Are we creating incidents?

August 26, 2015

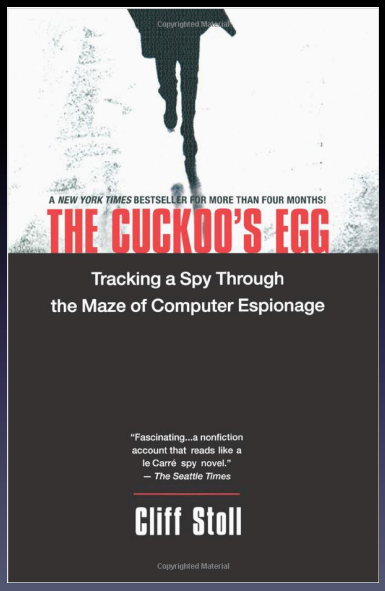
在 臺北

Shin Adachi, CISSP, CISM, CISA, PMP

Disclaimer

- The presentation itself, and the views and opinions expressed by the presenter therein do NOT reflect those of any of my affiliations at all.
- NONE of such affiliations above thereof assumes any legal liability or responsibility for the presentation.

Cuckoo's Egg



Source: http://www.amazon.com/Cuckoos-Egg-Tracking-Computer-Espionage/dp/1416507787

Cuckoo's Egg

Authentication Breach

....eventually realized that the unauthorized user was a hacker who had acquired root access to the LBL system by exploiting a vulnerability in the movemail function of the original GNU Emacs.

Vulnerability Exploited!

Privilege Escalation

Source: Wikipedia: http://en.wikipedia.org/wiki/The_Cuckoo%27s_Egg

Cuckoo's Egg

- Published in 1989
- Story on August 1986

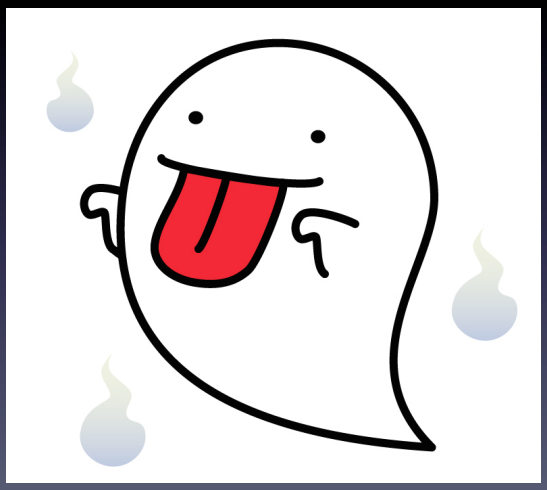
Source: Wikipedia: http://en.wikipedia.org/wiki/The_Cuckoo%27s_Egg

QUESTION

Why do we STILL have the same problems after almost 30 years?

Inventory and Lifecycle management

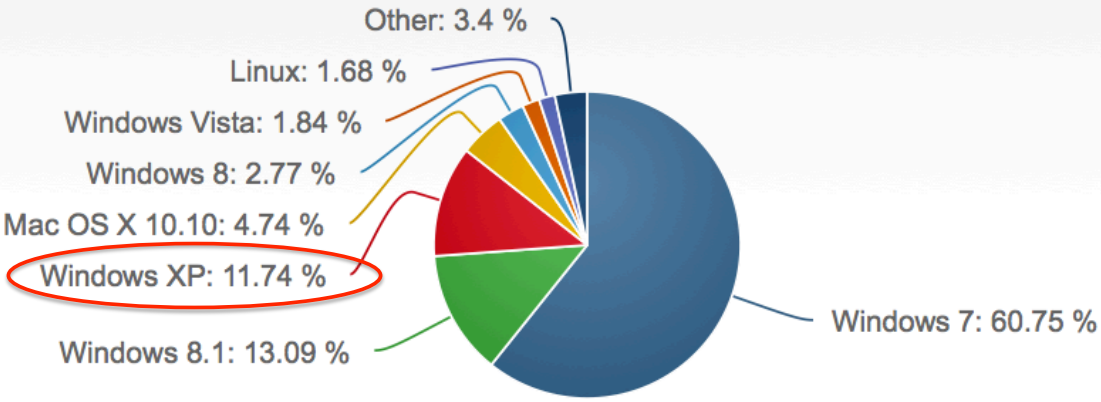
Do we know ALL we have up to date, or are legacies, zombies, or ghosts still alive?



Source: © Nekojin (ねこじん様)

Inventory and Lifecycle management

Are legacies, zombies, or ghosts still alive?



Source: NetMarketShare, July 2015:
http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0

Inventory and Lifecycle management

Are legacies, zombies, or ghosts still alive?

Windows Server 2003 extended support ended on July 14, 2015

What does this mean for you? Microsoft will no longer issue security updates for any version of Windows Server 2003. If you are still

Source: Microsoft:
https://www.microsoft.com/en-us/server-cloud/products/windows-server-2003/

Inventory and Lifecycle management

MS15-078- Critical: as Real Impact😰😱

Microsoft Security Bulletin MS15-078 – Critical

Vulnerability in Microsoft Font Driver Could Allow Remote Code Execution (3079904)

Published: July 20, 2015

Version: 1.0

Executive Summary

This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted document or visits an untrusted webpage that contains embedded OpenType fonts.

This security update is rated Critical for all supported releases of Microsoft Windows. For more information, see the **Affected Software** section.

On this pag
Executive Summa
Affected Software
Severity Ratings a
Vulnerability Iden

Source: Microsoft:
https://technet.microsoft.com/en-us/library/security/ms15-078.aspx

Inventory and Lifecycle management

- July 14, 2015 MS15-077 (Important) Released, covering Windows Server 2003
- July 14, 2015 Microsoft ended support for Windows Server 2003
- July 20, 2015 MS15-078 (Critical): replaces MS15-077, **without covering** Windows Server 2003…😰😱

Source: Microsoft:
https://technet.microsoft.com/en-us/library/security/ms15-077.aspx
https://technet.microsoft.com/en-us/library/security/ms15-078.aspx

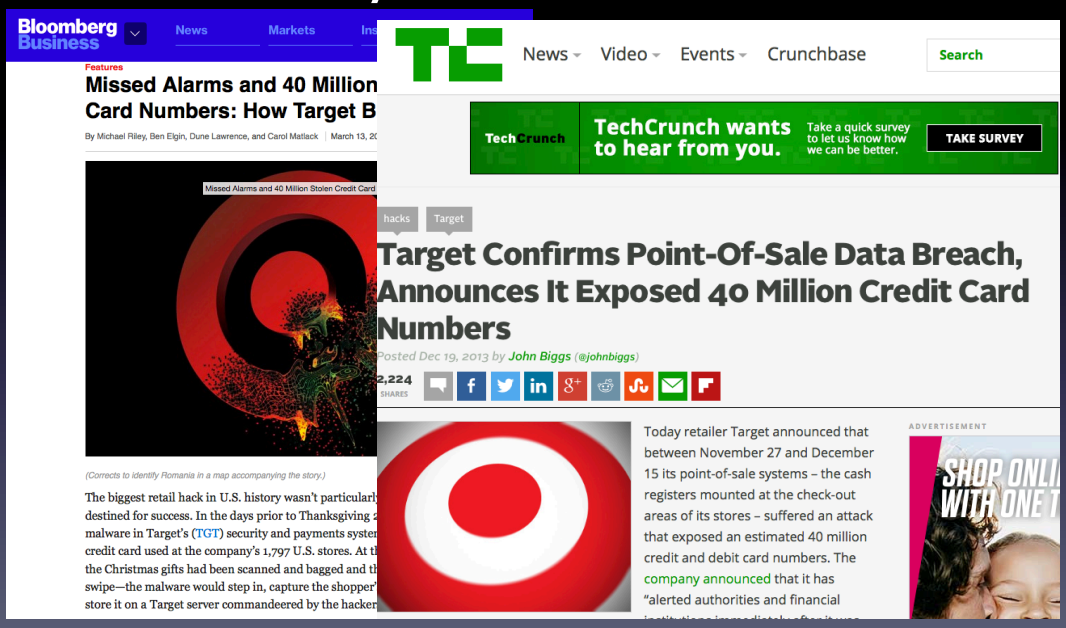
Inventory and Lifecycle management

Running OpenSSL 0.9.8 or 1.00? Are U ready?

- Support for version 0.9.8 **will cease on 2015-12-31.**
- Support for version 1.0.0 **will cease on 2015-12-31.**
- Version 1.0.1 will be supported until 2016-12-31.
- Version 1.0.2 will be supported until 2019-12-31. (updated on August 9, 2015)

Source: OpenSSL Release Strategy:
https://www.openssl.org/about/releasestrat.html

PoS System breach?



Source: TechCrunch and Bloomberg

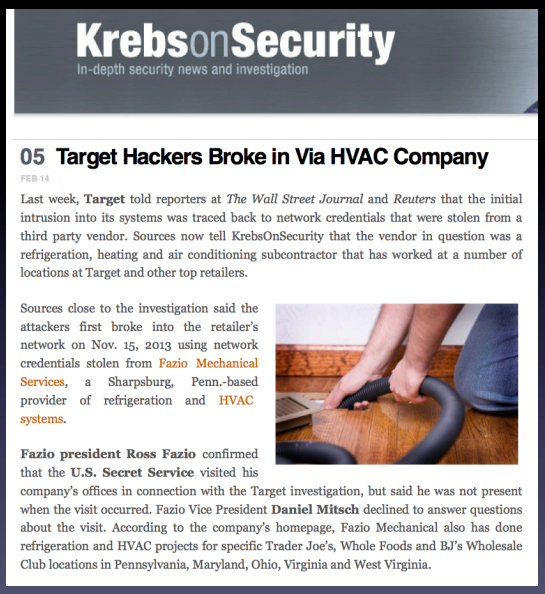
Policy and implementation

"the malware started transmitting the stolen data to an **external FTP server,** using another infected machine within the Target network."

- Why outgoing FTP allowed? 😨😰😓

Source: Seculert: http://www.seculert.com/blog/2014/01/pos-malware-targeted-target.html

Authentication and Authorization



KrebsonSecurity
In-depth security news and investigation

05 Target Hackers Broke in Via HVAC Company

FEB 14

Last week, **Target** told reporters at *The Wall Street Journal* and *Reuters* that the initial intrusion into its systems was traced back to network credentials that were stolen from a third party vendor. Sources now tell KrebsOnSecurity that the vendor in question was a refrigeration, heating and air conditioning subcontractor that has worked at a number of locations at Target and other top retailers.

Sources close to the investigation said the attackers first broke into the retailer's network on Nov. 15, 2013 using network credentials stolen from Fazio Mechanical Services, a Sharpsburg, Penn.-based provider of refrigeration and HVAC systems.

Fazio president Ross Fazio confirmed that the **U.S. Secret Service** visited his company's offices in connection with the Target investigation, but said he was not present when the visit occurred. Fazio Vice President **Daniel Mitsch** declined to answer questions about the visit. According to the company's homepage, Fazio Mechanical also has done refrigeration and HVAC projects for specific Trader Joe's, Whole Foods and BJ's Wholesale Club locations in Pennsylvania, Maryland, Ohio, Virginia and West Virginia.

Source: Krebs on Security: http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

"Last week, Target told reporters at The Wall Street Journal and Reuters that the ***initial intrusion into its systems was traced back to network credentials that were stolen from a third party vendor.***"

- Why did that vendor need access?
- What authorization granted?

Saga continues, costing $$$

abc7 NEWS
SAN FRANCISCO • OAKLAND • SAN JOSE

SECTIONS TRAFFIC VIDEO San Francisco East Bay South Bay Peninsula

BREAKING NEWS Health officials investigate another plague case in Yo

SHOPPING

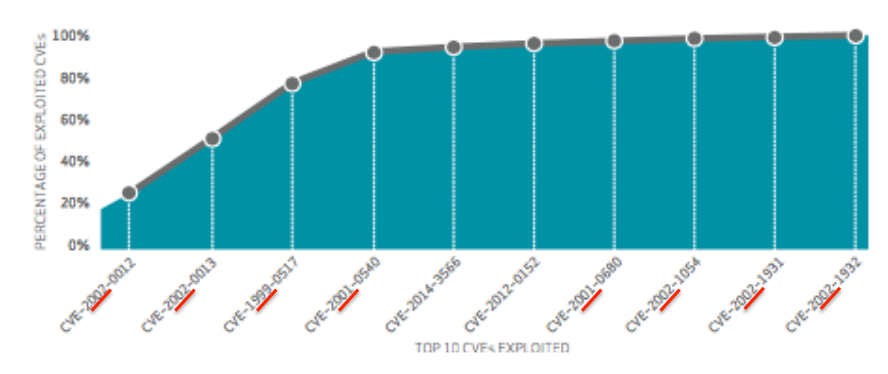
TARGET AGREES TO PAY VISA $67 MILLION AFTER 2013 DATA BREACH

TARGET

Source: ABC & News Bay Area, on Tuesday August 18, 2015: http://abc7news.com/shopping/target-agrees-to-pay-visa-$67-million-after-2013-data-breach/944667/

Software vulnerabilities and exploits

- Are we doing enough and right?

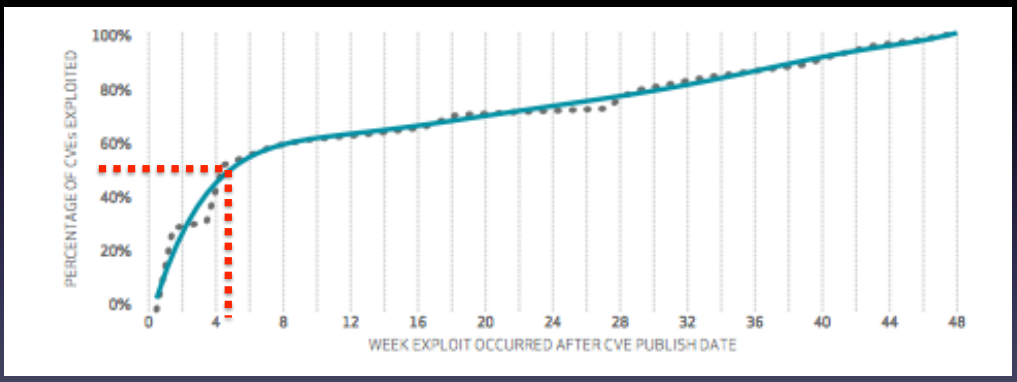


"99.9% OF THE EXPLOITED VULNERABILITIES WERE COMPROMISED MORE THAN A YEAR AFTER THE CVE WAS PUBLISHED." , according to 2015 Verizon DBIR

Source: p15, Verizon 2015 Data Breach Investigation Report

Software vulnerability and exploits

- Attackers move quickly..

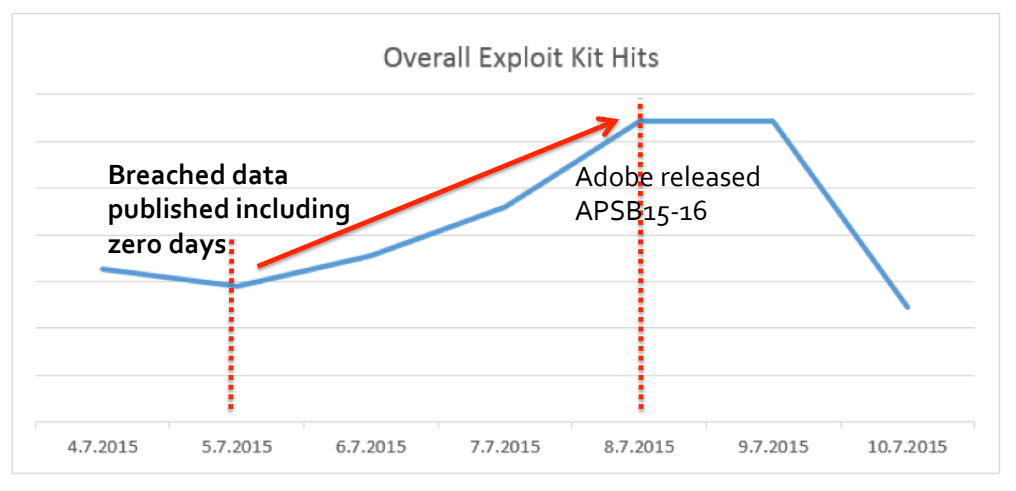


"About half of the CVEs exploited in 2014 went from publish to pwn in less than a month." , according to 2015 Verizon DBIR

Source: p16, Verizon 2015 Data Breach Investigation Report

Software vulnerability and exploits

- Even more quickly..



Source: F-Secure "Hacking Team 0-day Flash Wave with Exploit Kits"
https://www.f-secure.com/weblog/archives/00002819.html

Operational (In)Security

WorldCup 2014

Source: https://twitter.com/apbarros/status/481157619261116416/photo/1

Operational (In)Security

- Worldcup 2014

Source: https://twitter.com/apbarros/status/481157619261116416/photo/1

Operational (In)Security

- TV5 Monde in France on April 2015

Source: BBC, "**France TV5Monde passwords seen on cyber-attack TV report**"
http://www.bbc.com/news/world-europe-32248779

Mobile

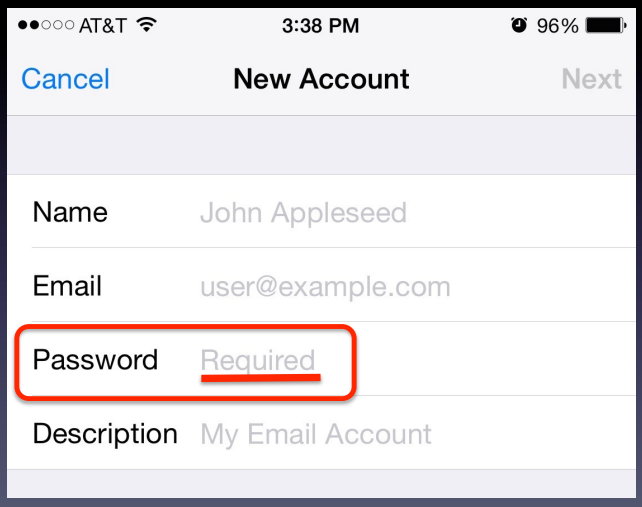
Especially smart phones are more scary than PCs

- Can be easily lost
- More personal info~ yours AND others
- Insecure "features"
- Do/Can you log out?

as well as software vulnerabilities

Mobile

- Insecure "requirement"



Source: My iPhone 6 Plus

Are we creating incidents?

- Are we doing enough?
- Are we doing right?
- Are we learning lessons?

Thoughts and possible takeaways

Authentication and Authorization

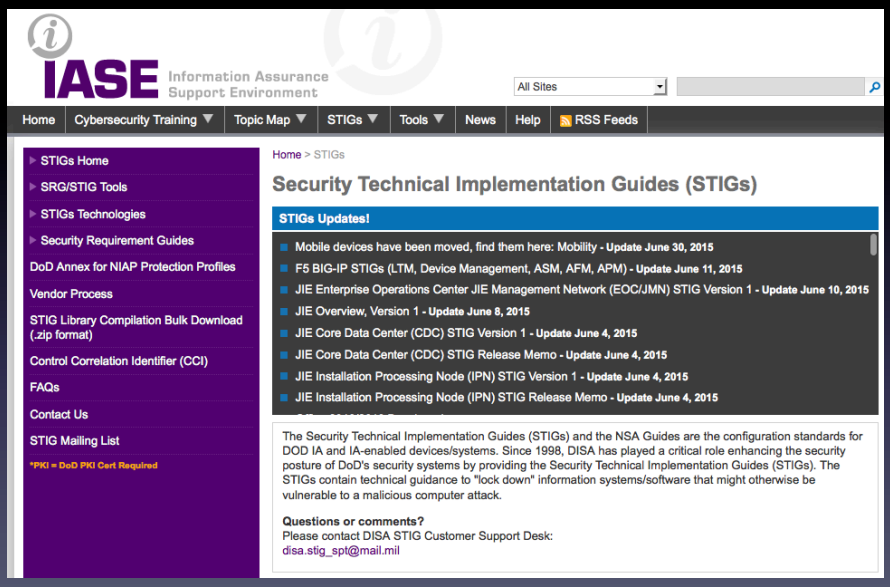
- Regardless of the attack vectors [old, new, or emerging]
- **Important** Identity and Access Management (IAM)
- Need broad scope and consideration:
  - Enrollment, Lifecycle, Credential, Key,
  - Identity Management for authentication,
  - Access control and Attribute management for authorization,
  - Level of identity or authentication assurance,
  - monitoring suspicious behaviors,
  - policy enforcement, etc.

Configure your assets secured
~ Configuration Matters!~

- Client Terminals
- Servers
- Routers
- Switches
- Printers etc.

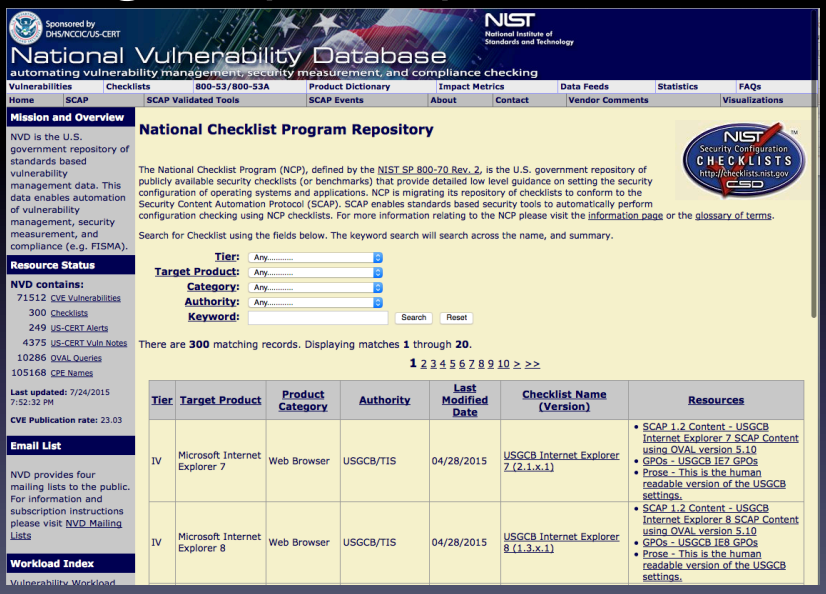
Great references available for FREE

Configure your system secured



Source: http://iase.disa.mil/stigs/Pages/index.aspx

Configure your system secured



Source: https://web.nvd.nist.gov/view/ncp/repository

Configure your system secured

Source: The United States Government Configuration Baseline (USGCB): http://usgcb.nist.gov/index.html

Segmentation

- Develop stable and updated policy
- Subnet based
- Hardware based
- Role or function based
- Usage based

Mobile

Detect the incidents ASAP!

- Disable access from that terminal ASAP
- Remote erase
- Kill switch

Monitoring and logging

- Synchronize CLOCK
- Detection focused
  - Keep confirming if there is anything unmonitored
- Keep thinking what can be "NOT NORMAL"
  - Time
  - Geolocation
- Mobile
  - Give priority to be monitored
  - Prepare for blocking them at any time

Check your outsourced resources
(e.g. your data on "Cloud")

- Think again what data can be really outsourced
- Confirm terms and conditions, contract, SLAs.
- Use as strong authentication as possible
- Check your "neighbors"
- Check access logs as often as possible
- Check how your providers are secured

Post Disaster

- Update your Disaster Recovery and Business Continuity plans if you are directly involved.
- Attacks after disasters
  - Malicious emails pretending donation, breaking news, etc.
- Analyze the disaster
  - Analyze impact as if it had happened to your business

Source: NASA http://earthobservatory.nasa.gov/NaturalHazards/view.php?id=86270

Incident Response

- Do our BEST to be prepared before incidents
- Train and exercise ourselves
- Identify and involve stakeholders "in advance"
- CSIRT

Communicating with others

- Expand our capability to ***learn*** from each other
  - to share something with them
  - to learn something from them
  - to notify, and to be notified
- Other companies, even competitors
- Government Agencies including LEAs and Regulators

Our possible next challenge

IoT, or Internet of Things

Do you think this is a problem in the future?

IoT

1. …IoT devices **are actively penetrating** some of the **world's most regulated industries including healthcare, energy infrastructure, government, financial services, and retail.**
2. Our analysis identified three principal risks that IoT devices present in protecting network environments with IoT devices:
   (1) IoT devices introduce **new avenues for potential remote exploitation** of enterprise networks;
   (2) the infrastructure used to enable IoT devices is **beyond both the user and IT's control**; and
   (3) IT's often casual approach to IoT device management can leave devices **unmonitored and unpatched**.

Source: OpenDNS "The 2015 Internet of Things in the Enterprise Report"
http://info.opendns.com/rs/033-OMP-861/images/OpenDNS-2015-IoT-Report.pdf

IoT

3. Some infrastructures **hosting IoT data are susceptible to highly-publicized and patchable vulnerabilities** such as FREAK and Heartbleed.
4. Highly prominent technology vendors are **operating their IoT platforms in known "bad Internet neighborhoods," which places their own customers at risk.**
5. Consumer devices such as Dropcam Internet video cameras, Fitbit wearable fitness devices, Western Digital "My Cloud" storage devices, various connected medical devices, and Samsung Smart TVs **continuously beacon out to servers in the US, Asia, and Europe–even when not in use.**

Source: OpenDNS "The 2015 Internet of Things in the Enterprise Report"
http://info.opendns.com/rs/033-OMP-861/images/OpenDNS-2015-IoT-Report.pdf

IoT

6. Though traditionally thought of as local storage devices, Western Digital cloud-enabled hard drives are now some of the most prevalent IoT endpoints observed. Having been ushered into **highly-regulated enterprise environments,** these devices are **actively transferring data to insecure cloud servers.**
7. And finally, a survey of more than 500 IT and security professionals found that **23 percent** of respondents have **no mitigating controls in place to prevent someone from connecting unauthorized devices to their company's networks**.

Source: OpenDNS "The 2015 Internet of Things in the Enterprise Report"
http://info.opendns.com/rs/033-OMP-861/images/OpenDNS-2015-IoT-Report.pdf

To conclude:

- Do "ALL" what we CAN do NOW!
  - before we create, or make incidents worse
  - before excuses
- Keep learning
- Keep Questioning

  "The important thing is not to stop questioning. Curiosity has its own reason for existing." Albert Einstein

To Conclude:

- 知彼知己者、百戰不殆、
- 不知彼而知己、一勝一負、
- 不知彼不知己、每戰必殆。

Source: 孫子　攻謀篇第三

Acknowledgement

Discussion with, and inspiration from NTT-CERT have contributed a lot to the idea of today's presentation

QUESTIONS?

- NOW!
- Catch me here today or tomorrow 😀
- @s_adachi

非常感謝!
Thank you very much!

Kate Wu 吳宛諭,

PeiKan Tsung,

Joel,

John

and last but never least,

All of you here!