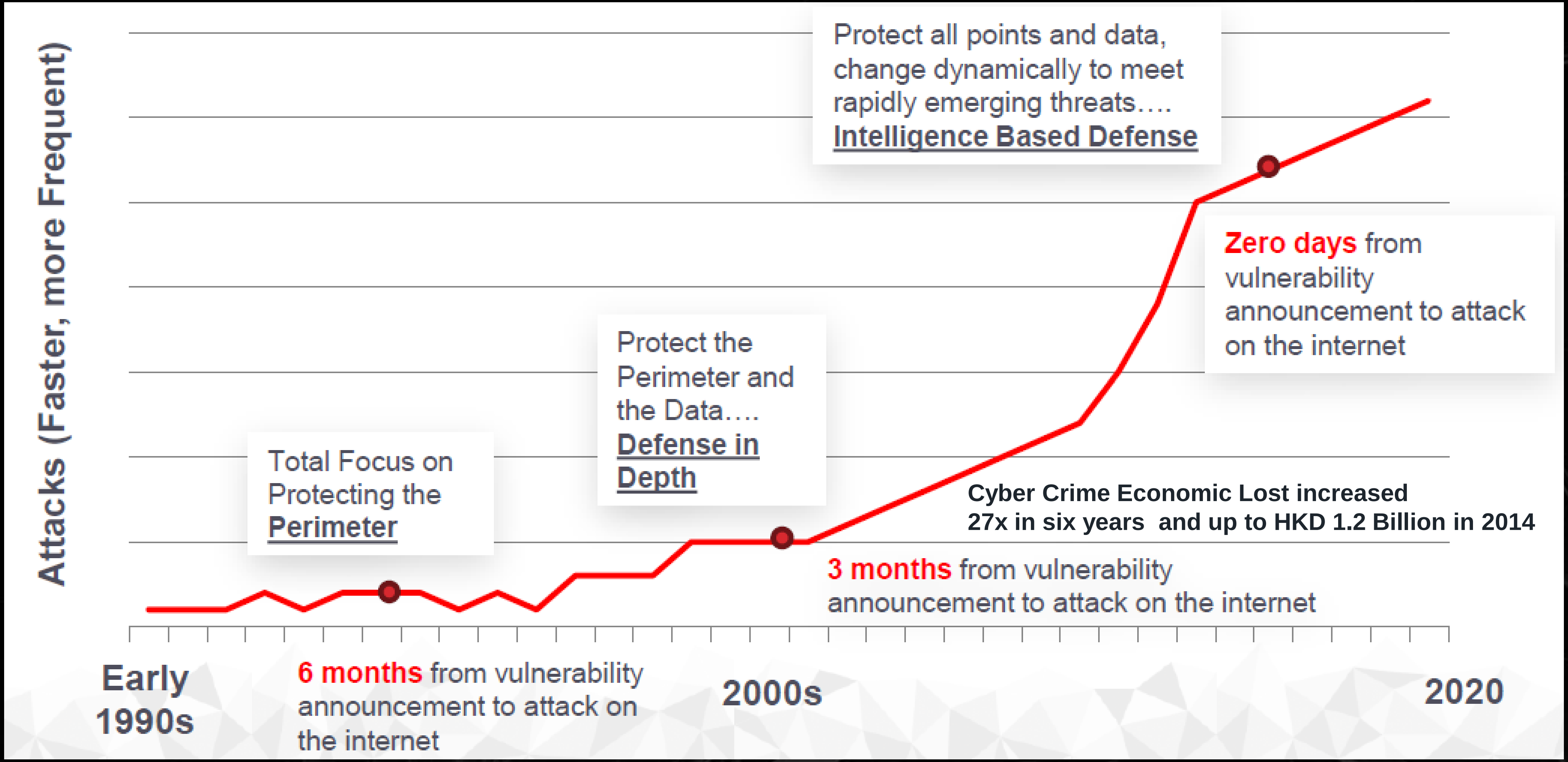
Targeted Attack on Enterprise

Matthew WONG

Consulting Systems Engineer, FireEye

Evolution of Cyber-Defense Strategies



Total Focus on Protecting the **Perimeter**

Protect the Perimeter and the Data…. **Defense in Depth**

Protect all points and data, change dynamically to meet rapidly emerging threats…. **Intelligence Based Defense**

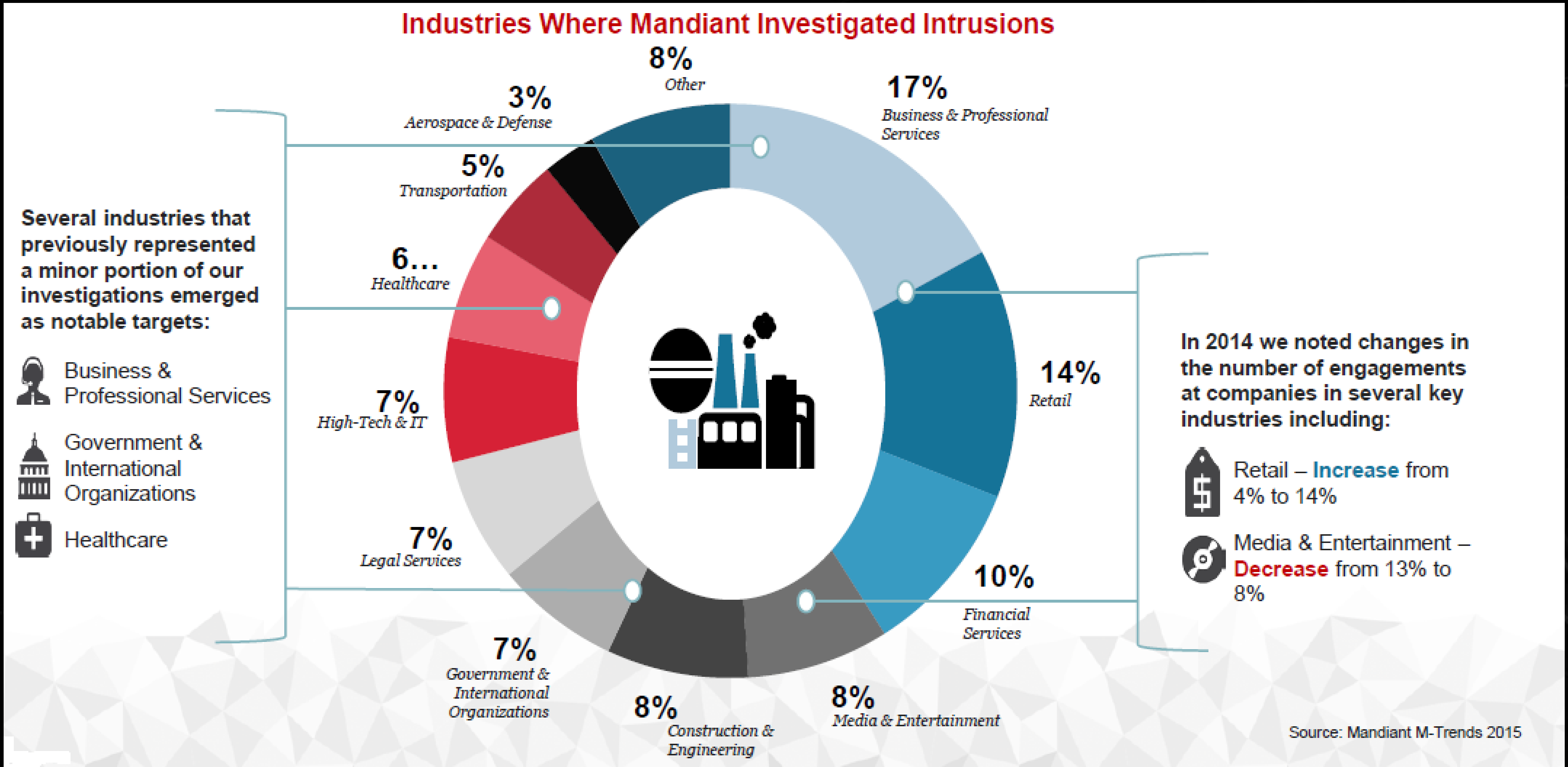
6 months from vulnerability announcement to attack on the internet

3 months from vulnerability announcement to attack on the internet

Zero days from vulnerability announcement to attack on the internet

Cyber Crime Economic Lost increased 27x in six years and up to HKD 1.2 Billion in 2014

The Number of Industries Targeted by Advanced Attackers continues to Expand and Evolve



Industries Where Mandiant Investigated Intrusions

Several industries that previously represented a minor portion of our investigations emerged as notable targets:

- Business & Professional Services
- Government & International Organizations
- Healthcare

In 2014 we noted changes in the number of engagements at companies in several key industries including:

- Retail – **Increase** from 4% to 14%
- Media & Entertainment – **Decrease** from 13% to 8%

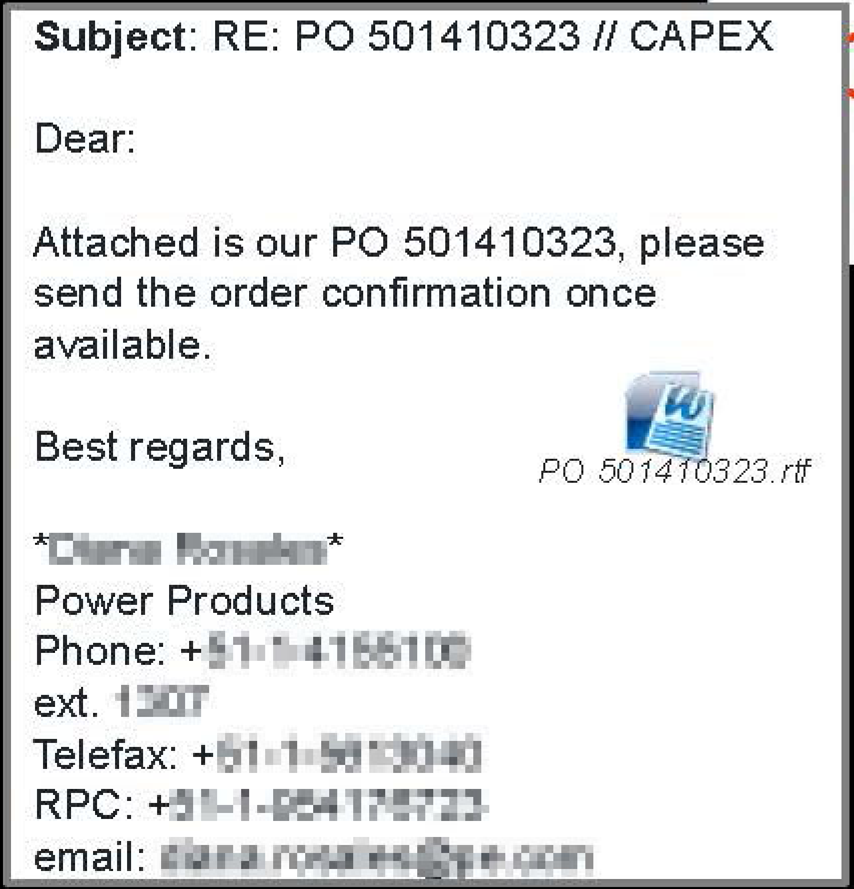
Source: Mandiant M-Trends 2015

Targeted Cybercrime Case Study

MAY 4

MAY 15

MAY 18



Subject: RE: PO 501410323 // CAPEX

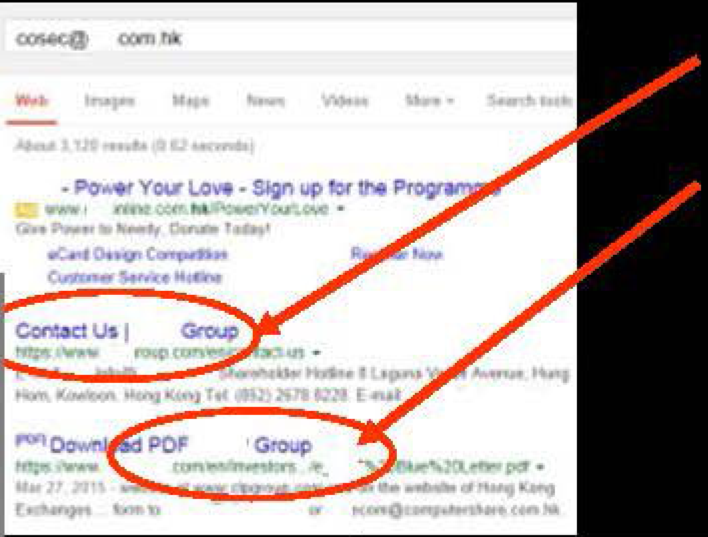
Dear:

Attached is our PO 501410323, please send the order confirmation once available.

Best regards,

PO 501410323.rtf

[redacted]
Power Products
Phone: +[redacted]
ext. [redacted]
Telefax: +[redacted]
RPC: +[redacted]
email: [redacted]



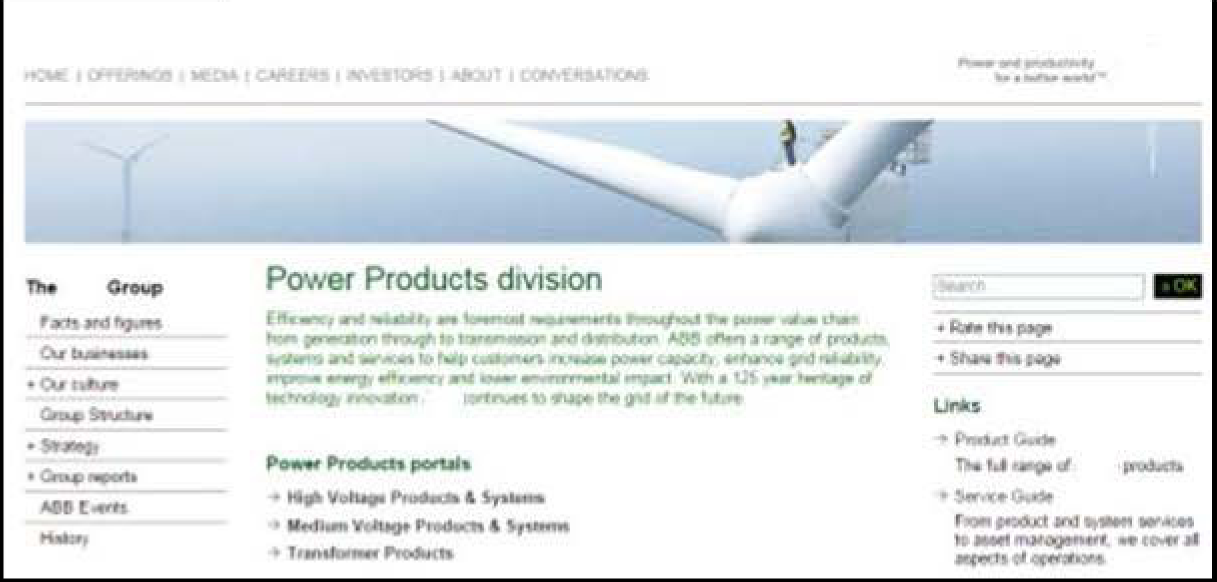
About 3,120 results (0.62 seconds)

- Power Your Love - Sign up for the Programme
www. .com.hk/PowerYourLove
Give Power to Needy, Donate Today!
eCard Design Competition Register Now
Customer Service Hotline

Contact Us | Group
https://www. roup.com/en/contact-us
Shareholder Hotline 8 Laguna Verde Avenue, Hung Hom, Kowloon, Hong Kong Tel: (852) 2678 8228. E-mail

[PDF] Download PDF Group
https://www. com/en/investors .../e_ %20Blue%20Letter.pdf
Mar 27, 2015 - on the website of Hong Kong Exchanges ... form to or ecom@computershare.com.hk

Recipient E-mail address can be search in Internet become low hanging food for attackers



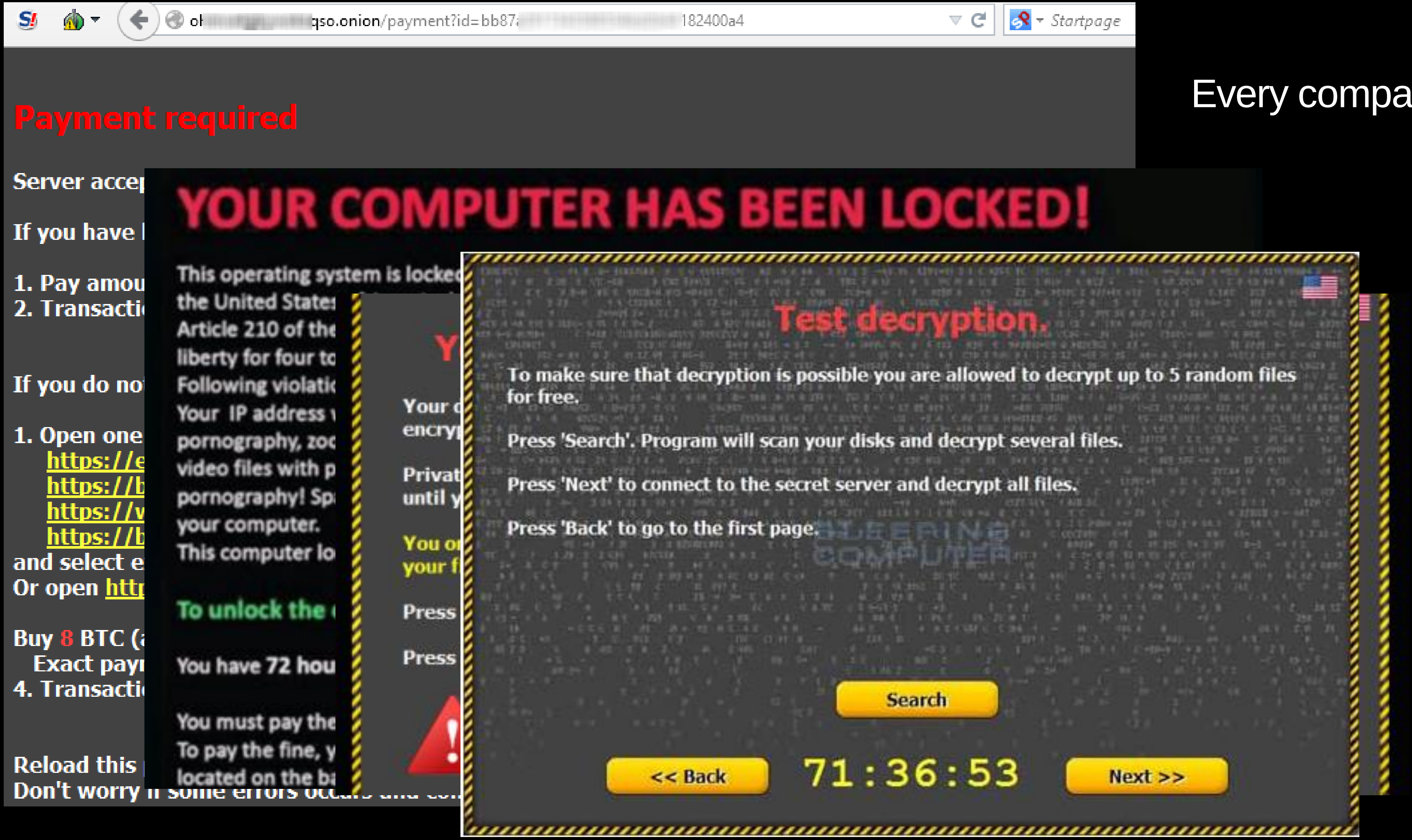
Power Products division

Efficiency and reliability are foremost requirements throughout the power value chain from generation through to transmission and distribution. ABB offers a range of products, systems and services to help customers increase power capacity, enhance grid reliability, improve energy efficiency and lower environmental impact. With a 125 year heritage of technology innovation, continues to shape the grid of the future.

Power Products portals
→ High Voltage Products & Systems
→ Medium Voltage Products & Systems
→ Transformer Products

Links
→ Product Guide
The full range of products
→ Service Guide
From product and system services to asset management, we cover all aspects of operations.

CTB locker ransomware still very active



ol[redacted]qso.onion/payment?id=bb87[redacted]182400a4

Payment required

Server accep

If you have l

1. Pay amou
2. Transacti

If you do no

1. Open one
   https://e
   https://b
   https://v
   https://b
and select e
Or open http

Buy 8 BTC (a
   Exact payn
4. Transacti

Reload this
Don't worry if some errors occurs and co

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked
the United States
Article 210 of the
liberty for four to
Following violatio
Your IP address w
pornography, zoo
video files with p
pornography! Sp
your computer.
This computer lo

To unlock the

You have 72 hou

You must pay the
To pay the fine, y
located on the ba

Y

Your c
encryp

Privat
until y

You o
your f

Press

Press

Test decryption.

To make sure that decryption is possible you are allowed to decrypt up to 5 random files for free.

Press 'Search'. Program will scan your disks and decrypt several files.

Press 'Next' to connect to the secret server and decrypt all files.

Press 'Back' to go to the first page.

Every company is facing this problem

The basics

Attacker’s Goal: Issue instructions on the victim PC

The basics

Application

Document

Types of attack

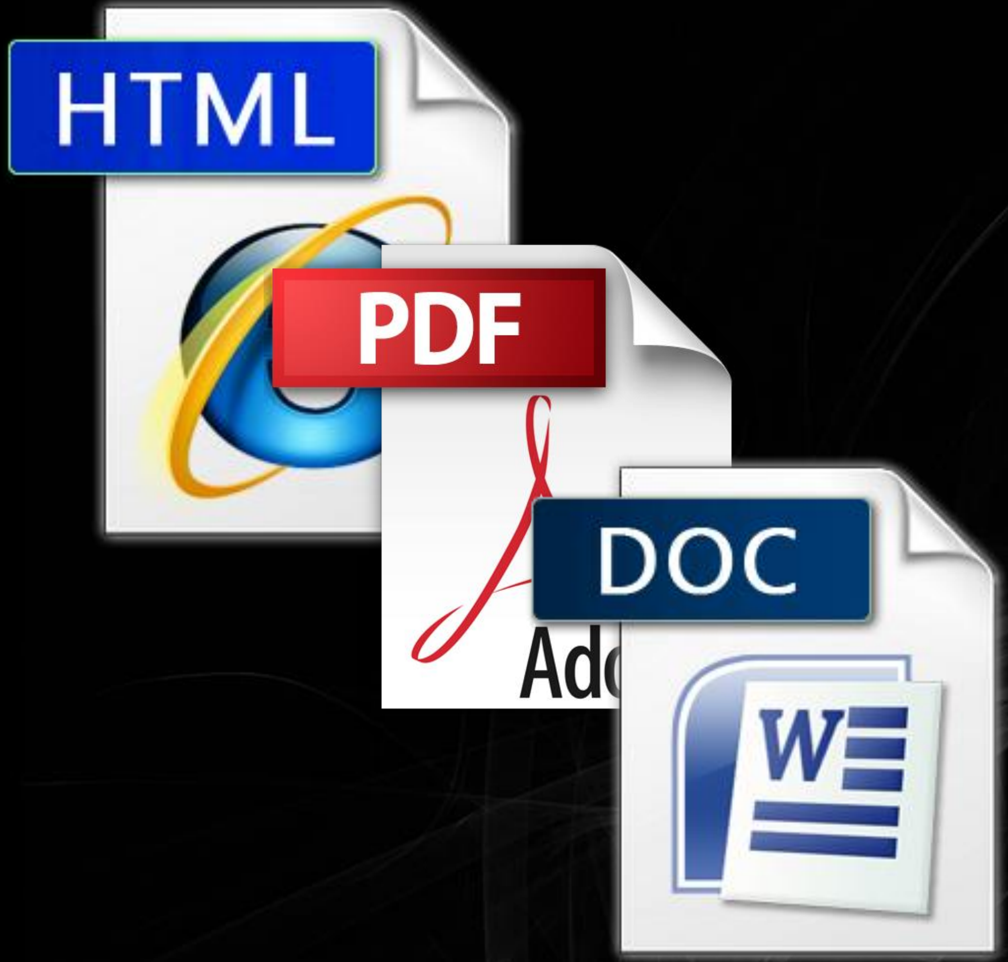
Fool the Human: Social Engineering

Fool the Computer: Exploitation

Types of attack: End User Social Engineering

Fool the Human: Social Engineering

Types of attack: Vulnerability Exploitation

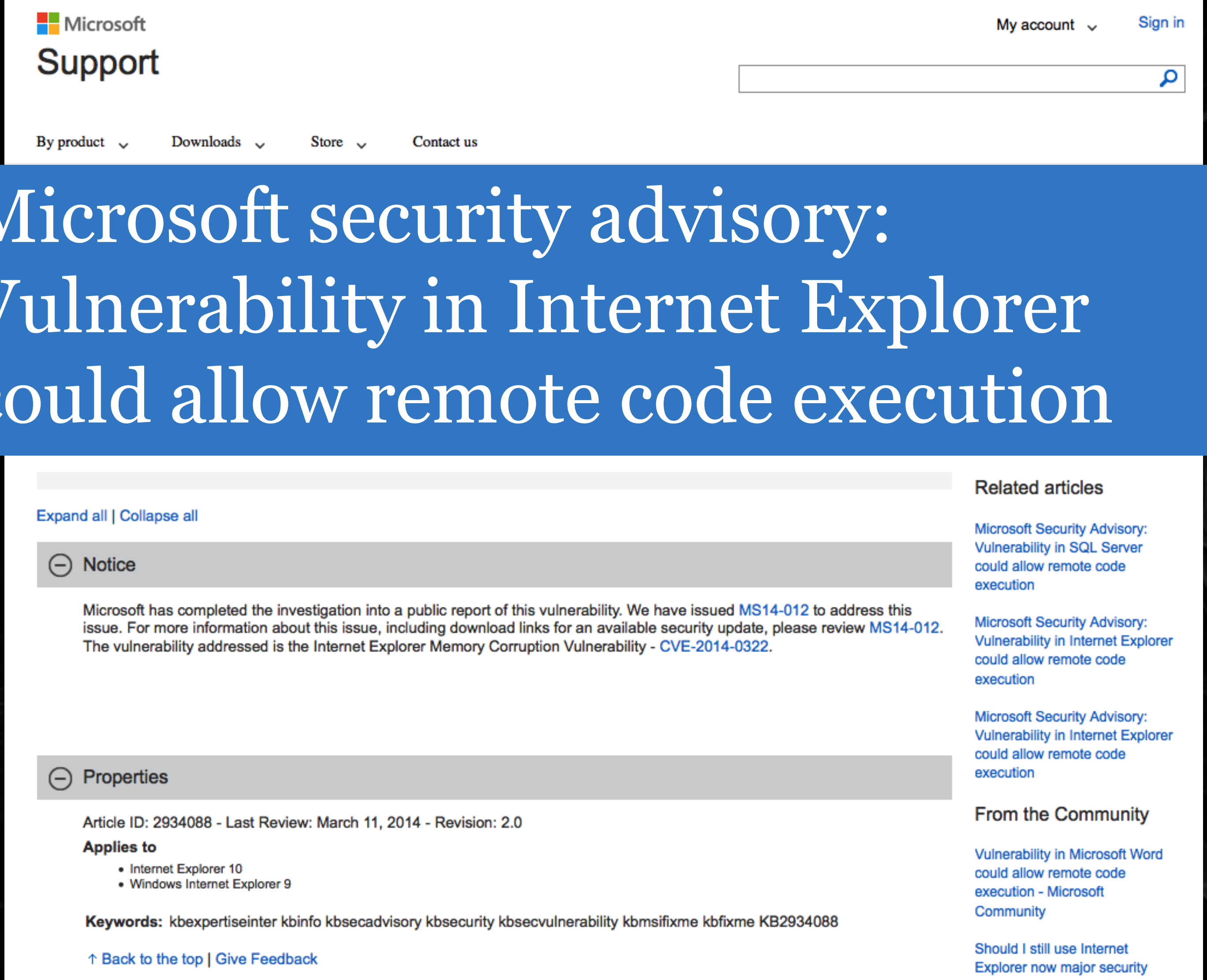


Fool the Computer: Exploitation

How do you “fool the computer”

Not meant to issue instructions, but
can if a vulnerability exists in the app
which uses this document / data

For example…



Microsoft security advisory: Vulnerability in Internet Explorer could allow remote code execution

Expand all | Collapse all

Notice

Microsoft has completed the investigation into a public report of this vulnerability. We have issued MS14-012 to address this issue. For more information about this issue, including download links for an available security update, please review MS14-012. The vulnerability addressed is the Internet Explorer Memory Corruption Vulnerability - CVE-2014-0322.

Properties

Article ID: 2934088 - Last Review: March 11, 2014 - Revision: 2.0

Applies to

- Internet Explorer 10
- Windows Internet Explorer 9

Keywords: kbexpertiseinter kbinfo kbsecadvisory kbsecurity kbsecvulnerability kbmsifixme kbfixme KB2934088

↑ Back to the top | Give Feedback

Related articles

Microsoft Security Advisory: Vulnerability in SQL Server could allow remote code execution

Microsoft Security Advisory: Vulnerability in Internet Explorer could allow remote code execution

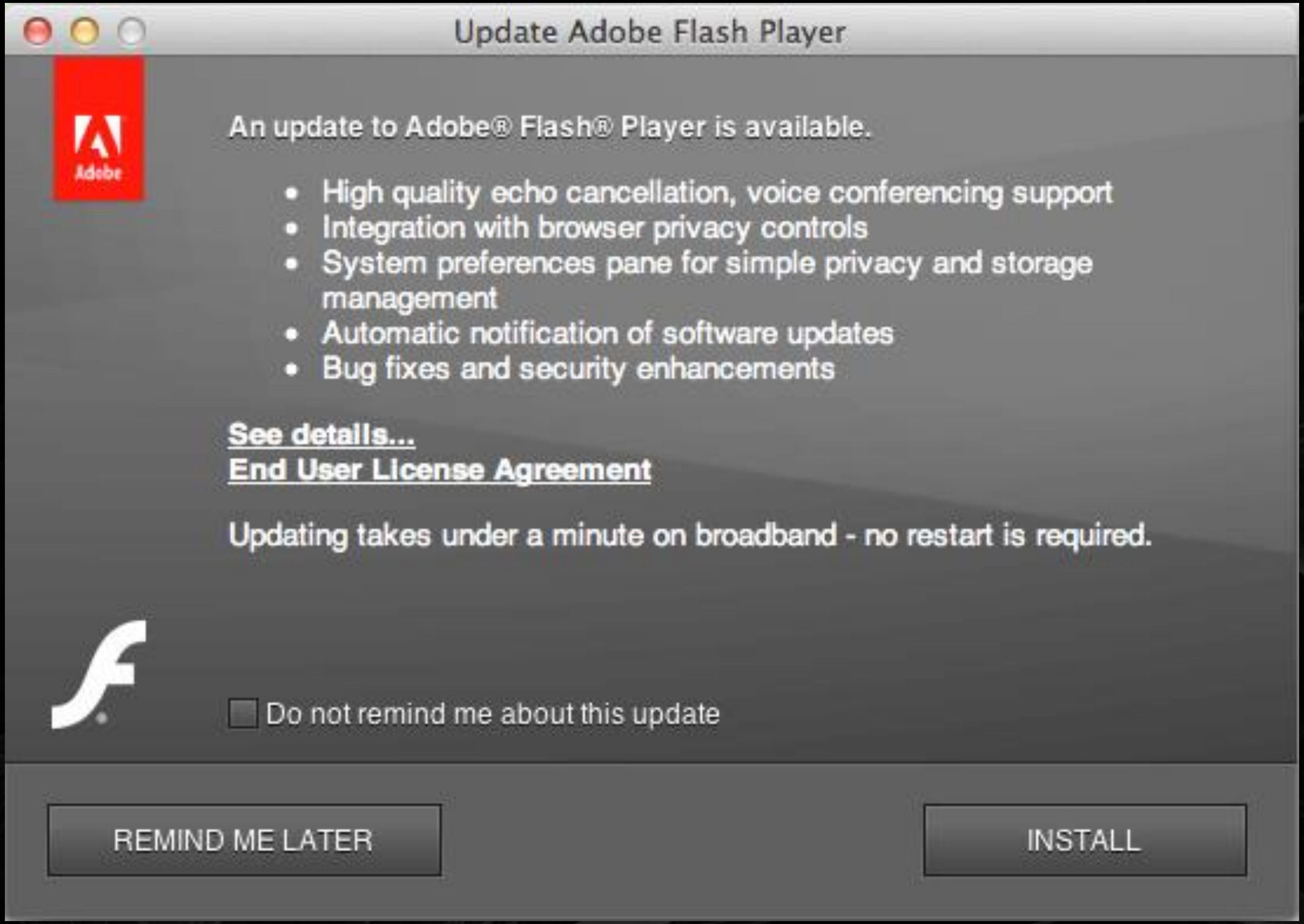
Microsoft Security Advisory: Vulnerability in Internet Explorer could allow remote code execution

From the Community

Vulnerability in Microsoft Word could allow remote code execution - Microsoft Community

Should I still use Internet Explorer now major security

Importance of patching



An update to Adobe® Flash® Player is available.

- High quality echo cancellation, voice conferencing support
- Integration with browser privacy controls
- System preferences pane for simple privacy and storage management
- Automatic notification of software updates
- Bug fixes and security enhancements

See details...
End User License Agreement

Updating takes under a minute on broadband - no restart is required.

☐ Do not remind me about this update

BEHIND THE WHEEL