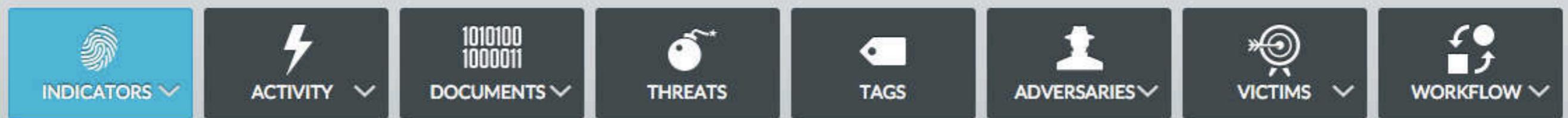
Type: Adversary

Owner: Common Community

Added: 02-13-2014

Tags: Advanced Persistent Threat

Indicators of Compromise



Filter



Type	Summary	Rating	Owner	Date Added
File	190921C61FCF20CF579E625587A2CAE868099523...	💀💀💀💀	Common Community	07-29-2013
Url	http://alliedagencies.biz/questions/doc/doc/doc...	💀💀💀💀	PhishTank Source	04-12-2015
Address	122.151.223.203	💀💀💀💀	Common Community	12-05-2013
Url	http://www.completepc.pt/catalog/images/mail...	💀💀💀💀	PhishTank Source	04-12-2015
Url	http://unitedstatesreferral.com/santos/gucci201...	💀💀💀💀	PhishTank Source	04-12-2015
File	3B8BD0A0C6069F2D27D759340721B78FD289F92...	💀💀💀💀	Common Community	08-11-2014
Url	http://argumentall.com/funds/box/index.php	💀💀💀💀	PhishTank Source	04-09-2015
Url	http://cbsa-passaros.com.br/FORCA_PREMIADA...	💀💀💀💀	PhishTank Source	04-12-2015
Url	http://kuchijewelleryonlinestore.com/gmh/index...	💀💀💀💀	PhishTank Source	04-09-2015
Url	http://signin.ebay.com.715-385-964-980.715-38...	💀💀💀💀	PhishTank Source	05-05-2015

(1 of 13326)

10

1 2 3 4 5 6 7 8 9 10

Threats

INDICATORS ▾ ACTIVITY ▾ DOCUMENTS ▾ THREATS TAGS ADVERSARIES ▾ VICTIMS ▾ WORKFLOW ▾

Filter

Name	Owner	Date Added
SemParar Phishing	Common Community	05-01-2015
Carbanak APT	Common Community	02-16-2015
fin4	Common Community	02-09-2015
Asprox botnet	Common Community	12-09-2014
FIN4	Common Community	12-05-2014
Operation Cleaver	Common Community	12-02-2014
comRAT	Common Community	11-12-2014
The Darkhotel APT	Common Community	11-10-2014
Operation SMN (Axiom)	Common Community	10-31-2014
APT28	Common Community	10-28-2014

(1 of 4) 10 1 2 3 4 >

The Darkhotel APT

DETAILS PIVOT

Description:

The Darkhotel APT is a threat actor possessing a seemingly inconsistent and contradictory set of characteristics, some advanced and some fairly rudimentary. Inhospitably operating for almost a decade, the threat actor is currently active. The actor's offe

Type: Threat
Owner: Common Community
Added: 11-10-2014

Tags: apt Nemim Tapaoux Pioneer Karba APAC

Wednesday, May 6, 15

Threat Actor Overview

OVERVIEW **TASKS** **ACTIVITY** **ASSOCIATIONS** **SHARING**

 Common Community

Description:

finance010 / 0x4500 says:

- None

The Darkhotel APT is a threat actor possessing a seemingly inconsistent and contradictory set of characteristics, some advanced and some fairly rudimentary. In hospitably operating for almost a decade, the threat actor is currently active. The actor's offensive activity can be tied to specific hotel and business center Wi-Fi and physical connections, some of it is also tied to p2p/file sharing networks, and they have been known to spear-phish targets as well. Darkhotel tools are detected as 'Tapaoux', 'Pioneer', 'Karba', and 'Nemim', among other names.

The following list presents a set of characteristics for the crew:

- operational competence to compromise, mis-use, and maintain access to global scale, trusted commercial network resources with strategic precision for years
- advanced mathematical and crypto-analytical offensive capabilities, along with no regard for undermining the trust extended to the Certificate Authorities and the PKI
- indiscriminately infect systems with some regional clarity over trusted and untrusted resources to build and operate large botnets
- well-developed low level keyloggers within an effective and consistent toolset
- a focus throughout campaigns on specific victim categories and tagging them
- a larger, dynamic infrastructure built of apache webservers, dynamic dns records, crypto libraries, and php webapps
- regular 0-day access - recent deployment of an embedded Adobe Flash 0-day spear-phishing exploit, and infrequent deployment of other 0-day resources to sustain larger campaigns over several years

Details

Type: Threat

Added: 11-10-2014

Follow:

Security Labels

 Choose Security Labels 

TLP GREEN

Tags:



CHOOSE COMMON TAGS

APAC  apt  Karba 
Nemim  Pioneer 

Threat Actor Associations

Type	Summary	Rating	Owner	Action
File	FFA97EB4875129646376BC88E9FF99FFEFFF2C68BA3A06F6727D5F343FC7F6B51	💀💀💀💀	Common Community	Dissociate
File	2D1C383143C39CA05CECBF35004BF9085D1D742	💀💀💀💀	Common Community	Dissociate
Host	trade-inf.com	💀💀💀💀	Common Community	Dissociate
Host	ms-hotfix.com	💀💀💀💀	Common Community	Dissociate
Host	window-services.net	💀💀💀💀	Common Community	Dissociate
Host	ms-updates.com	💀💀💀💀	Common Community	Dissociate
Host	www.news-updates.org	💀💀	Common Community	Dissociate
Host	msdn4-updates.com	💀💀💀💀	Common Community	Dissociate
Host	www.universal-online.com	💀💀💀💀	Common Community	Dissociate
Host	office-revision.com	💀💀💀💀	Common Community	Dissociate

(1 of 61)

10 | ← 1 2 3 4 5 6 7 8 9 10 →

What are some open sources of this data?

“APTnotes” reports:

<https://github.com/kbandla/APTnotes>

ShadowServer:

<https://www.shadowserver.org/>

REN-ISAC’s Collective Intelligence Framework

<http://csirtgadgets.org/>

#CIF on FreeNode

Vocabulary for Event Recording and Incident Sharing

<http://veriscommunity.net>

What do you do with all this data?

Integrate ThreatConnect with Splunk

<https://splunkbase.splunk.com/app/1893/>

Block known hostiles at the system level:

Host Based Firewalls

Email Filtering

IDS Alerts

Discover hashes with HIDS (Tripwire, OSSEC, et al.)

Bro-IDS

Let Palo Alto Networks do it for you

APT Detection with Wildfire:
Sandbox threats and automatic signature generation!

End point protection with Traps:
Kills 27 exploit techniques

High confidence IoCs automatically blocked

Thank you! Questions??

Upcoming events

BSidesMSP Unconference

Tue May 12 @ 11a-3p
Eagle Street Grill, St Paul

CryptoParty MN
Sat May 9 @ 1300
Hack Factory



Security B-Sides MSP 2015 Sat & Sun **June 13-14**
Theme “Threat Intelligence” - RSVP at BSidesMSP.org
Target Commons, Downtown Minneapolis

This presentation can be found at
<http://github.com/itriskltd>