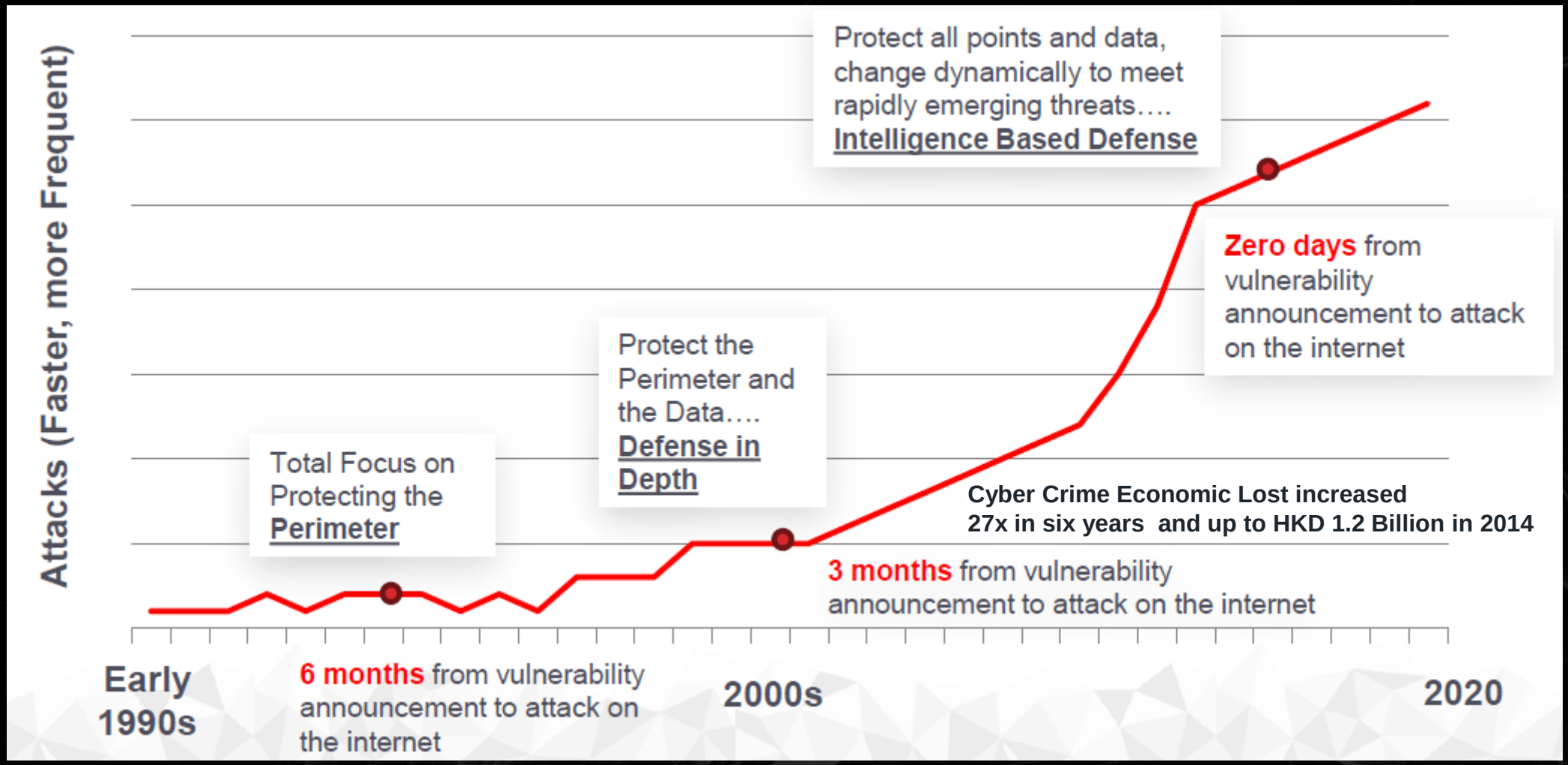
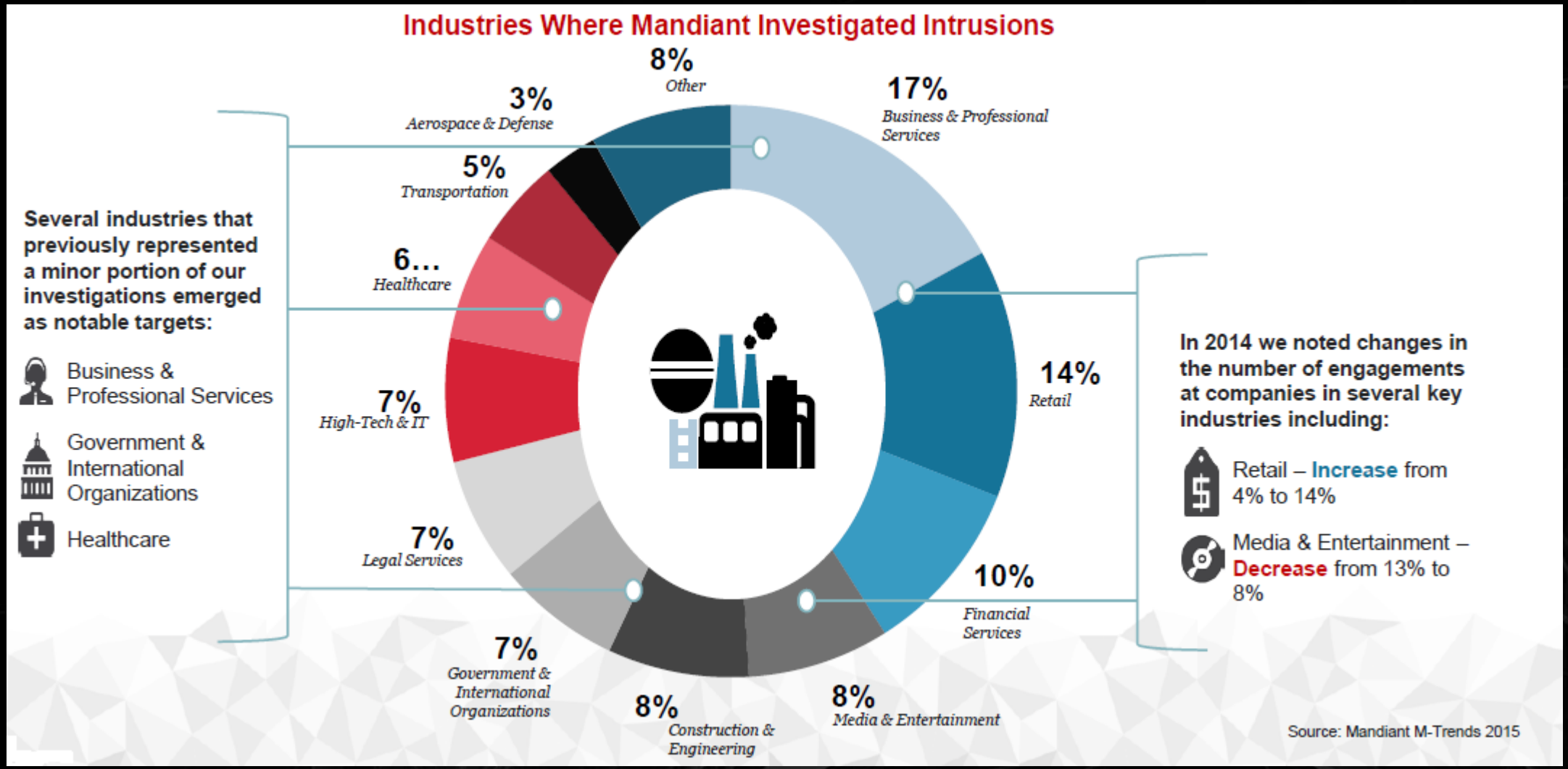
Targeted Attack on Enterprise

Matthew WONG
Consulting Systems Engineer, FireEye

Evolution of Cyber-Defense Strategies



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



Targeted Cybercrime Case Study

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

Subject: RE: PO 501410323 // CAPEX

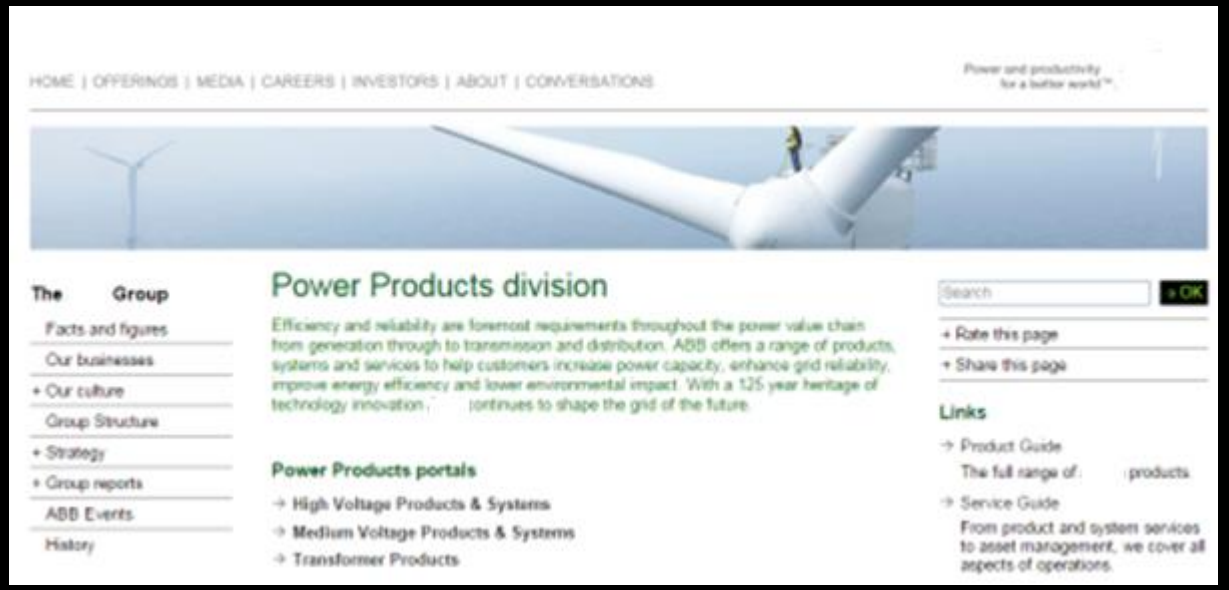
Dear:

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

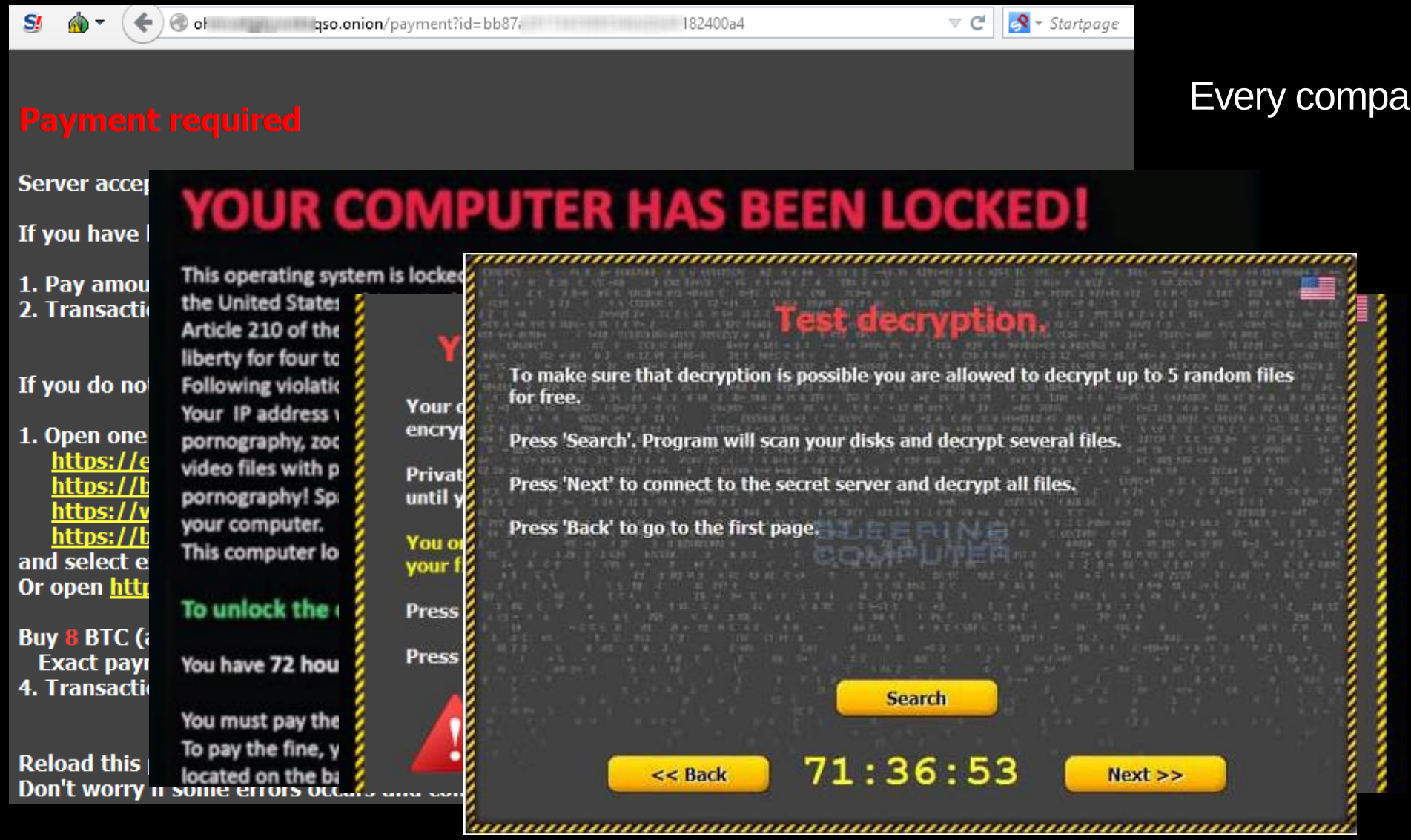
Best regards,

PO 501410323.rtf

Diana Rosales
Power Products
Phone: +51-1-4155100
ext. 1307
Telefax: +51-1-5613040
RPC: +51-1-954176723
email: diana.rosales@pe.com



CTB locker ransomware still very active



Every company is facing this problem

The basics

Attacker’s Goal: Issue instructions on the victim PC

The basics

Application

Document

Types of attack

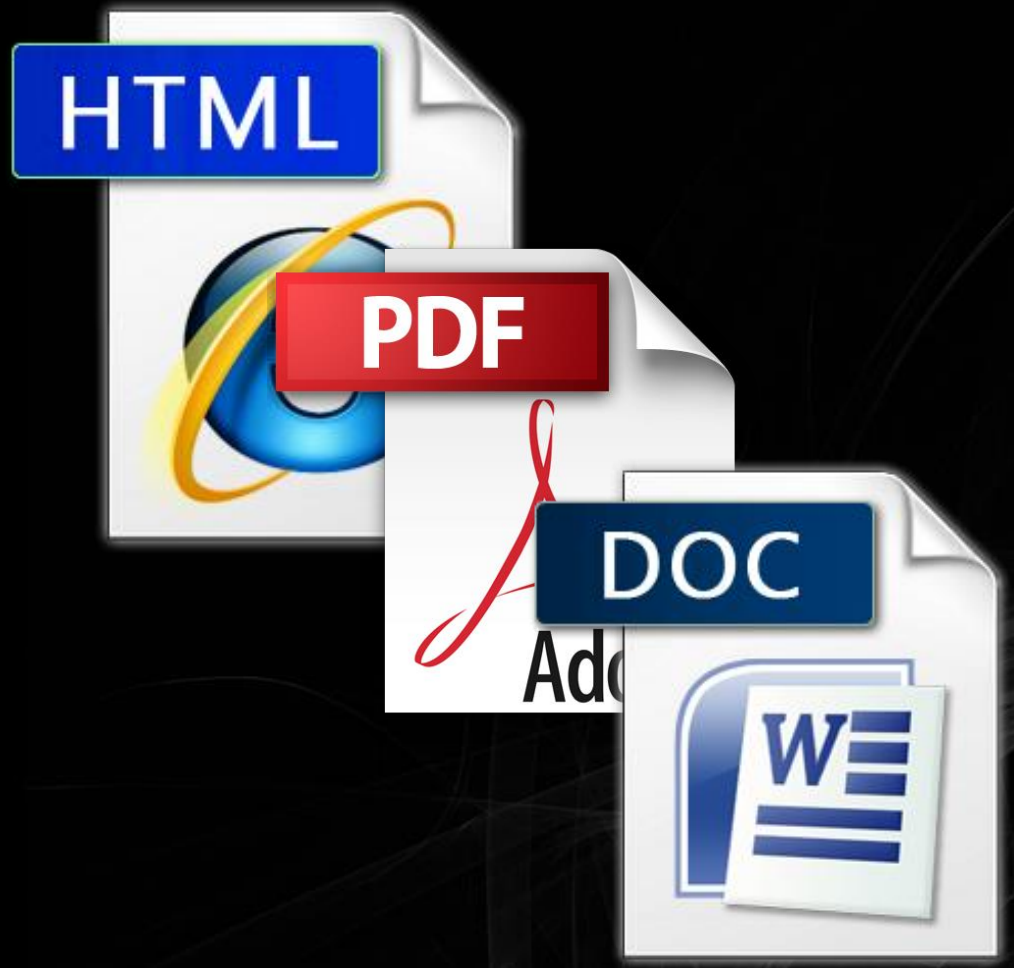
Fool the Human: Social Engineering

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
Support
My account
Sign in
By product
Downloads
Store
Contact us
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

BEHIND THE WHEEL