CYBER 503x
Cybersecurity Risk Management

Unit 8: Special Topics

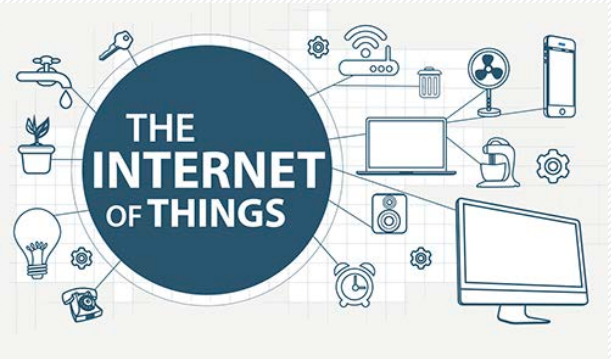
The Era of Internet:

Internet of Contents (WWW)

Internet of Services (Web2.0)

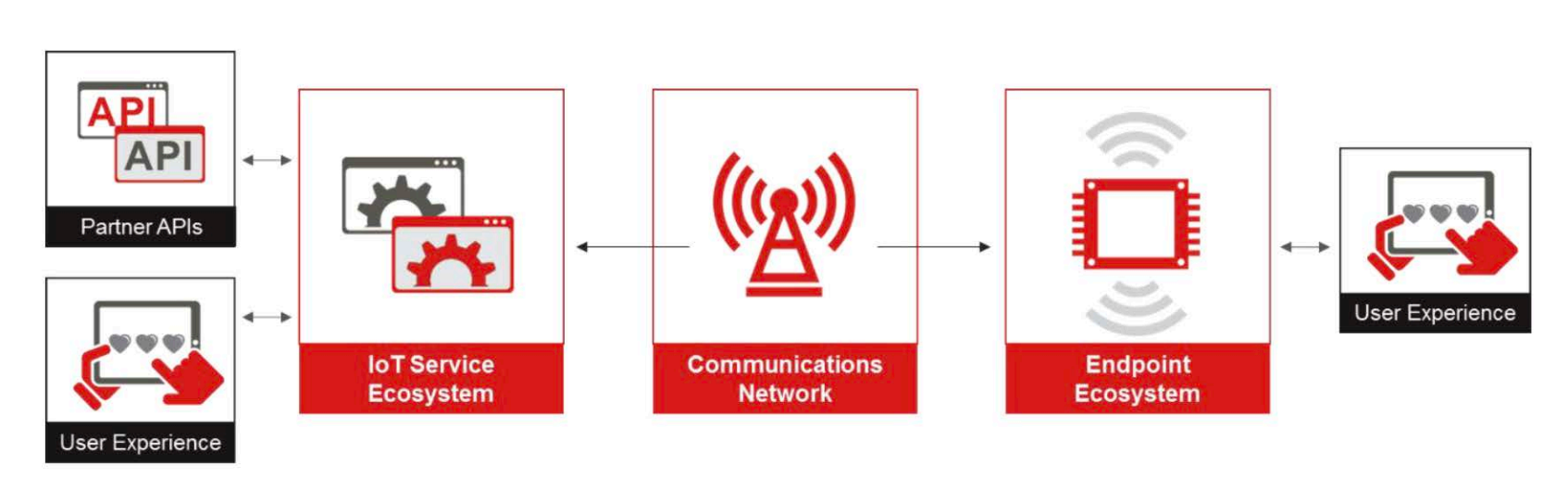
Internet of People (Social & Mobile)

Forecasts show an expected IoT universe with between 20 and 30 billion connected devices by 2020.



Case Study: WiFi Camera Vulnerabilities

IoT Ecosystem Model



IoT Security Guidelines Overview Document

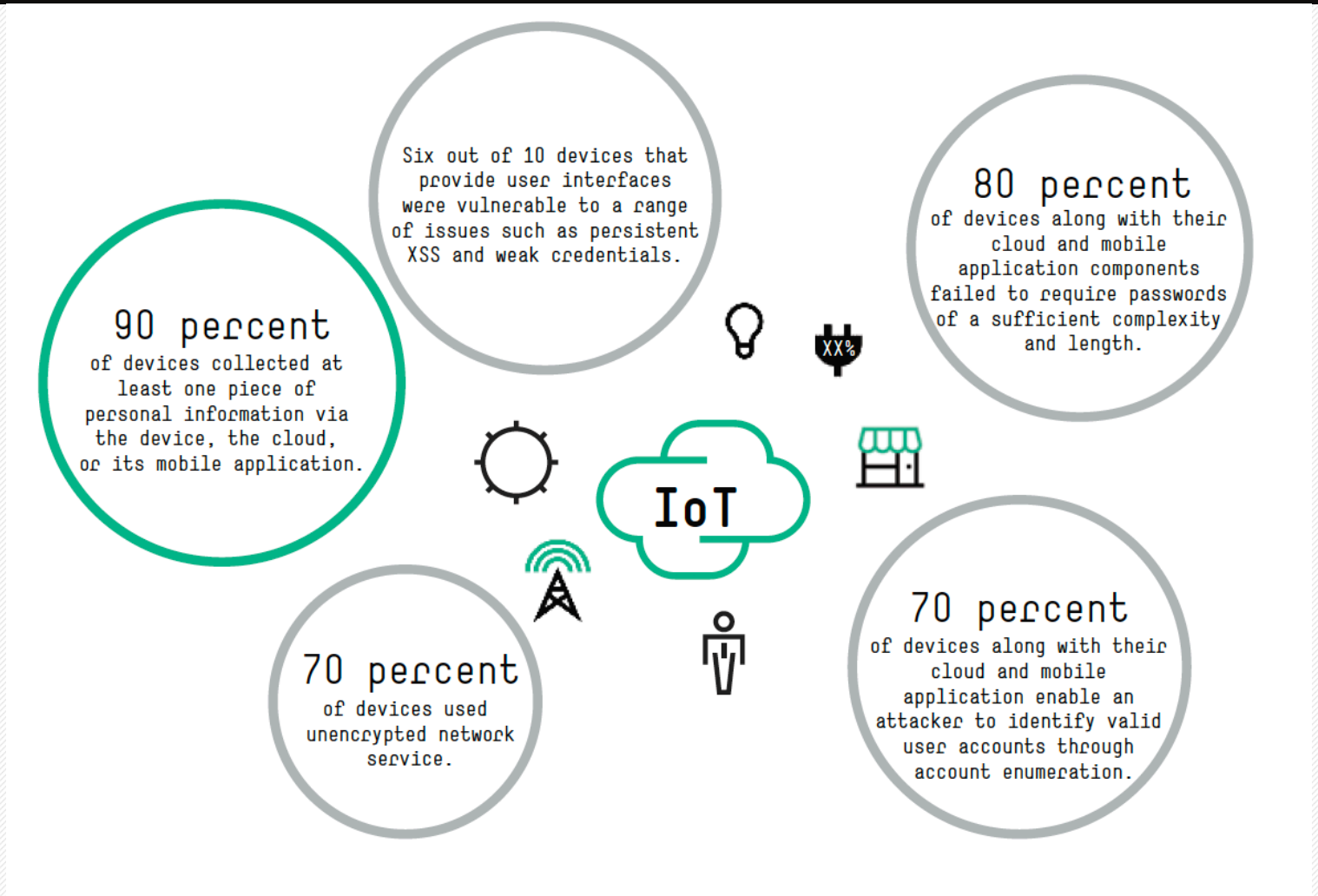
The IoT Security Pandemic

- What:
  - Millions of devices that have been or will soon be discovered, hacked, modified or hijacked
- Who is affected:
  - Enterprise, industrial, government, consumers
- Where:
  - Worldwide
- How:
  - Poor crypto practices
  - weak or non-existent firmware update practices
  - manufacturers in denial
  - limited regulatory oversight

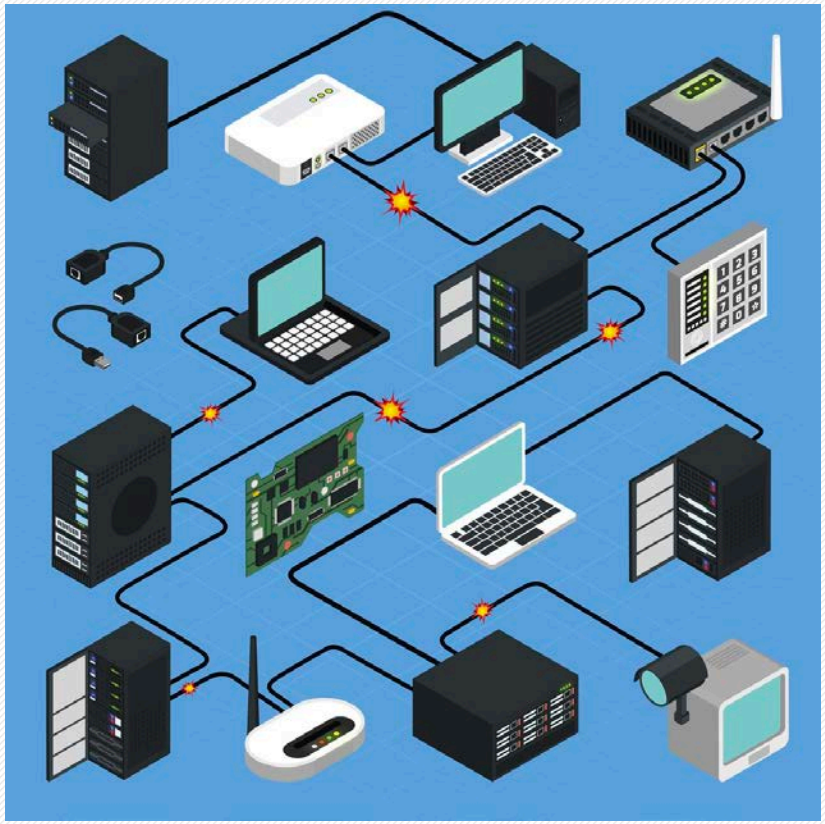
IoT Security! = Device Security

- Risks:
  - Disabled or hijacked world objects like Mirai
  - Modified endpoint data
  - Ransomware attacks
  - Spying
  - Homeland security
  - Personal safety

Research Findings by HP Internet of Things State of Union Study



Mirai Botnet: DDoS-for-hire Service



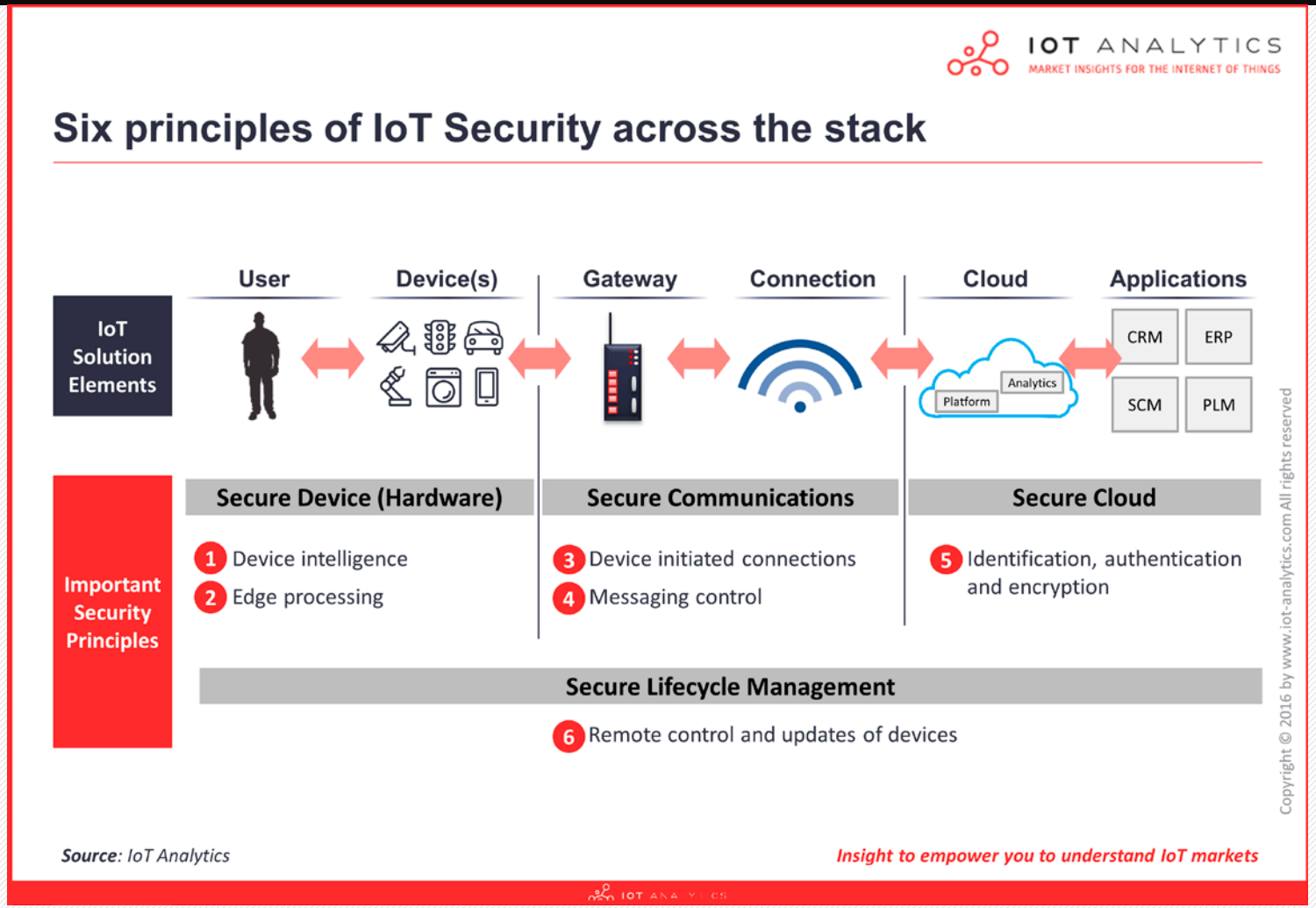
- Internet of Botnet malware: reminiscent of viruses, worms, and intense email spam that plagued early internet uses
- One important distinction: less user interactions with IoT devices, not easy to detect, hard to kill
- Mirai isn’t the only IoT botnet, but very accessible and adjustable
- It is certainly not going away any time soon

Case Study: DDoS (Distributed Denial of Service) attack on Dyn Servers

Key Findings

- The Dyn servers' attack has been analyzed as a complex & sophisticated attack, using maliciously targeted, masked TCP and UDP traffic over port 53.
- Dyn confirms Mirai botnet as primary source of malicious attack traffic.
- Attack generated compounding recursive DNS retry traffic, further exacerbating its impact.
- Attacker is likely tied to an amateur Hacking Forum Community, which is neither state-sponsored, nor financially motivated.

Six Principles of IoT Security Across the Stack



Hurdles Securing the IoT

- There is no consistent or official software update process or mechanism
- There is little or no understanding of the cyber threats embedded in their systems
- There is lack of accountability for device security
- Improper configuration or purpose-built features that equate to security flaws
- Data privacy

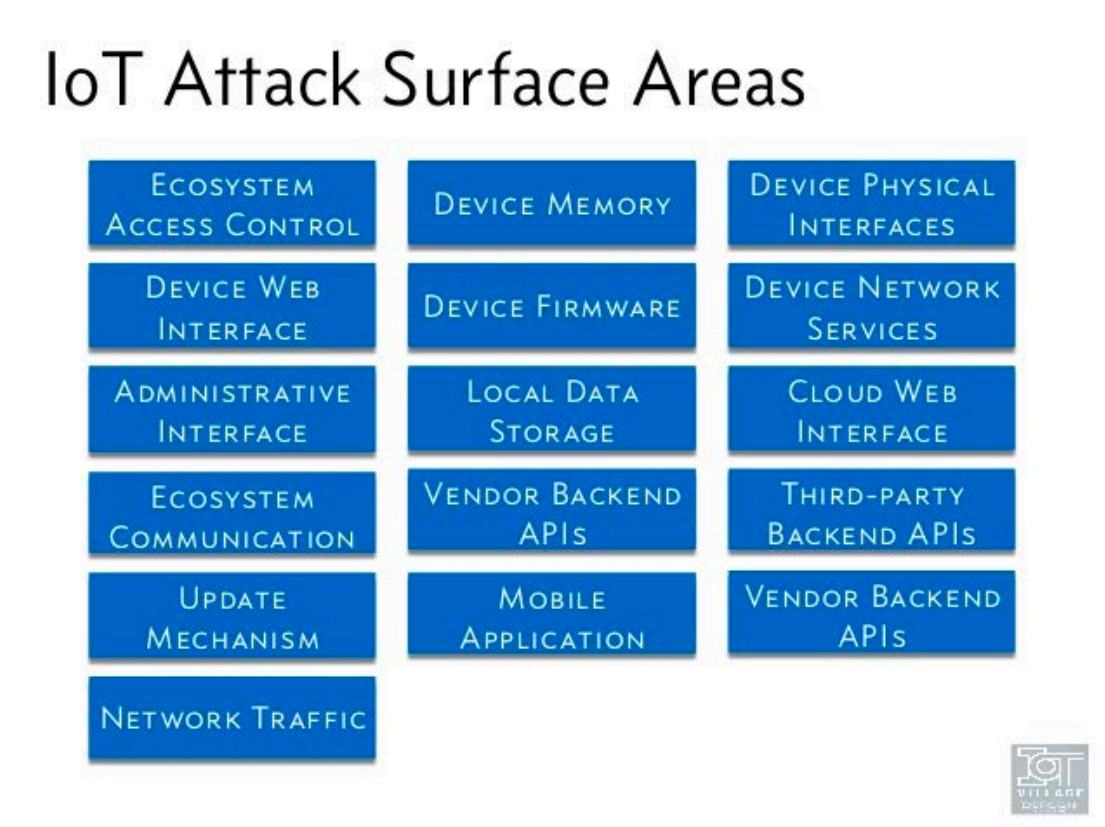
Practical IoT Security Assessment

- Define system scope for assessment
- Understand designs and technical capabilities
  - Device component, communication protocols, the end-to-end system
- Model threats & resilience expectations
  - Device level (data storage, firmware), connection levels and system level
- Model traffic flow and trust boundaries
  - On device, Device to System – traffic, System – data and functionality
- Assess:
  - Review configuration, standard app/product assessment, debug and vulnerability test tools, code review

Securing the IoT

- Keep your software/firmware updated
- Ensure that connectivity is secure (e.g. Two factor authentication)
- Secure the location of data being reported by IoT-linked devices
- Ensure supply chain security
- Support IoT Security
- Use out of band (OOB) systems – closed systems (intranets) that are not open to the public
- Stay Informed

Securing the IoT: support standardization & Best Practices (e.g. OWASP – Open Web Application Security Project)



IoT Surface Area: Ecosystem Access Control

- Authentication
- Session management
- Implicity trust between components
- Enrollment security
- Decommissioning syste,
- Lost access procedures

IoT Surface Area: Device Memory

- Cleartext usernames
- Cleartext passwords
- 3rd-party credentials
- Encryption keys

IoT Surface Area: Device Firmware

- Hardcoded passwords
- Sensitive URL disclosure
- Encryption keys

IoT Surface Area: Web Cloud Interface

- SQL injection
- Cross-site scripting
- Username enumeration
- Weak passwords
- Account lockout
- Known credentials

IoT Surface Area:
Device Network Services

- Information disclosure
- User Command Line Interface (CLI)
- Administrative CLI
- Injection
- Denial of Service

IoT Surface Area: Local Data Storage

- Unencrypted data
- Data encrypted with discovered keys
- Lack of data integrity checks

IoT Surface Area: Vendor Backend APIs

- Unencrypted Personal Identifiable Information (PII)
- Encrypted PII sent
- Device information leaked
- Location leaked
- Inherent trust of cloud or mobile application
- Weak authentication & access control

IoT Surface Area: Update Mechanism

- Update sent without encryption
- Updates not signed
- Update location writable

IoT Surface Area: Network Traffic

- LAN (Local Area Network)
- LAN to Internet
- Short range
- Non-standard

Examples: Mapping Attack Surfaces to Vulnerabilities and to Data Asset

Attack Surface Areas	Vulnerability	Data Asset
Administrative interface	• Weak password policy • Lack of account lockout	• credentials
Local data storage	• Data stored without encryption	• PII
Web cloud interface	• SQL Injection	• PII • Account data
Device Firmware	• Sent over HTTP • Hardcoded passwords • Hardcoded encryption keys	• Credentials • Application data
Vendor backend APIs	• Permissive API Data Extraction	• PII • Account data

What is Ransomware?

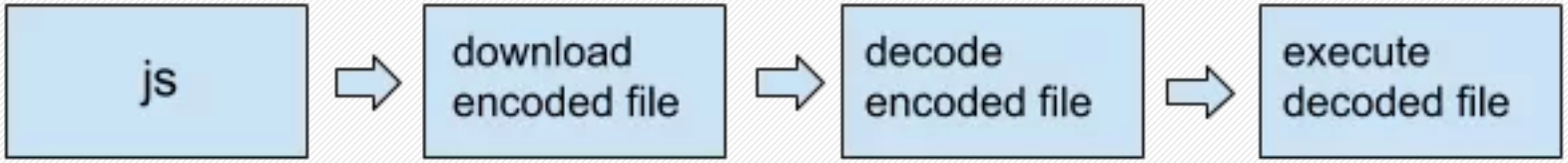
- The term comes from “ransom” and “software”.
- A type of computer virus that attacks the “Availability” aspect of InfoSec C.I.A model.
- Often through email phishing scheme.
- Average ransom demand for consumers and small business owners is $300 to $500.

“Locky” Ranswomware – How does it work?

- The common way that Locky arrives as following:
  - You receive an email containing an attached document (Troj/DocDl-BCF)
  - The document advises you to enable macros “if the data encoding is incorrect”
  - If you enable macros, you don’t actually correct the text encoding; instead you run code inside the document that saves a file to disk and runs it.
  - The saved file (Troj/Ransom-CGX) serves as a downloader, which fetches the final malware payload from the attackers.
  - The final payload could be anything, but in this case is usually the Locky Ransomware.

“Locky” Ransomware variation– yet another new attack scenario (reported in June 2016)

- The steps of a “Locky” Ransomware attack:
  - Spam email & zip archive attachment.
  - The Javascript file



- The Locky Binary – the distinct behavior syscall patterns
  - Delete shadow copies
  - Drive enumerations
  - Files enumeration
  - Encryption routine

Why are Ransomware surging?

- Phishing emails – the human factor
  - Blanket phishing
  - Spear phishing
  - Whaling
- Access to the digital currency Bitcoin

Healthcare – Especially Vulnerable to Ransomware Attacks

- Health information is intensely personal and universal
- Health IT- legacy systems, outdated protective measures
- Near exclusive focus on safeguarding data only; but the reality tells – it should be more than that
- “Health systems have the money and they are willing to pay …”, one CSO of Health System said.

Ransomware Case 1: Hollywood Presbyterian Medical Center

- Hit by the “Locky” ransomware in Feb 2016
- Likely the attack occurred because an employee mistakenly clicked on an email attachment that was actually a phishing scam
- Soon the hospital was crippled by unable to access the network; doctors unable to access patient’s medical histories etc..
- Response actions:
  - Internal emergency was declared and the computer system taken offline
  - Some patient diverted to nearby hospital
  - Resort to doing patient admissions and other record-keeping by pen & paper
- Eventually paid $17,000 (about 40 BCT then) to get their records back

Ransomware Case 2: WannaCry

- In May 2017, a worldwide cyber attack named “Wannacry” – the worst ransomware
- Affected victims:
  - More than 230,000 users in some 150 counties
  - NHS in UK, Telephonica, FedEx operations, etc.
- Ransom demanded:
  - $300 in BCT for each affected user

Ransomware Case 2: WannaCry

- Vulnerability it exploited:
  - Microsoft Windows XP
- Other Risks revealed:
  - A leaked NSA hacking tool, that had been obtained and posted online last year by Shadow Brokers, is at the base of WannaCry
- Likely attacker profile:
  - NSA has linked the WannaCry computer worm to North Korea – but not conclusive yet

What to do to ensure the readiness for Ransomware?

- Train your users
- Anti-spam tools (but less effective against spear phsihing)
- Conventional security measures
  - Backup regularly and keep a recent backup copy off-site
  - Business continuity procedures in place
  - Patch early, patch often
  - Segment the network
  - Principle of least privilege
  - Application whitelistings

Building Risk Resilience:
Beyond protection, detection, and prevention

Every control will fail

Cyber attacks: it's not a question of if, but when?

- Incident Response Planning (IRP)
- Disaster Recovery Planning (DRP)
- Business Continuity Planning (BCP)

Incident Response & Disaster Recovery

- Incident response plan – a plan to follow during the incident to mitigate, reduce and contain the damage
  - It ties strongly with monitoring and detection
- Disaster recovery plan - a plan that hopefully allows the business to recover from damages after the incident has occurred
  - It is designed to reduce decision-making activities during a disaster mode.

Business Continuity & Disaster Recovery

- BCP – planning to continue your key business operations to minimize risks
  - It does NOT seek to detect or prevent every possible disaster
  - Business-focused
- DRP – planning to recover from disaster situations
  - When in the disaster mode, it guides the actions of emergency-response team until the end goal is reached (i.e. the business restored to full operating capacity in its primary facilities)
  - IT-focused

Example: Locky Ransomware Case – How to plan ahead?