RESILIENT VERMONT

Cyber Security: A concern for all

NO LOCAL, INDUSTRY OR ORGANIZATION IS BULLETPROOF WHEN IT COMES TO THE COMPROMISE OF DATA.

(VERSION 2016 SECURITY REPORT)

TO START: SOME DEFINITIONS

- Malware: Short for malicious software, is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems , or display unwanted advertising. An umbrella term.

- Virus: A piece of code that is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

- Worm: A standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program.

- Trojan: any malicious **computer** program which misrepresents itself to appear useful, routine, or interesting in order to persuade a victim to install it. The term is derived from the Ancient Greek story of the wooden horse that was used to help Greek troops invade the city of Troy by stealth.

CLOUD COMPUTING: Cloud computing is a general term for the delivery of hosted services over the internet. Cloud computing enables companies to consume computer resources as a utility, just like electricity, rather than having to build and maintain computing infrastructures in-house.

Advantages

- Self-service provisioning: End users can spin up computing resources for almost any type of workload on-demand.
- Elastic: Companies can scale up as computing needs increase and then scale down again as demands decrease.
- Pay per use: Computing resources are measured at a granular level, allowing users to pay only for the resources and workloads they use
- Cloud computing services can be private, public or hybrid.

Disadvantages

- Legal issues with data retrieval: national and international law in regards to data acquisition and warrant responsiveness
- Multitenancy: leads to vulnerabilities. Virtual machines owned by separate parties have the same physical computing resources.
- Security, privacy and compliance: Security can be a concern in the cloud, particularly if you manage confidential data like customer information. Compliance in the cloud may be an issue, which may require deploying a private cloud if you have to secure private data.

Disaster Recovery: Lessons learned from Hurricane Irene

"No battle plan survives contact with the enemy."

German military strategist,
Helmuth von Moltke

NO ONE IS SAFE:

http://digital.vpr.net/post/email-and-website-hacks-show-vulnerabilities-vermont-towns-it

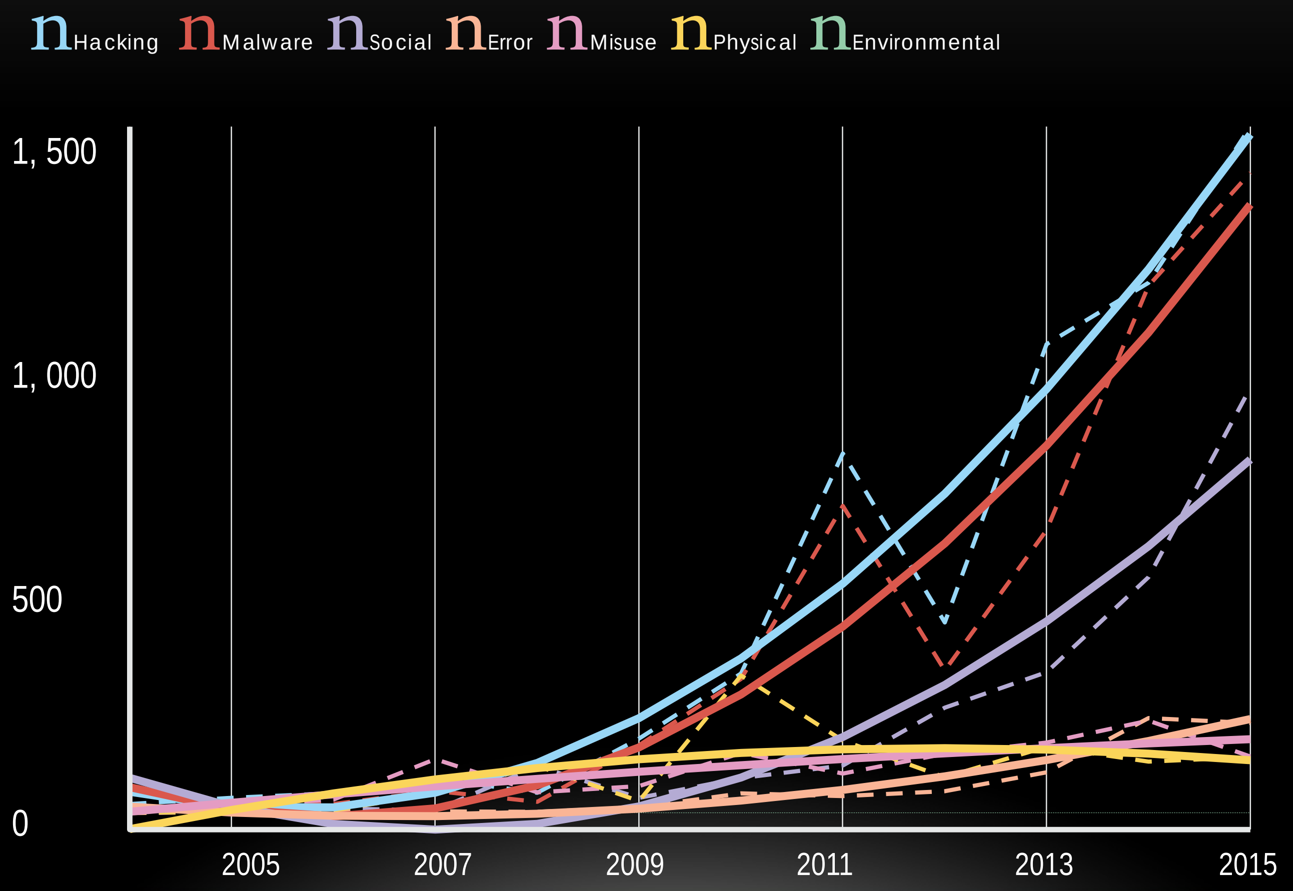
- Essex police investigate data breach
- *Posted: Apr 18, 2016 7:17 PM EDT* By WCAX News
- -
- ESSEX, Vt. - Essex police are investigating an email fraud that reportedly leaked personal information for hundreds of current and former town employees.
- On April 7 and 8, an unknown person sent fraudulent emails to the town of Essex, pretending to be an Essex town official. This email requested payroll records for all Essex town personnel. Mistakenly, town staff sent the requested payroll records.
- The fraud was discovered four days later when several town employees tried to file their taxes and found their accounts had been compromised.
- Officials say the records provided contained personal identifying information of 262 current and past staff members, including W-2 forms, phone numbers, date of birth and rate of pay information.
- Essex Police and the Vermont attorney general's office are investigating.

- Wilmington Town Website Infected By 'Alarming' Virus
- By Amy Kolb Noyes • May 3, 2016
- Wilmington residents looking for minutes and agendas of municipal meetings are being told not to look on the town website, www.wilmingtonvermont.us, at least for the time being. The site has been infected with a virus, and they're working to get to the bottom of it.

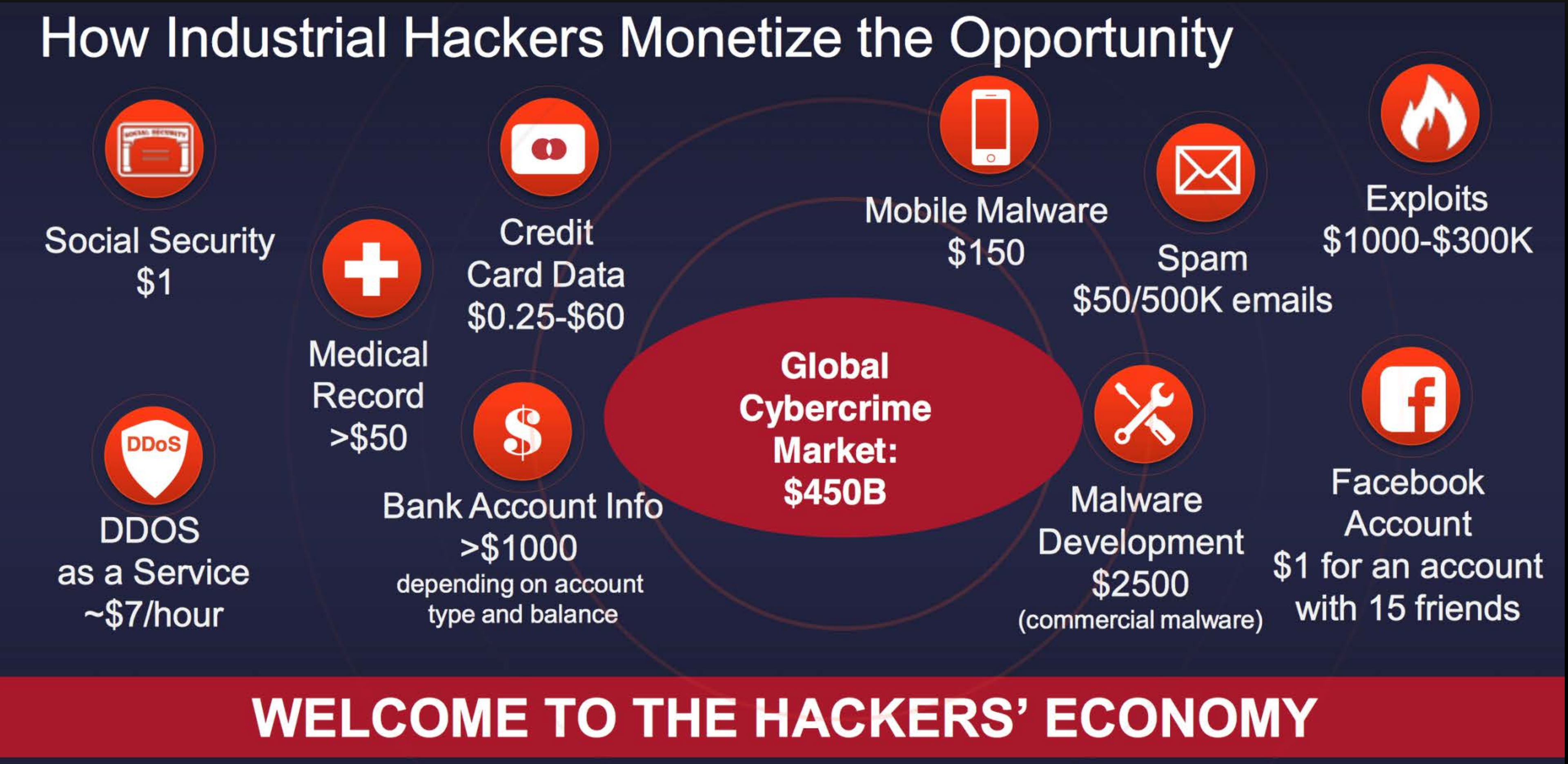
WHO IS AFTER YOU?

NUMBER OF BREACHES

2016 Version Report



“THE HACKERS ECONOMY”



How Industrial Hackers Monetize the Opportunity

Social Security
$1

Medical
Record
>$50

Credit
Card Data
$0.25-$60

DDOS
as a Service
~$7/hour

Bank Account Info
>$1000
depending on account
type and balance

Global
Cybercrime
Market:
$450B

Mobile Malware
$150

Spam
$50/500K emails

Exploits
$1000-$300K

Malware
Development
$2500
(commercial malware)

Facebook
Account
$1 for an account
with 15 friends

WELCOME TO THE HACKERS’ ECONOMY

Slide: Cisco, http://www.cisco.com/assets/global/GR/connect2014/pdfs/Cisco_Nikos_Mourtzinos.pdf

SO, WHAT ARE THESE ATTACKS?
THE TOP 3
1. SOCIAL ENGINEERING:

- Social Engineering: Social engineering in its basic form is simply to dupe or trick someone into doing something they would not otherwise do.
  - Phishing: (The Essex breach is an example of this.) is malicious correspondence trying to get the recipient to take the bait in the form of an attachment or embedded link. DO NOT CLICK ON THE LINK!!!
  - The median time for the first user of a phishing campaign to open the malicious email is 1 minute, 40 seconds. The median time to the first click on the attachment was 3 minutes, 45 seconds (Verizon 2016 Data Breach Investigation Report), thus proving that most people are clearly more on top of their email than I am.
- What to do?
  - Employee awareness and training programs
  - Implement strong authentication and network segmenting
  - Email filtering and monitor outbound traffic for potential exfiltration of data

2. RANSOMWARE: on the rise

- Ransomware is malware that encrypts files resident on the infected device and, in worst cases, attached file shares. Extortion demands follow, leveraging the need for availability of the data.

The top 5 malware vectors are:

1. Email attachment
2. Web drive-by
3. Email link
4. Download by malware: exploit known vulnerabilities
5. Network propagation

What to do:

1. Keep OS patches up to date!
2. Don’t allow programs to run scripts, have email remove file extensions as attachments in email.
3. Look at the different types of malware in your organization and, if possible, the entry point.

3. ADVANCE PERSISTENT THREAT (APT)

- What is it?
  - An advanced persistent threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time.
- Why do hackers use it?
  - The intention of an APT attack is to steal data rather than to cause damage to the network or organization. APT attacks target organizations in sectors with high-value information, such as national defense, manufacturing and the financial industry.
- How do they do it?
  - The goal is not to get in and out but to achieve ongoing access. To maintain access without discovery, the intruder must continuously rewrite code and employ sophisticated evasion techniques.
  - Use social engineering/spear phishing to gain access. The establish a back door.
- What to do?
  - APT attacks are difficult to identify. Detecting anomalies in outbound data is the best way for an administrator to discover that a network has been the target of an APT attack.

WHAT TO DO TO SECURE SYSTEMS

- Penetration testing
- Security awareness and training programs
- Double check links before clicking on them

PROPOSAL: TOWARDS A CYBER RESILIENT VERMONT

- Norwich University Centre for Advanced Computing
  - Cyber Threat Intelligence Centre

REFERENCES:

- http://www.techtarget.com/
- http://www.itbestofbreed.com/slide-shows/2016-verizon-report-10-must-know-security-trends-solution-providers/page/0/5?itc=refresh
- http://www.crn.com/slide-shows/security/300080475/2016-verizon-data-breach-investigations-report-10-security-trends-solution-providers-need-to-know.htm/pgno/0/9
- 2016 Data Breach Investigations Report (this is the full report) http://www.verizonenterprise.com/verizon-insights-lab/dbir/