Emerging Cybersecurity Threats and Challenges

Ole Kjeldsen
National Technology & Security Officer
Microsoft Denmark

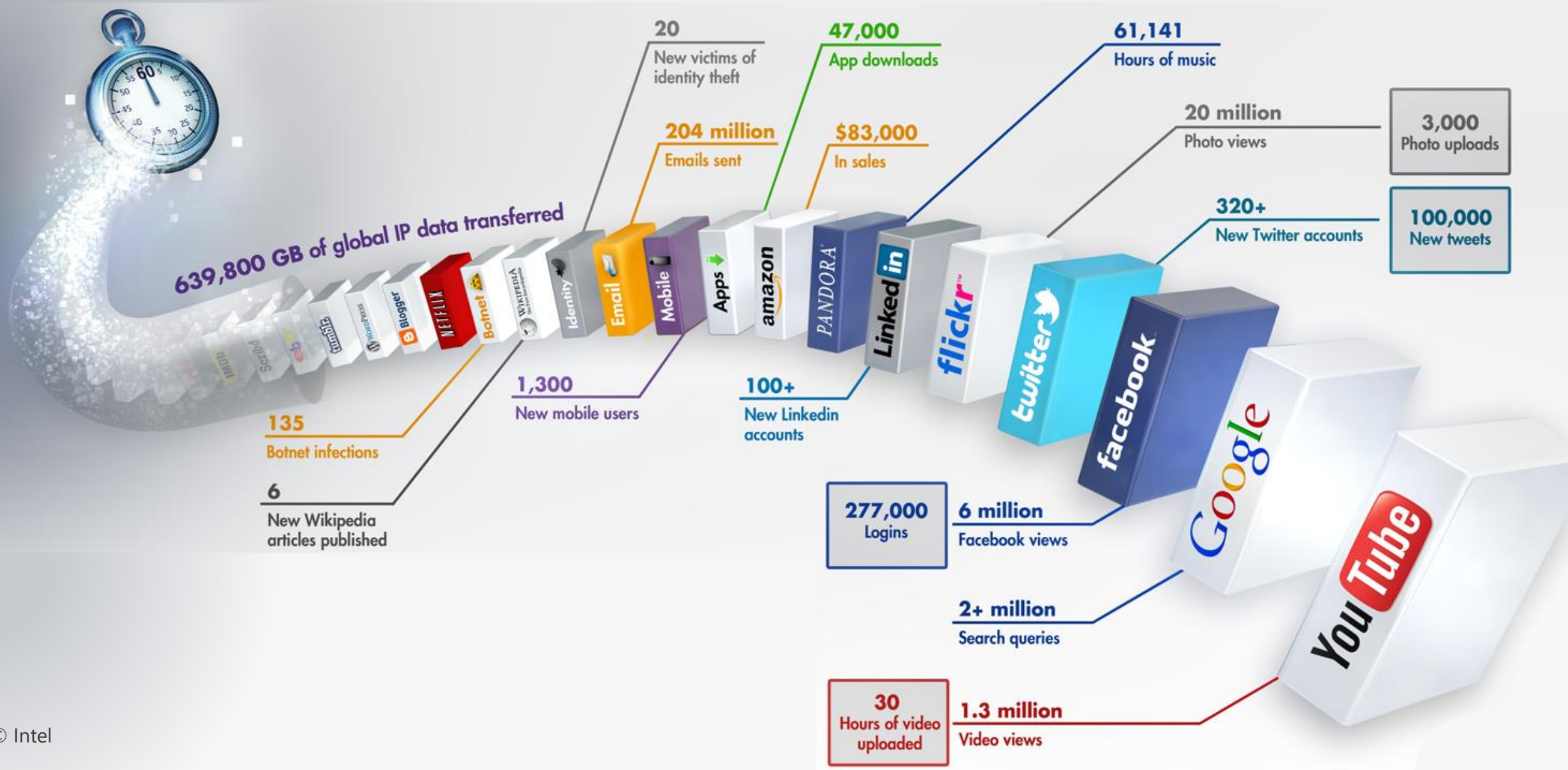
Microsoft

AGENDA

- A balanced approach
- The concept and dimensions of data
- How Microsoft approach cybersecurity
- Specifically how we approach cyber crime

- Q&A

1 minut online – in 2013



MILLENNIALS

ALWAYS MOBILE

ALMOST ALWAYS ONLINE

OFTEN IN THE PROCESS OF SHARING (EVERYTHING?)

Mega Trends – for everyone

70% af CIOs ser mobile som den mest disruptive teknologi de næste 10år

2014, var 1/2 af al ny applikations-udvikling med en mobil form factor som mål

Social networking vil følge ikke blot mennesker, men også husholdningsenheder devices og andre produkter

57% af enterprises havde investeret i enterprise social i 2014

>70% af CIOs vil adoptere en cloud-first strategi i 2016

54% af organisationer øgede public cloud forbrug i 2013

Forbrug på Big Data:

$10 milliarder 2013 > $20 milliarder 2016

Procent af det digitale univers tagged:

3% (idag)

33% (2020)

Totalt digitalt indhold vil gro

800% Fra 2012 = 8 zettabytes i 2015

"WE LIVE IN A MOBILE FIRST & CLOUD FIRST WORLD!"

SATYA NADELLA
[CEO, MICROSOFT - 2015]

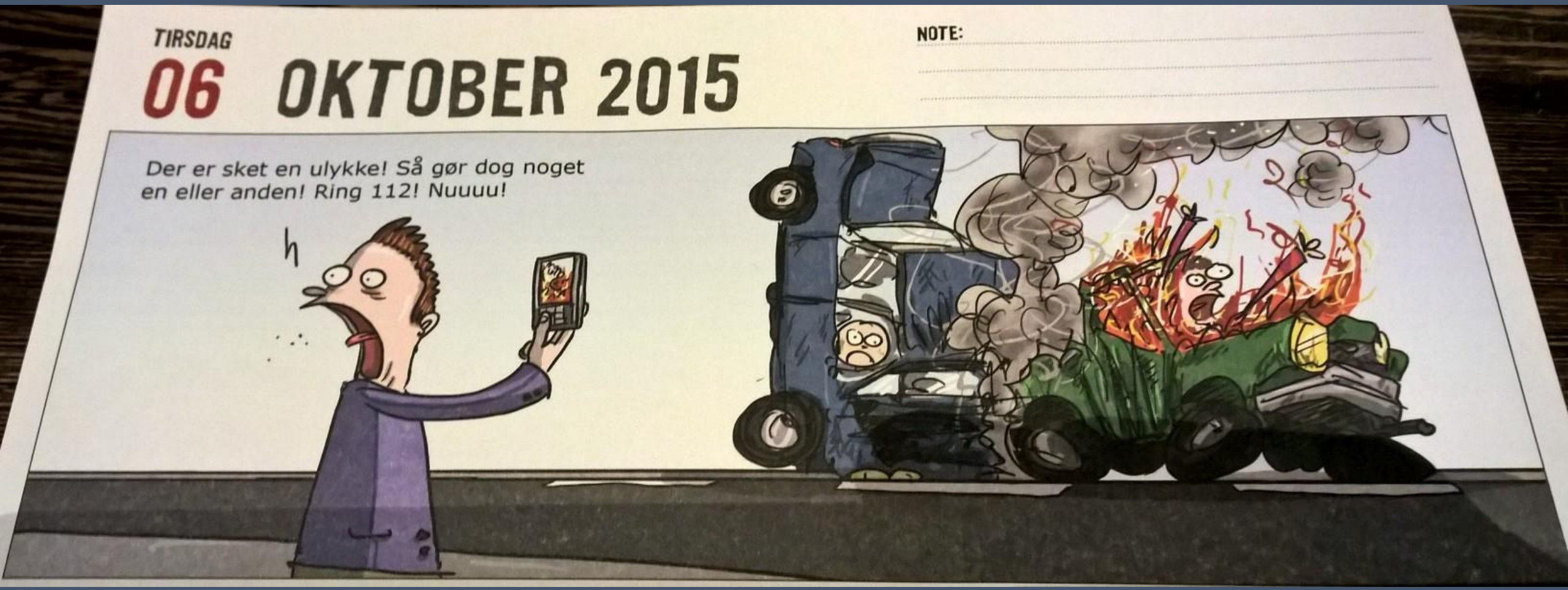
2013

2003

TIRSDAG

06 OKTOBER 2015

NOTE:



Every second,
12 people are victims of cybercrime:
400 million every year.*

50% of online adults have
been victims in the past year.

1 in 5
Small and medium enterprises
are targeted by cyber criminals.**

Cybercrime costs businesses
$450 billion a year.***

Financial Fraud
53% of the world's securities
exchanges were targeted in 2012.

Online Child Exploitation
The NCMEC has reviewed more than
90M images and videos
of child pornography.****

* *2013 Norton Report*
** *National Cyber Security Alliance*
*** *2014 McAfee / Center for Strategic & International Studies study*
**** *National Center for Missing and Exploited Children*

Cybercrime
What's at stake?

Organizations Lose
their customers and intellectual property, & damage their brand

Senior Executives Lose
their jobs

Individuals Lose
their privacy & money

* *2013 Norton Report*
** *National Cyber Security Alliance*
*** *2014 McAfee / Center for Strategic & International Studies study*
**** *National Center for Missing and Exploited Children*

Toxic environment

It-sikkerhed i statens centralnervesystem får hug

07.10.15 INFRASTRUKTUR Ritzau

En række helt centrale statsinstitutioner får kritik af Rigsrevisionen, når det kommer til it-sikkerhed.

Skat har sy

09.09.15 LEDEL

Tidligere skyld
kammeradvoka

Kommuner sløser med datasikkerhed om pas

21.08.15 INFRASTRUKTUR Ritzau

Borgeres
forkerte h

oplysninger fra

Datatil
kundec

18.08.15

DSB skal
oplysninger til andre kunder.

Ministe
med pe

13.08.15

Ifølge DSI
at personoplysninger, de har givet t
bygningsministeren er stærkt bekyr

Politiker hacket og snydt for 200.000 kroner

25.02.15 INFRASTRUKTUR Ritzau

Lokalpolitikeren Peter Hansen fra Sønderborg var for nylig udsat for et større hackerangreb i en af sine virksomheder. Han kalder angrebet dybt udspekuleret og har fortalt sin historie til DR Syd.

Hacker-angre

04.02.15 POLITIK

En vedhæftet fil i
række servere for
på serverne. Inger
virker stadig.

Hackerangreb mod kommune

20.01.15 INFRASTRUKTUR 1 Gribskov Kommune

Hackere er brudt ind i en del af Gribskov Kommunes it, og har omdøbt filer på kommunen computerdrev. Sagen er politianmeldt.

Dårlig datasikkerhed skal koste millionbøde

07.01.15 POLITIK Ritzau

Politikerne i EU-Parlamentet har valgt at hæve strafferammen til et langt højere niveau end i Danmark.

THERE IS NO WAY WE COULD IMPLEMENT AND MAINTAIN THE SAME LEVEL OF SECURITY AS WE GET FROM THOUGHTFULLY USING CLOUD COMPUTING

CISO of major Danish Manufactoring Company

Data …

Integrity

HOPE
IS NOT A STRATEGY.

attributed the American football coach Vince Lombardi.

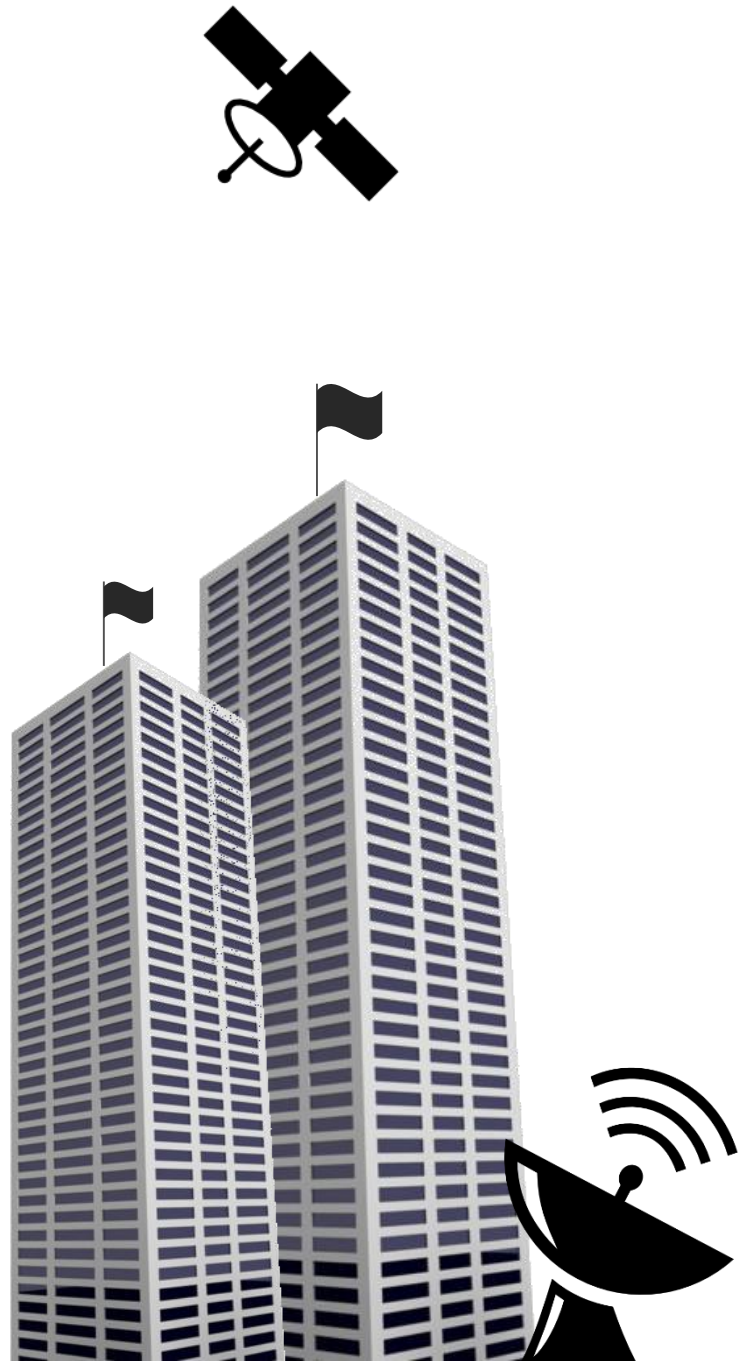

You have many of the best security solutions…


...but the security landscape has changed.

TODAY, CUSTOMERS ARE EXPERIENCING A

REVOLUTION

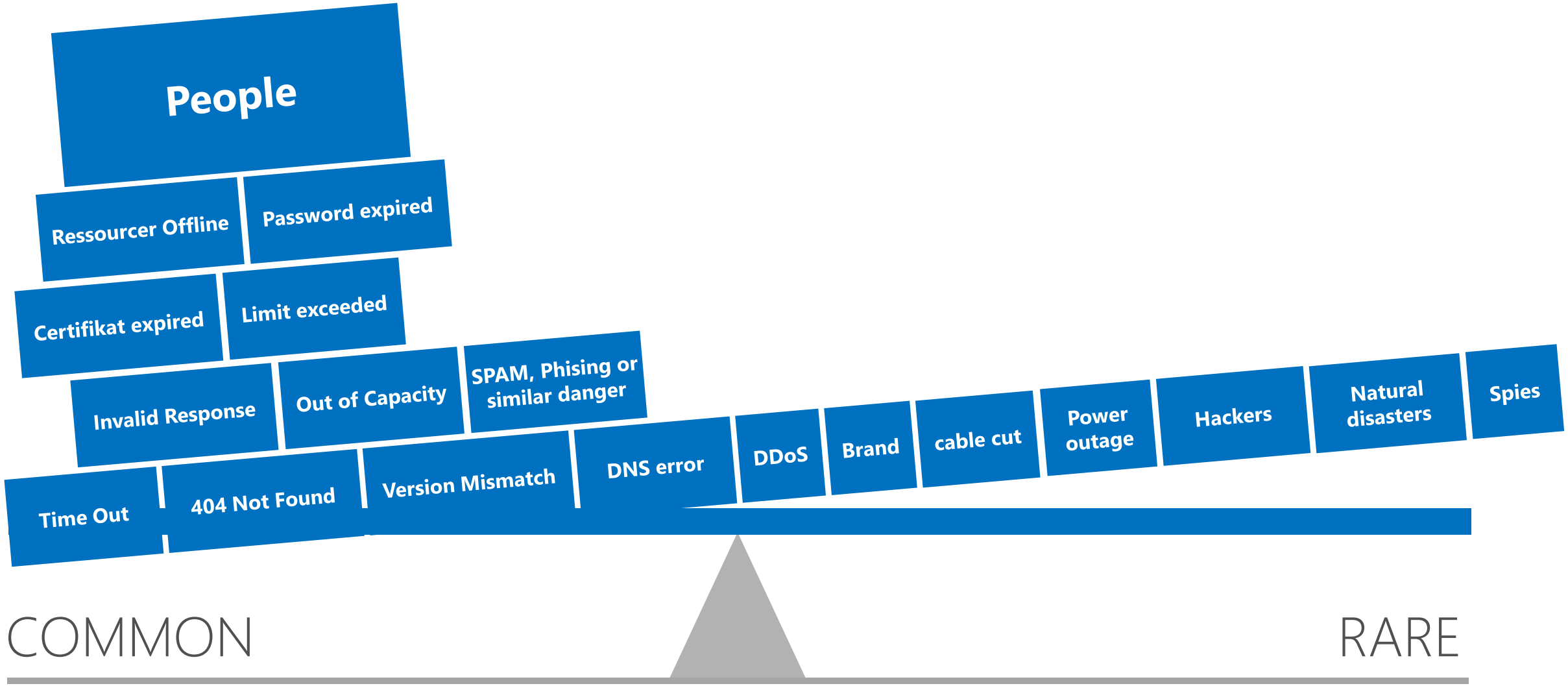
OF **CYBER-THREATS**



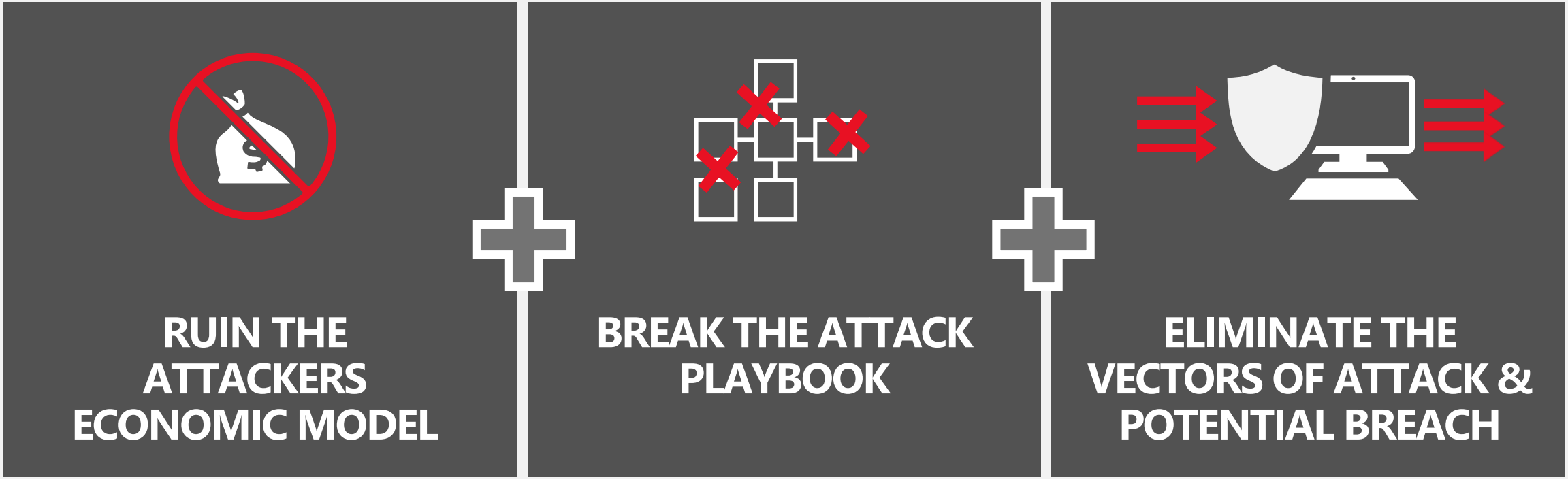
FEAR
IS A BAD ADVISOR.

Unknown origin ...

Risk based approach to data security breaches



ADDRESSING THE THREATS REQUIRES A NEW APPROACH:



Security from the inside out – beyond bigger walls

PROTECT CUSTOMERS FROM MODERN SECURITY THREATS

Microsoft Cybercrime Center

Big data

Investigations

Legal action

DCU Botnet Takedowns and Malware Disruptions

Conficker

February 2010

Microsoft-lead model of industry-wide efforts to counter the threat

Botnet Worm sending SPAM and attempting to steal confidential data and passwords

b49 Waledac

February 2010

First MS takedown operation, proving the model of industry-led efforts

Disconnected70,000-90,000 infected devices from the botnet

Botnet Worm sending SPAM (1,5B)

b107 Rustock

March 2011

Supported by stakeholders across industry sectors

Involved US and Dutch law enforcement, and CN-CERT

SPAM, in average 192 spam messages per compromised machine per minute

b79 Kelihos

September 2011

Partnership between Microsoft and security software vendors

First operation with named defendant

SPAM, Bitcoin Mining, Distributed Denial of Service Attacks

b71 Zeus

March 2012

Cross-sector partnership with financial services

Focused on disruption because of technical complexity

Identity Theft / Financial Fraud

b70 Nitol

September 2012

Nitol was introduced in the supply chain relied on by Chinese consumers

Settled with operator of malicious domain

Malware Spreading, Distributed Denial of Service Attacks

b58 Bamital

February 2013

Bamital hijacked people's search results, took victims to dangerous sites

Takedown in collaboration with Symantec, proactive notification and cleanup process

Advertising Click Fraud

b54 Citadel

June 2013

Citadel committed online financial fraud responsible for more than $500Min losses

Coordinated disruption with public-private sector

Identity Theft / Financial Fraud

b68 ZeroAccess

December 2013

ZeroAccess hijacked search results, taking victims to dangerous sites

It cost online advertisers upwards of $2.7 million each month

Advertising Click Fraud

b157 Game over Zeus

June 2014

GameoverZeus (GOZ) was a banking Trojan

Worked in partnership with LE providing Technical Remediation

Identity Theft / Financial Fraud

b106 Bladabindi & Jenxcus

June 2014

Malware using Dynamic DNS for command. It involved password and identity theft, webcam, etc.

Over 200 different types of malware impacted.

Identity Theft / Financial Fraud / Privacy Invasion

b93 Caphaw

July 2014

Caphaw was focused on online financial fraud responsible for more than $250M in losses

Coordinated disruption with public-private sector

Identity Theft / Financial Fraud

b75 Ramnit

February 2015

Module-based malware, stealing credential information from banking websites. Configured to hide itself.

Credential Information Theft/Disable Security Defenses

b46 Simda

April 2015

Theft of personal details, including banking passwords, as well as to install and spread other malicious malware.

Theft personal data/Install and spread other malware





Protecting vulnerable populations

Online child protection | Elder fraud





Microsoft PhotoDNA

- **Creates signatures** of the worst known child abuse images
- **Can locate** these images among the millions online
- **Shared with** law enforcement and licensed to over 50 organizations around the world for free
- **Industry standard** – used by Facebook, Twitter, Google

Outlook.com bing OneDrive

Technical support scams

How the scam works

- Fraudsters pose as technical support from Microsoft or another reputable tech company
- Scams reach customers either by the cybercriminals calling victims, or by search engine ads directing customers to the fraudsters' websites
- Victims give access to their PCs, pay for the fake service, and are harmed by the cybercriminals' malware and identity theft

In US alone 3.3 million people become victims every year, losses over $1.5 billion

PRIVACY
IS BECOMING A LUXURY.

Maciej Ceglowski, Pinboard founder & WEB Privacy advocate

"Many of our customers have serious concerns about government surveillance of the Internet. We share their concerns. That's why we are taking steps to ensure governments use legal process rather than technological brute force to access customer data."

Brad Smith
General Counsel, EVP Legal and Corporate Affairs
Microsoft

UNITED STATES DISTRICT COURT

for the
Southern District of New York

13 MAG 2814

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Microsoft Corporation

Case No.

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the WESTERN District of WASHINGTON
(identify the person or describe the property to be searched and give its location):
The PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Microsoft Corporation (see attachments).

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:
See attachments.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before December 18, 2013
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Microsoft fights warrant for customer emails stored overseas

By James O'Toole @jtotoole June 11, 2014: 2:41 PM ET

PHOTO: MIKE FUENTES/BLOOMBERG VIA GETTY

Allowing the warrant to move forward, Microsoft argues, "would violate international law and treaties, and reduce the privacy protection of everyone on the planet."

NEW YORK (CNNMoney)

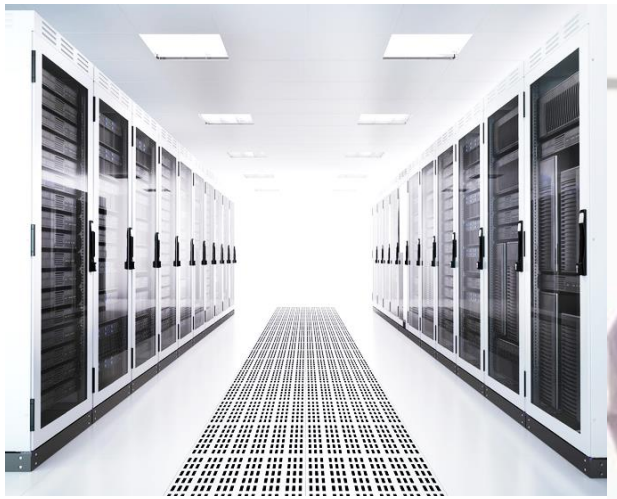
Microsoft is fighting a government search warrant seeking customer emails stored abroad in a case that could have far-reaching implications for how tech companies deal with law

"… users are going to embrace technology ***only*** if they can trust it."

– Satya Nadella; Microsoft CEO

Microsoft guiding principles

Non-negotiable foundation for our business



Cyber security

- State of the art security technology, procedures and controls
- Strongest possible encryption
- Red teaming & Digital Crimes Unit
- Geo-location offerings
- All about securing availability & integrity

Data Privacy

- Privacy by design
- Simple acces to Privacy policy
- No commercial use of customer data or metadate
- Confidentiality can only be suspended with law in hand!

Compliance

- ALWAYS be at the forefront of implementing newest and strictest international and regional standards .. Eg ISO27018
- 'skin in the game' legally, financially and through our contracts

Transparency

- Open source our model
- Publish rules and frameworks that govern our collaboration with authorities
- Law Enforcement Request Reports
- Challenge mis-use of authority
- Highlight need for legal action

Microsoft Security & Privacy efforts

Global scale

Microsoft Digital Crimes Unit help stressing cyber criminals

We develop tools assisting in countering organized crime, human trafficing, pedophelia groups and cyber crime in general

24x7

Constant developing and expanding our use of encryption, processes etc. to counter new emerging threaths

Renewed focus on PhoneScams (in UK and Denmark in EU)

Prof & Consum cust.

25y+ experience running global intensive cloud services & 35y+ building sw

Professionel customers help make us sharper every day benefitting private users

Principled Approach

ALWAYS up to par and often beyond the newest standards and highest legal bars on data security & compliance

AND we challange authorities where appropriate!

X platform

It is a new world & a new Microsoft – we are present on every platform ☺

summary

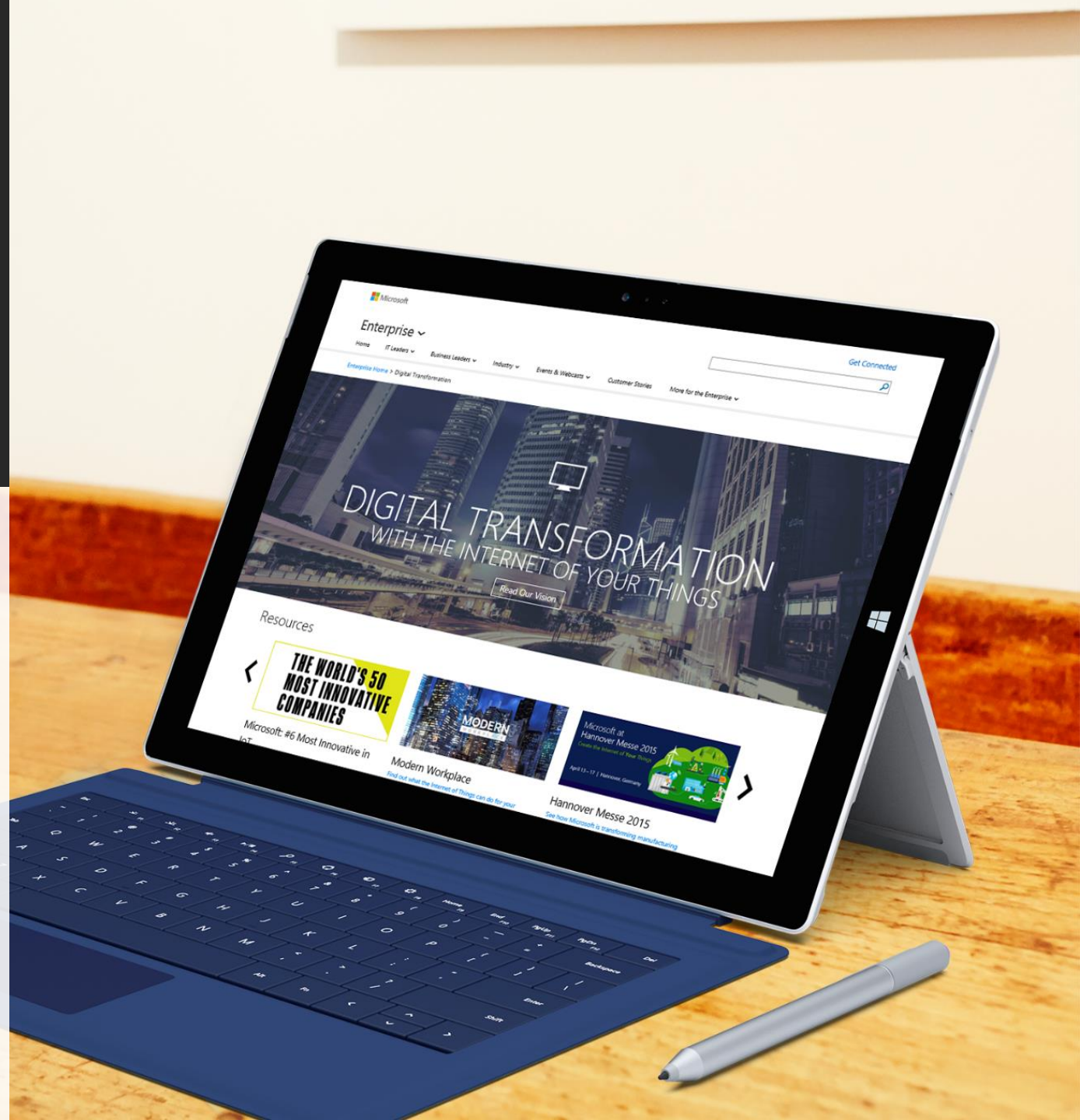
http://www.microsoft.com/security/cybersecurity

Microsoft

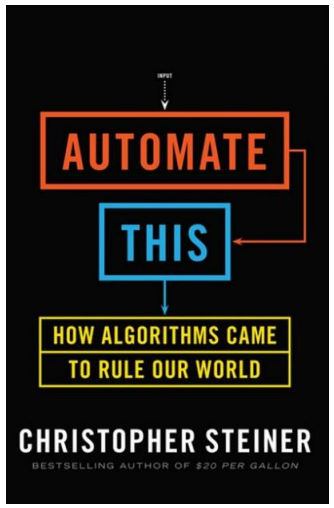
Thank You!

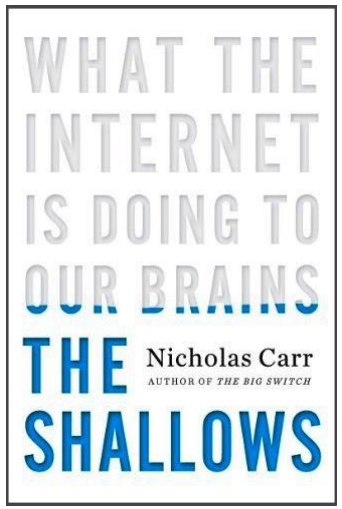
Microsoft

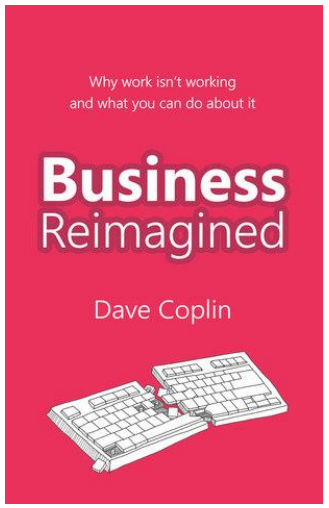
olek@microsoft.com
@olekATlive

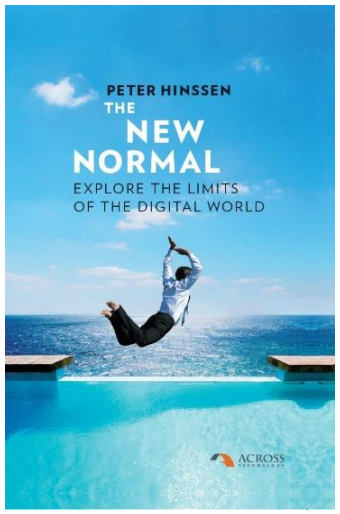


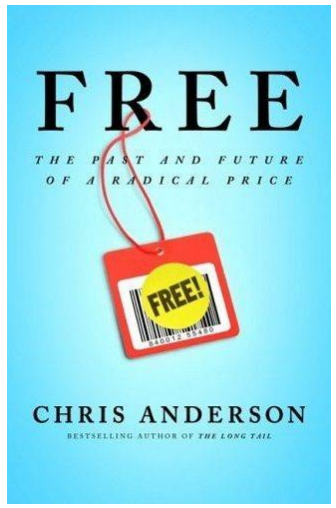
Book recommendations

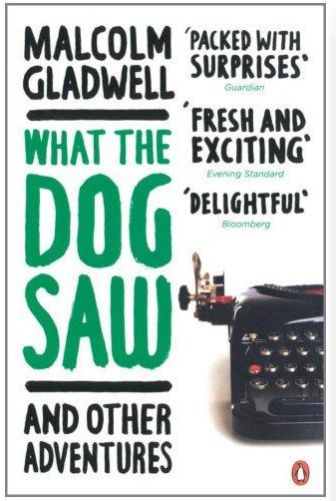


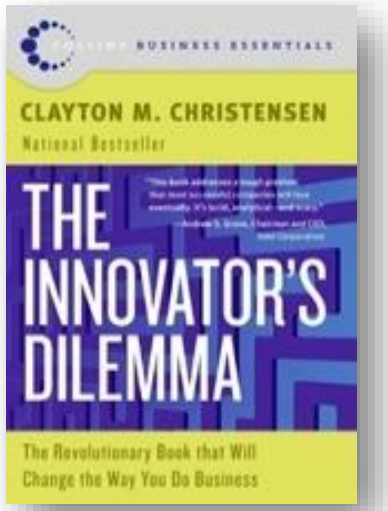












- Lucas, Robert E., Jr. (2002). Lectures on Economic Growth. Cambridge: Harvard University Press. pp. 109–10.
- Maddison, Angus (2003). The World Economy: Historical Statistics. Paris: Development Centre, OECD. pp. 256–62, Tables 8a and 8c.
- Malcolm Gladwell, "What The Dog Saw", 2009
- Clayton Christensen, "The Innovators Dilemma"
- Chris Anderson, "Free"
- Nicholas Carr, "The Shallows"
- Peter Hinssen "The New Normal", 2010
- Christopher Steiner "Automate this: How Algorithms came to rule our world"
- Cave Coplin, "Business Reimagined" 2013 (free dwnl: http://bit.ly/15JTTl4)
- Machine Learning on Azure, MS Press free dwnl: http://www.microsoftvirtualacademy.com/ebooks

Data protection

Microsoft Cloud provides customers with strong data protections – both by default and as customer options

Data isolation

Logical isolation segregates each customer's data from that of others is enabled by default.

At-rest data protection

Customers can implement a range of encryption options for virtual machines and storage.

In-transit data protection

Industry-standard protocols encrypt data in transit to/from outside components, as well as data in transit internally by default.

Encryption

Data encryption in storage or in transit can be deployed by the customer to align with best practices for ensuring confidentiality and integrity of data.

Data redundancy

Customers have multiple options for replicating data, including number of copies and number and location of replication data centers.

Data destruction

Strict standards for overwriting storage resources before reuse and the physical destruction of decommissioned hardware are by default.

THE COURT (GRAND CHAMBER) HEREBY RULES:

1. Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003, read in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive as amended, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.
2. Decision 2000/520 is invalid.

SOURCE: INFOCURIA - JURISPRUDENTIE VAN HET HOF VAN JUSTITIE; HTTP://CURIA.EUROPA.EU/JURIS/DOCUMENTS.JSF?NUM=C-362/14

"In the meantime, transatlantic data flows between companies **CAN CONTINUE USING OTHER MECHANISMS** for international transfers of personal data available under EU data protection law."

EU
First Vice-President Timmermans
Commissioner Jourová

Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, requires Member States to permit transfers of personal data to countries outside the European Union only where there is adequate protection for such data, unless one of a limited number of specific exemptions applies.

Article 26 (4) of the Directive allows the Commission, with the support of a Management Committee composed of Member State representatives, to issue **standard contractual clauses which those transferring data to non-EU countries can use to fulfil the requirements set down by the Directive**.

EU
Standard Contractual Clauses
2005

MICROSOFT ONLINE SERVICES TERMS (OST)

Attachment 3 – The Standard Contractual Clauses (Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, Customer (as data exporter) and Microsoft Corporation (as data importer, whose signature appears below), each a "party," together "the parties," have agreed on the following Contractual Clauses (the "Clauses" or "Standard Contractual Clauses") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

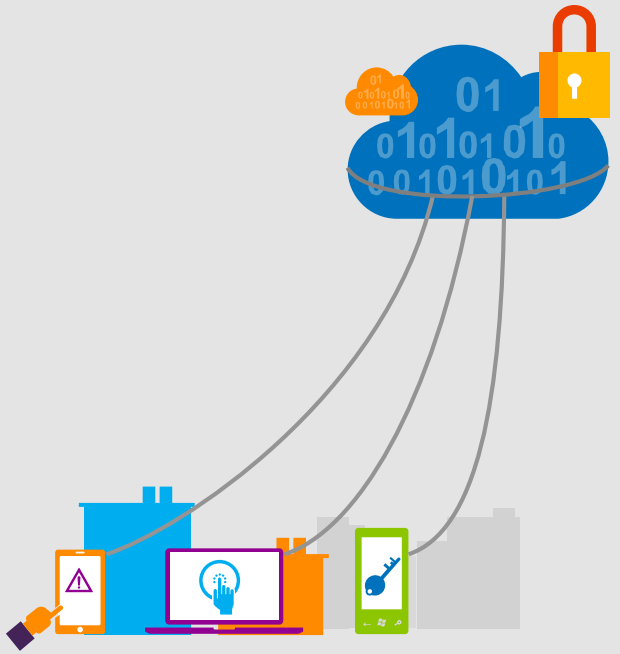
SOURCE: MICROSOFT VOLUME LICENSING; HTTP://WWW.MICROSOFTVOLUMELICENSING.COM/DOCUMENTSEARCH.ASPX?MODE=3&DOCUMENTTYPEID=31

ISO/IEC 27018

Microsoft is the first major cloud provider to adopt the first international code of practice for governing the processing of personal information by cloud service providers.

Prohibits use of customer data for advertising and marketing purposes without customer's express consent.

Prevents use of customer data for purposes unrelated to providing the cloud service.



We understand that **GOVERNMENTS HAVE A DUTY TO PROTECT THEIR CITIZENS**.

But this summer's revelations highlighted the **URGENT NEED TO REFORM GOVERNMENT SURVEILLANCE PRACTICES WORLDWIDE**. The balance in many countries has tipped too far in favor of the state and away from the rights of the individual rights that are enshrined in our Constitution. This undermines the freedoms we all cherish. It's time for change.

For our part, we are focused on **KEEPING USERS' DATA SECURE** deploying the latest encryption technology **TO PREVENT UNAUTHORIZED SURVEILLANCE** on our networks, and by pushing back on government requests to ensure that they are legal and reasonable in scope.

LAW ENFORCEMENT ACCESS
GOVERNMENT SURVEILLANCE
HTTP://WWW.MICROSOFT.COM/EN-US/NEWS/PRESS/2013/DEC13/12-08COMPANYCOALITIONPR.ASPX





Protecting vulnerable populations

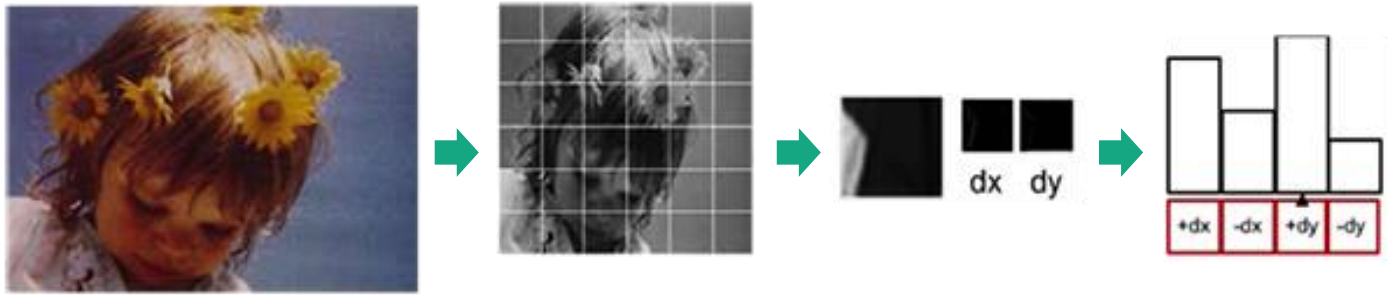
Online child protection | Elder fraud





PhotoDNA

Putting a digital fingerprint on child abuse content



PhotoDNA in action

Creates signatures of the worst known child abuse images

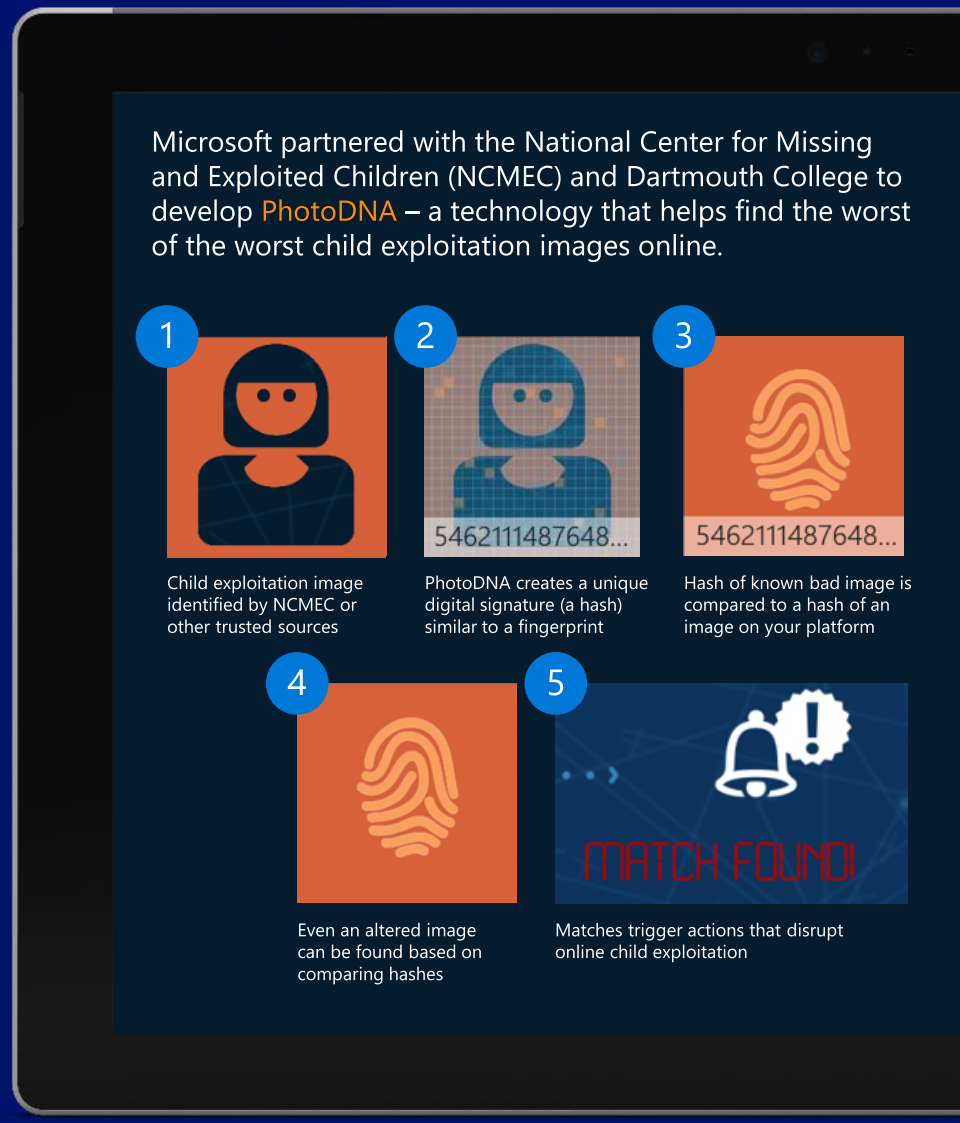
Can locate these images among the millions online

Shared with law enforcement to accelerate prosecution

Also used by Facebook, Google, and Twitter and others

Microsoft PhotoDNA

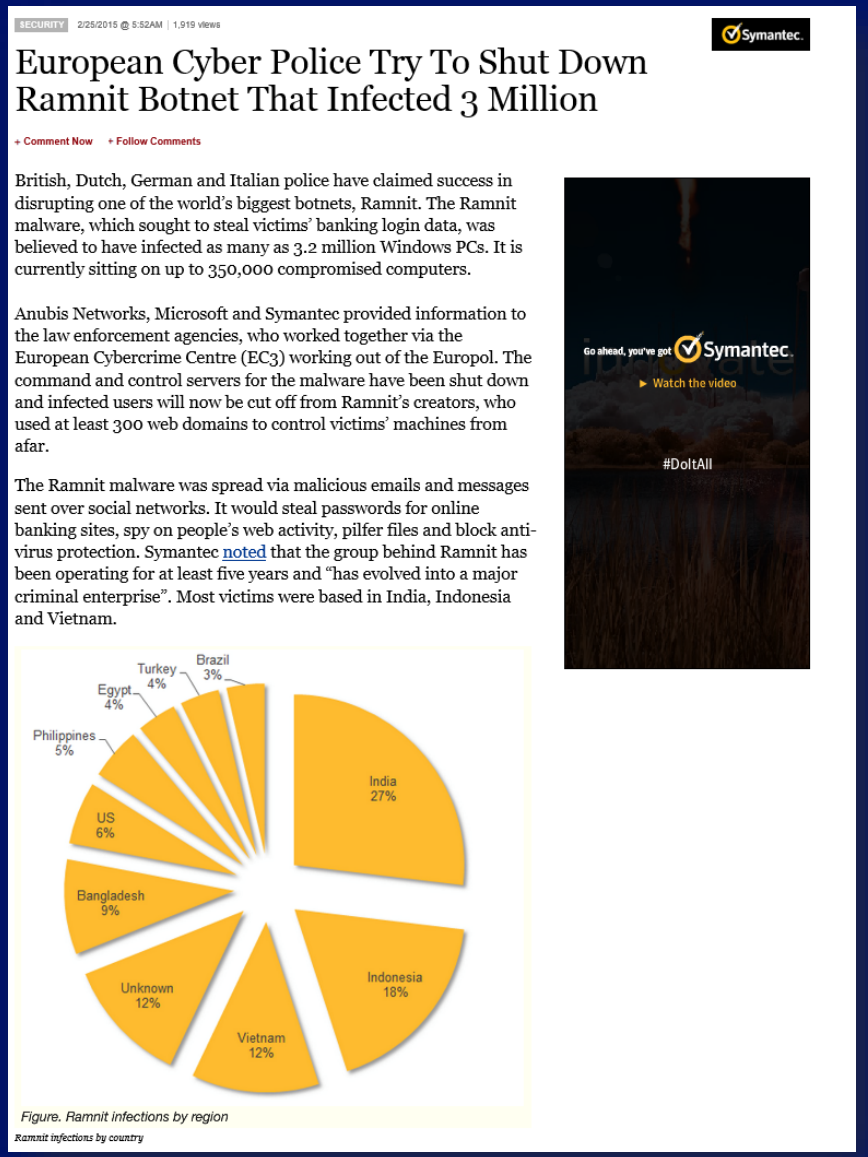
- **Creates signatures** of the worst known child abuse images
- **Can locate** these images among the millions online
- **Shared with** law enforcement and licensed to over 50 organizations around the world for free
- **Industry standard** – used by Facebook, Twitter, Google



Outlook.com bing OneDrive

Ramnit Botnet Takedown February 24, 2015

- Hague – joint international operation coordinated by **Europol's European Cybercrime Centre (EC3)**
- Over **3.2 million infected computers** (through links contained in spam emails or through visiting infected websites) all around the world
- Used by criminals to **steal personal and banking information** and to **disable antivirus protection**
- Investigators from **Germany, Italy, Netherlands, UK** with technical assistance from Microsoft, Symantec and AnubisNetworks handled the operation
- Command control servers were shut down and **300 Internet domain addresses** used by the botnet's operators were redirected



SECURITY 2/25/2015 @ 5:52AM | 1,919 views

Symantec.

European Cyber Police Try To Shut Down Ramnit Botnet That Infected 3 Million

+ Comment Now + Follow Comments

British, Dutch, German and Italian police have claimed success in disrupting one of the world's biggest botnets, Ramnit. The Ramnit malware, which sought to steal victims' banking login data, was believed to have infected as many as 3.2 million Windows PCs. It is currently sitting on up to 350,000 compromised computers.

Anubis Networks, Microsoft and Symantec provided information to the law enforcement agencies, who worked together via the European Cybercrime Centre (EC3) working out of the Europol. The command and control servers for the malware have been shut down and infected users will now be cut off from Ramnit's creators, who used at least 300 web domains to control victims' machines from afar.

The Ramnit malware was spread via malicious emails and messages sent over social networks. It would steal passwords for online banking sites, spy on people's web activity, pilfer files and block anti-virus protection. Symantec noted that the group behind Ramnit has been operating for at least five years and "has evolved into a major criminal enterprise". Most victims were based in India, Indonesia and Vietnam.

Figure. Ramnit infections by region

Ramnit infections by country