



Understanding the Data Breaches of 2014: Did it have to be this way?

Josef Meier

Manager Pre Sales Engineering Fortinet Germany

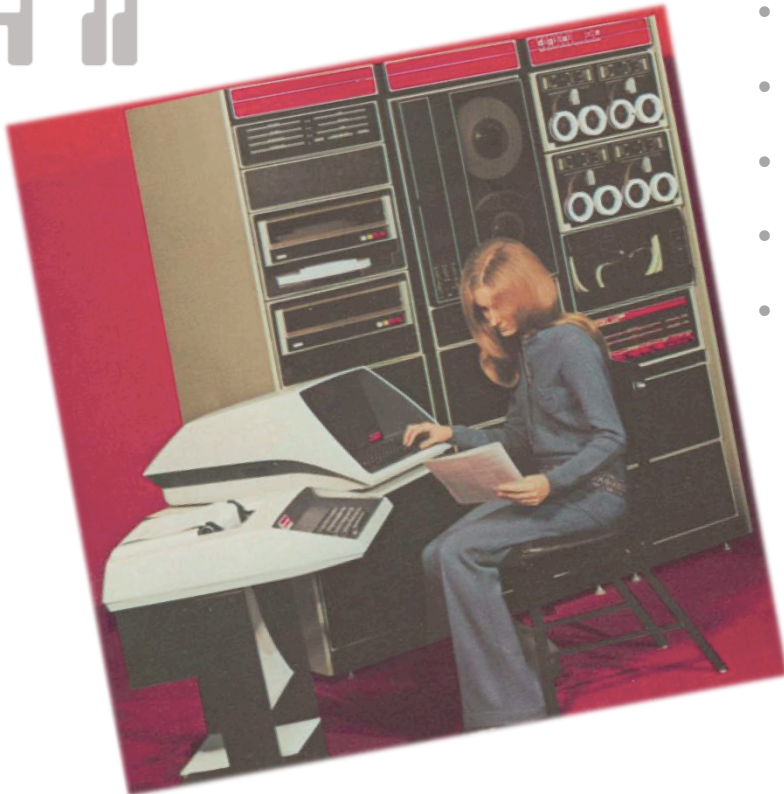
The year?



IM THE CREEPER, CATCH ME IF YOU CAN!

The Creeper – “Catch me if you can”...

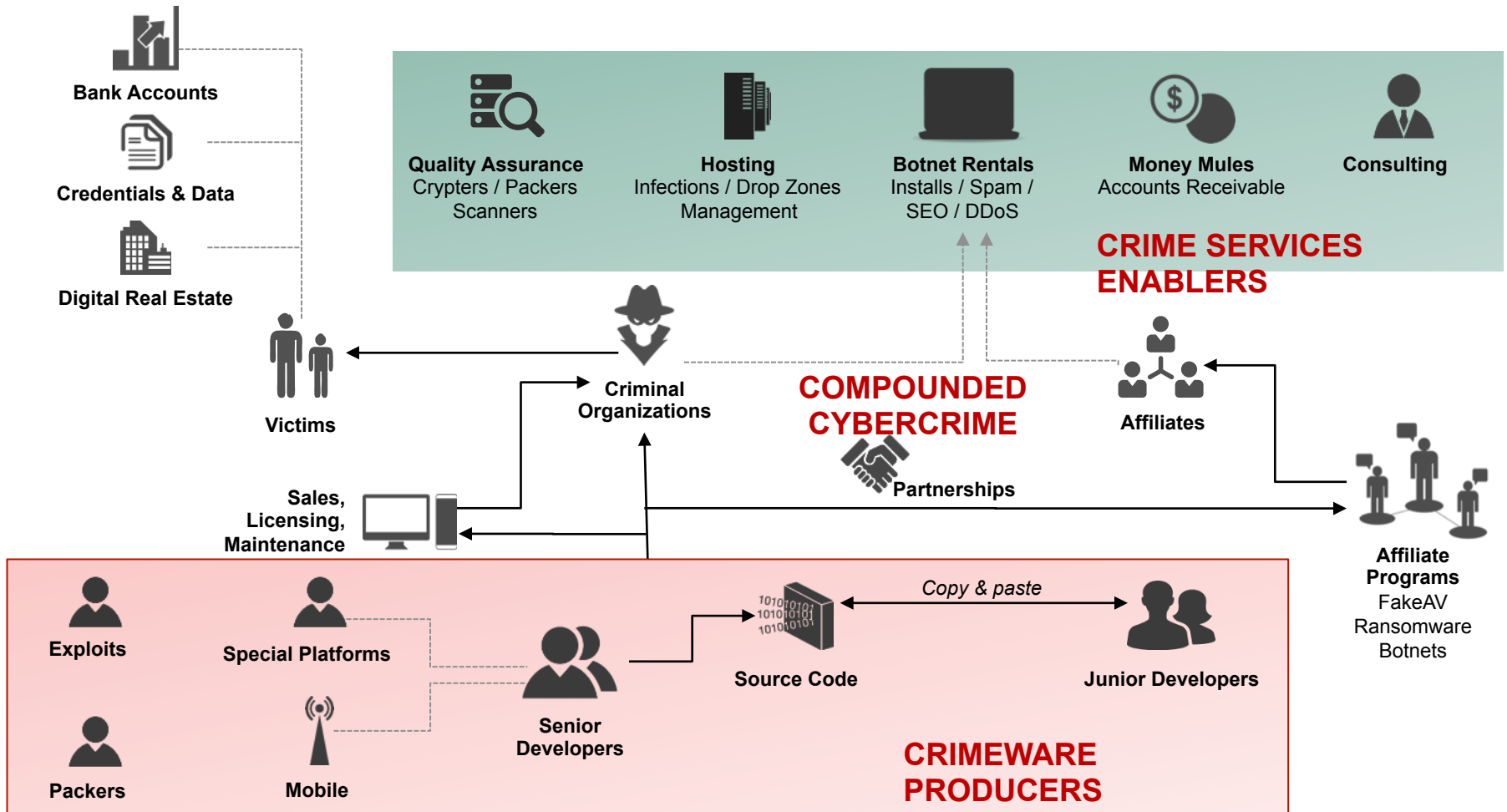
1971



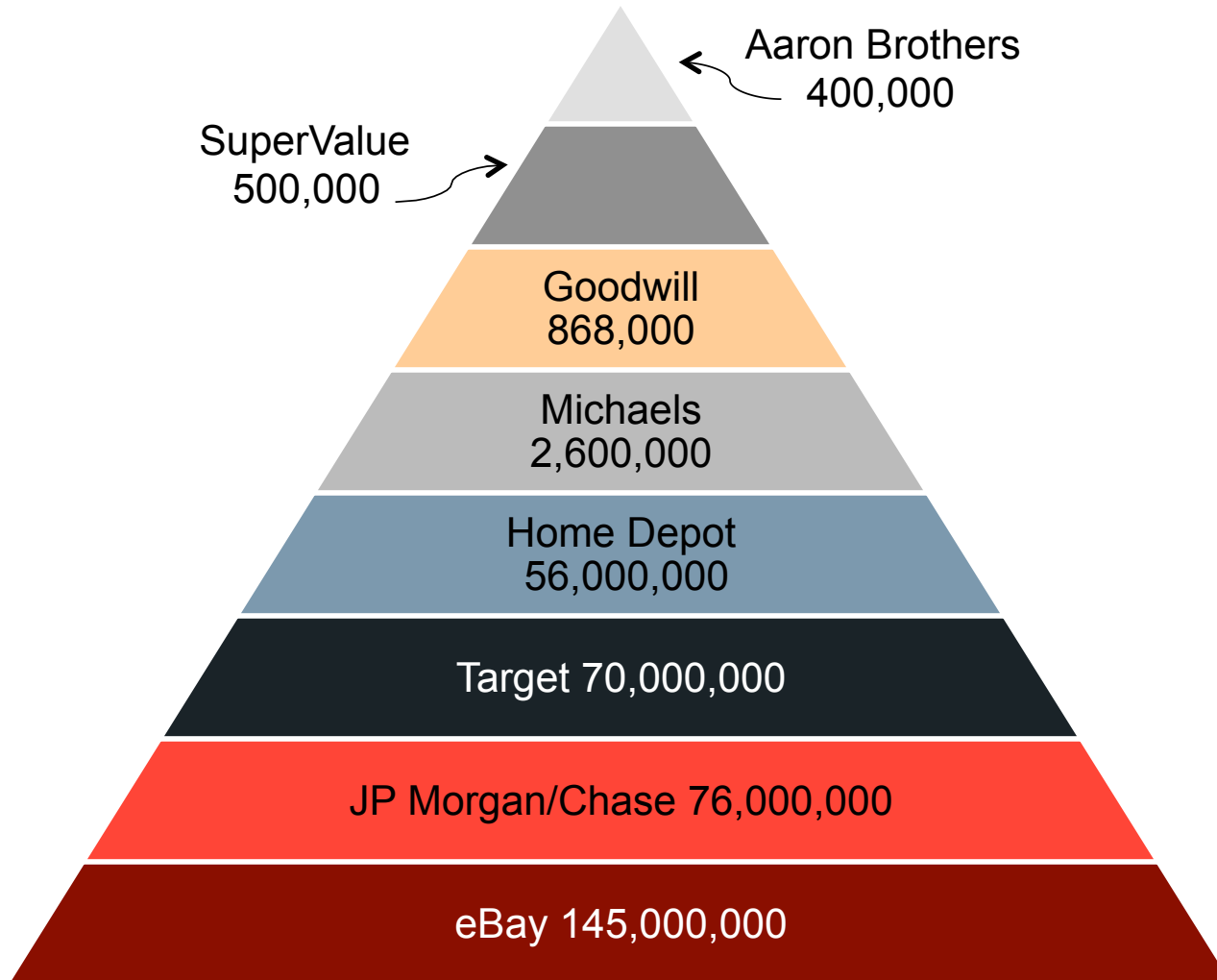
- Experimental self-replicating program
- Written in 1971 by Bob Thomas of BBN
- Infected DEC PDP-10 computers
- Just one year after unix epoch began
- ‘Reaper’ worm created in 1972 to delete it



Crimeware and Crime Services



Anyone Want To Add Anything?



*Milton Security

Point of Sale

- 2013 was the “year of the megabreach”
- Target and Home Depot made the headlines
- Between them details of 90 million credit cards stolen
- POS attacks still very prevalent
small targets, large scale
- PCI 3.0 released in 2013 to reinforce protection

Price List :
Usa ccv : 3\$
Usa ccv : 3\$
Usa ccv : 6\$
Usa ccv : 6\$
Usa ccv With D.o.B : 12\$
Usa ccv Fullz : 25\$
Usa ccv With Full Infos : 30\$

Uk ccv : 5\$
Uk ccv : 5\$
Uk ccv : 8\$
Uk ccv With D.o.B : 15\$
Uk ccv Fullz : 25\$
Uk ccv With Full Info : 35\$

Germany ccv : 10\$
Germany ccv : 10\$
Germany ccv With D.o.B : 15\$
Germany ccv Fullz 30\$
Germany ccv With Full Info : 40\$

Italy ccv : 10\$
Italy ccv : 10\$
Italy Ccv With D.o.B : 15\$
Italy ccv Fullz : 25\$
Italy ccv With Full Info : 30\$

TRACK 1 & 2

US types :

- USA	Classic/Standart	\$ 30
- USA	Gold/Premier/Platinum	\$ 35
- USA	Business/Corporate/Purchasing	\$ 40
- USA	All Types	\$ 30
- USA	USA	\$ 30
- USA	USA	\$ 20

UK types:

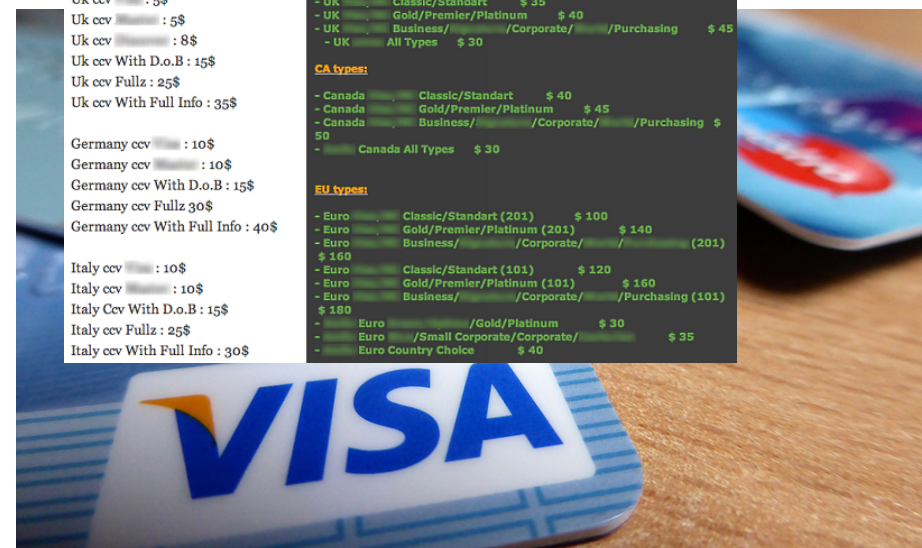
- UK	Classic/Standart	\$ 35
- UK	Gold/Premier/Platinum	\$ 40
- UK	Business/Corporate/Purchasing	\$ 45
- UK	All Types	\$ 30

CA types:

- Canada	Classic/Standart	\$ 40
- Canada	Gold/Premier/Platinum	\$ 45
- Canada	Business/Corporate/Purchasing	\$ 50
- Canada	All Types	\$ 30

EU types:

- Euro	Classic/Standart (201)	\$ 100
- Euro	Gold/Premier/Platinum (201)	\$ 140
- Euro	Business/Corporate/Purchasing (201)	\$ 160
- Euro	Classic/Standart (101)	\$ 120
- Euro	Gold/Premier/Platinum (101)	\$ 160
- Euro	Business/Corporate/Purchasing (101)	\$ 180
- Euro	/Gold/Platinum	\$ 30
- Euro	/Small Corporate/Corporate/	\$ 35
- Euro	Country Choice	\$ 40



Finding the Common Thread



Target - Outside contractor clicks on phishing email

<http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data#p2>
<http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>

Home Depot Stolen login credentials from Third party vendor

<http://krebsonsecurity.com/2014/11/home-depot-hackers-stole-53m-email-addresses/>
<http://www.eweek.com/security/home-depot-breach-expands-privilege-escalation-flaw-to-blame.html>

JP Morgan/Chase – Stolen employee credentials

<http://www.computerworld.com/article/2862578/twofactor-authentication-oversight-led-to-jpmorgan-breach-investigators-reportedly-found.html>



- Havex – the sequel to Stuxnet
- RAT (remote administration tool)
- Harvests information on hardware control systems (SCADA)

- OPC – OLE for Process Control
- Communication between Windows and control hardware
- OPC servers control machines via PLC

Stuxnet-like 'Havex' Malware Strikes European SCADA Systems

Thursday, June 26, 2014 Swati Khandelwal

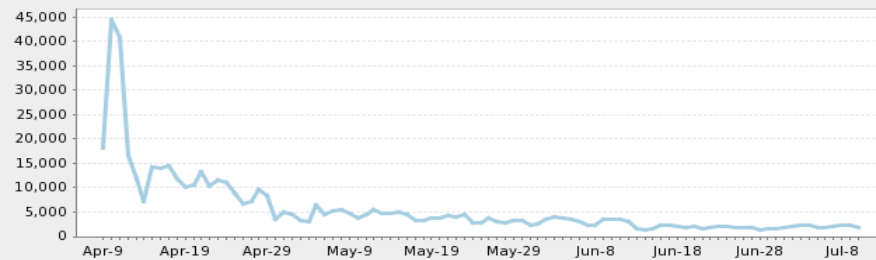
[G+](#) 114 [Like](#) 1.2k [Share](#) 705 [Tweet](#) 463 [Share](#) 112 [ShareThis](#) 2646



Server-side Attacks

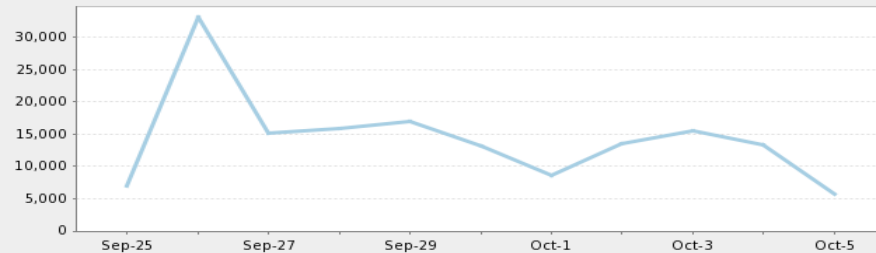


HeartBleed



500,000 Web Servers Affected

ShellShock



— Devices

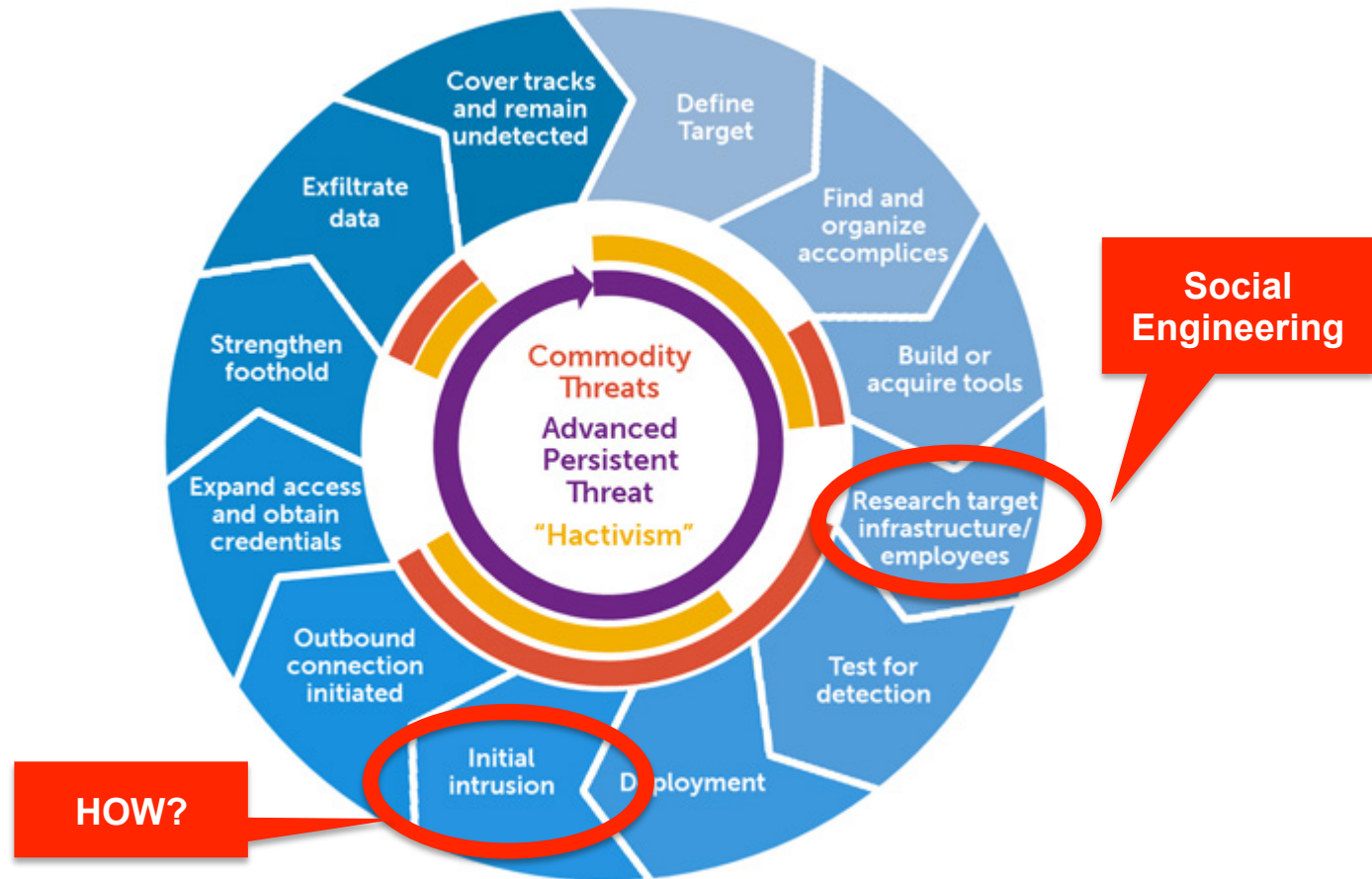
Time to Protect Critical
Surge in attacks while fresh

Millions of Internet Connected Devices Affected



Shellshock

Advanced Persistent Threat Structure



*Wikipedia Commons

Exploiting the Weak Link



The Technology Side of Things

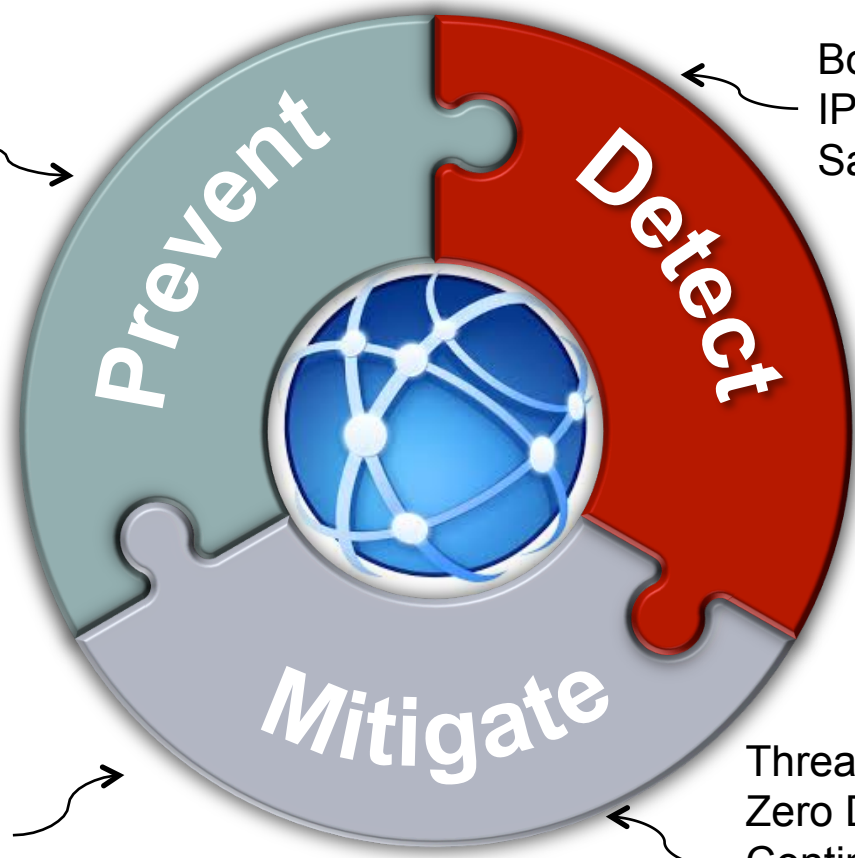


Two Factor Authentication
Anti-Virus
Intrusion Prevention
Secure Email Gateway
Web Application Firewall
End Point Protection

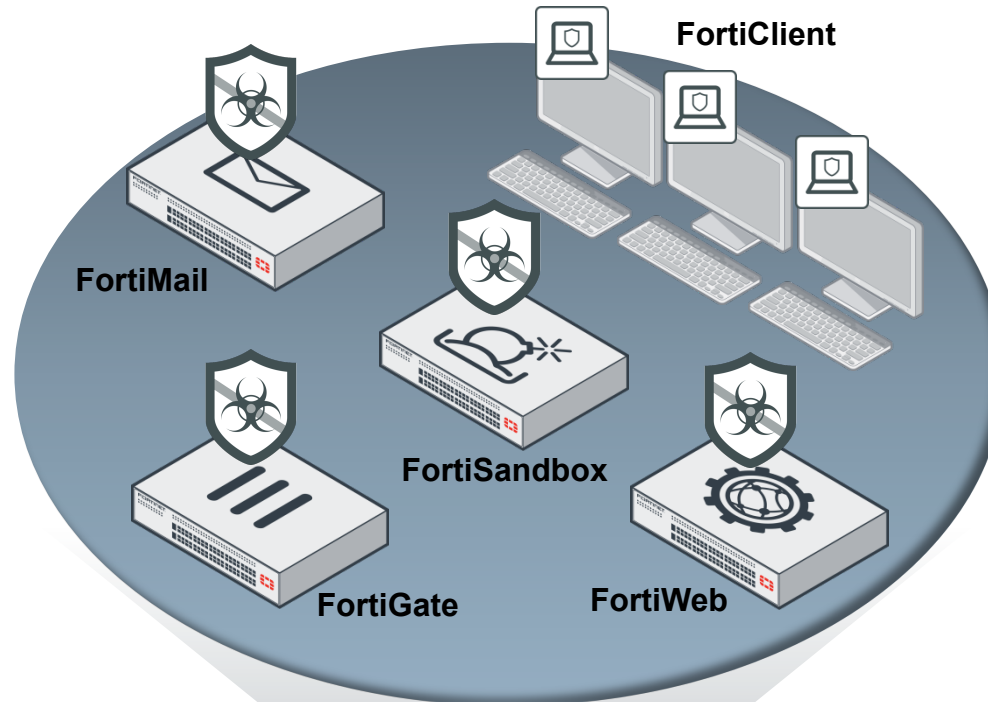
Botnet Detection
IP & Client Reputation
Sandboxing

People
Process
Technology

Threat Intelligence
Zero Day Research
Continuous updates



Advanced Threat Protection



FortiGuard Lab
FortiGuard Services



The FortiGuard Minute

THE FORTIGUARD MINUTE

25,000

Spam e-mails intercepted

390,000

Network intrusion attempts resisted

83,000

Malware programs neutralized

5,800

Application control rules

100

Intrusion prevention rules

170 Terabytes

of threat samples

160,000

Attempts to access malicious websites blocked

59,000

Botnet command and control attempts thwarted

2 Million

New and updated antivirus definitions

17,500

Intrusion prevention rules

39 Million

Website categorization requests

8,000

Hours of research in labs around the globe

250 Million

rated websites in 78 categories

47 Million

New and updated antispam rules

173

Zero-Days discovered

1.3 Million

New URL ratings

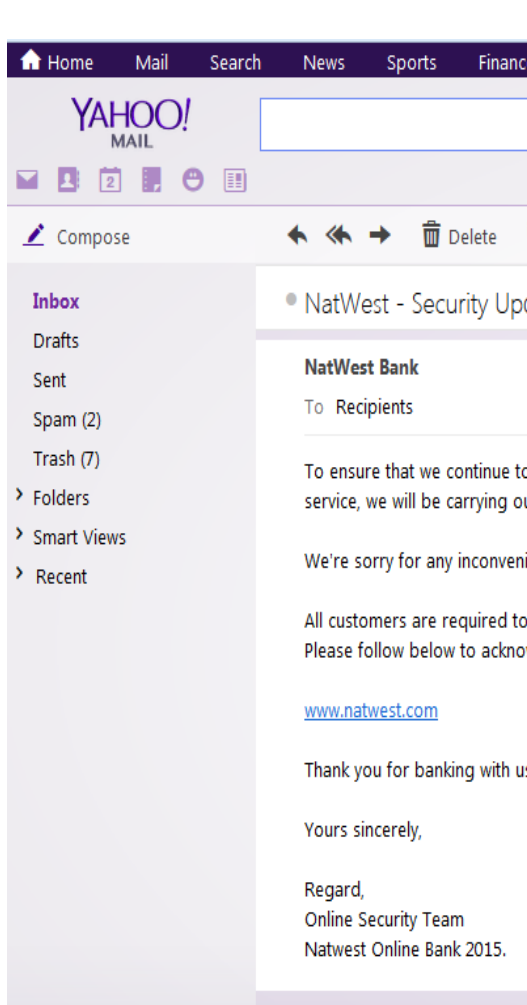
FORTIGUARD DATABASE



UPDATES PER WEEK



So What Do We Do With Dave?



Date: Thu, 15 Jan 2015 15:07:19 +0100
From: "Internal Revenue Service" <complaints@irs.gov>
To: <rpastore@cxo.com>
Subject: Complaint against your company

Dear business owner,

A criminal complaint has been filed against your company.

Your company is being accused of trying to commit tax evasion schemes.

The full text of the complaint file (PDF type) can be viewed on the IRS website, by visiting the following link :

http://www.irs.gov/complaints/view_complaint.aspx?complaint_id=931998&hash=329yt8dhui8g14

An official response from your part is required, in order to take further action.

Please review the charges brought forward in the complaint file, and contact us as soon as possible by :

Telephone Assistance for Businesses:

Toll-Free, 1-800-829-4933

Email: complaints@irs.gov

Thank you,

Internal Revenue Service

Fraud Prevention Department

Training To Raise Awareness



<http://krebsonsecurity.com/2012/01/phishing-your-employees-101/>

- Policy
- Procedure
- Process



And At the Opposite End of the Spectrum...

AdultFriendFinder Hookup, Find Sex or Meet Someone Hot Now
Username Password [Login](#)
[Forgotten password?](#)

[Join Now](#) [Home](#) [Browse](#) [Hookup](#) [Dating Forums](#) [Live Chat](#)

For more information on the security incident please go to <http://afn.com/security-updates>

The Hottest
Dating, Hookup & Community

Waiting for adultfriendfinder.com...

Members Login ▾

ASHLEY MADISON®

Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select

[See Your Matches »](#)

Over **37,610,000** anonymous members!



As seen on: Hannity, Howard Stern, TIME, BusinessWeek, Sports Illustrated, Maxim, USA Today

Ashley Madison is the world's leading married dating service for **discreet** encounters



SSL Secure Site



- ✓ **Technology is only part of the solution**
- ✓ **Single vendor solutions may provide an advantage**
 - ✓ **But only if elements actually work together**
- ✓ **Remember your network extends beyond you**
 - ✓ **Remote employees, third party suppliers and contractors**
- ✓ **Your employees are the first line of defense**
 - ✓ **Equip and use them**
- ✓ **Never assume**
 - ✓ **You're fully protected**
 - ✓ **The network hasn't already been breached**



Understanding the Data Breaches of 2014: Did it have to be this way?

Vielen Dank!