

Defending Your Organization Against Cyber Thugs

Lee Painter, Principal
Cybersecurity
CliftonLarsonAllen
CISSP, CRISC, HCISPP, CCSFP

IGFOA ANNUAL CONFERENCE • SEPTEMBER 8-10, 2019



What do the following have in common?

Date Made Public	Company	Type of breach	Total Records
22-May-18	Golden 1 Credit Union	HACK	500
20-Apr-18	SunTrust Banks, Inc.	HACK	1,500,000
26-Feb-18	Southern National Bancorp of Virginia, Inc. d/b/a/ Sonabank	HACK	24,999
5-Feb-18	1st Mariner Bank	HACK	1,500
5-Jan-18	RBC Royal Bank	HACK	66,000
29-Mar-17	CFG Community Bank	HACK	155

- All reported breaches within the past 12 months

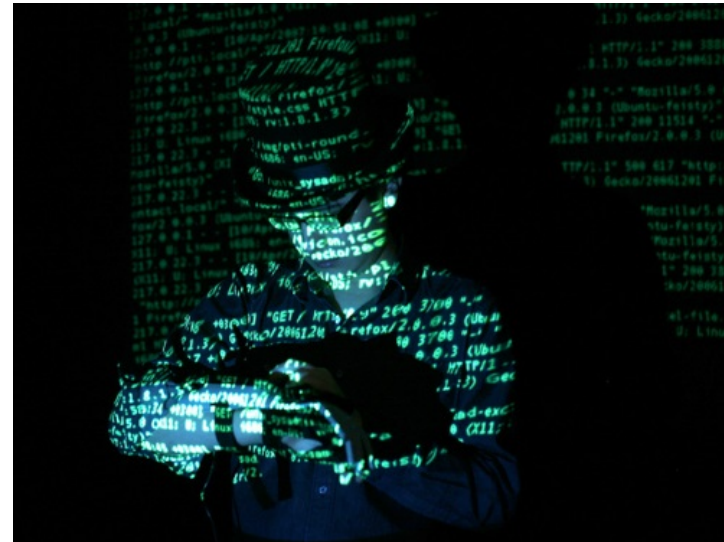
Cyber Fraud Themes

- Hackers have “monetized” their activity
 - More sophisticated hacking
 - More “hands-on” effort
 - Smaller organizations targeted
 - Cybercrime as an industry
- Everyone is a target...
- Phishing is a root cause behind the majority of cyber fraud and hacking attacks



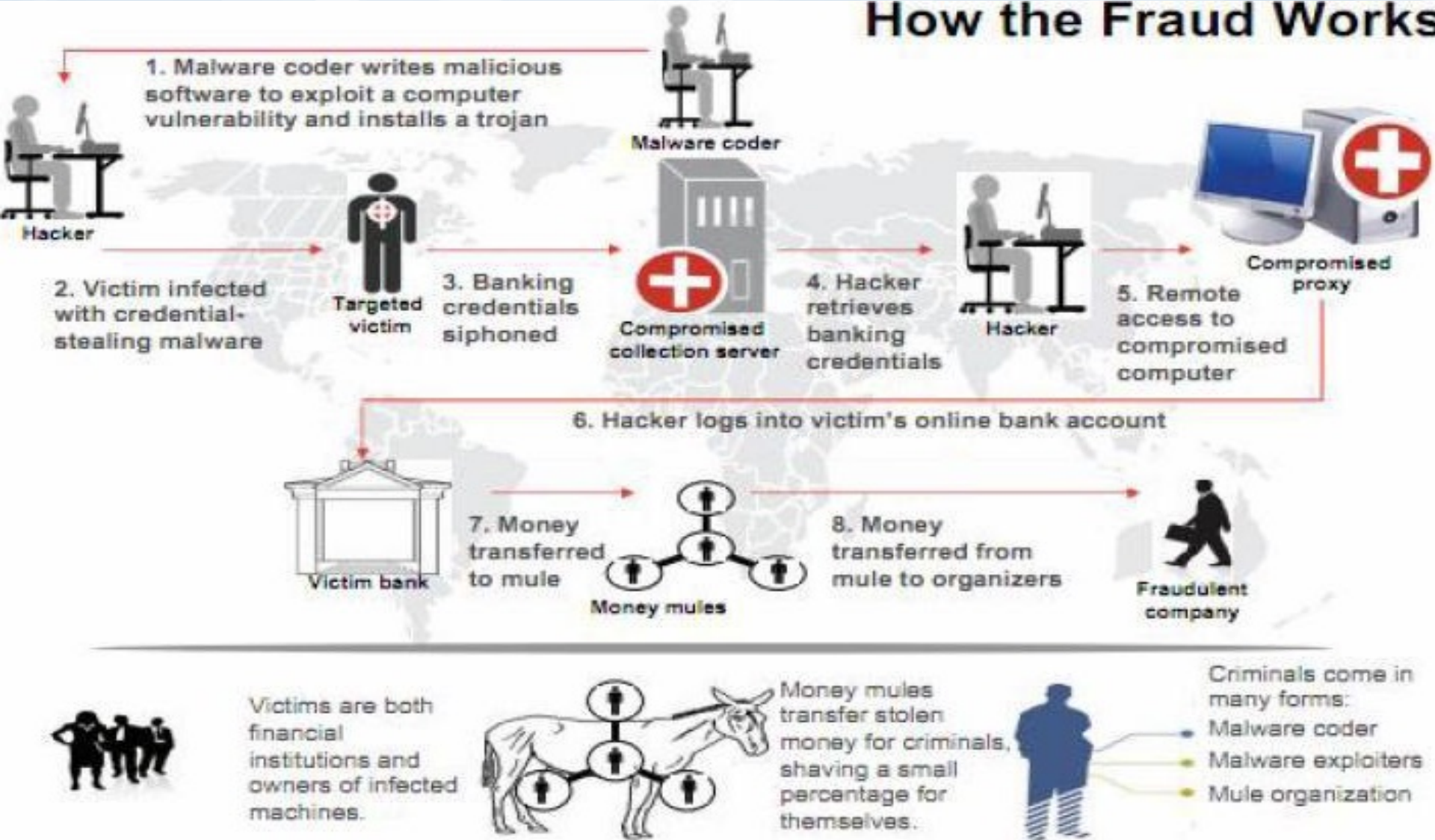
Largest Cyber Fraud Trends - Motivations

- Black market economy to support cyber fraud
 - Business models and specialization
- Most common cyber fraud scenarios we see affecting our clients
 - Theft of PII and PFI
 - W2/Payroll/Benefit info
 - Theft of credit card information
 - Account take overs
 - Ransomware and Interference w/ Operations



Specialization

How the Fraud Works



Marketplace for Stolen Information

- Attackers buy and sell data on cyber black market
 - “The Dark Web” - Similar to amazon.com

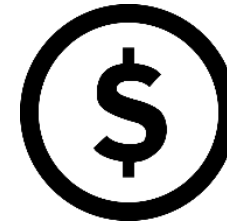
Home Buy CC CC Orders Buy Dumps Dump orders Checker Tickets Hello, [redacted] Cart (1) 9.45\$ Balance: 3.0\$ Add money Replace policy Logout

101 201

Didn't find the bin you were looking for? Need more dumps of particular bin? Try our partner's shop - [Bulk Orders - Low Prices!](#) Clear Search

<input type="checkbox"/>	Bin	Card	Debit/Credit	Mark	Expres	Track 1	Code	Country	Bank	Base	Price	Cart
<input type="checkbox"/>	371736	AMEX	CREDIT		07/15	Yes	110	United States, 23456, Virginia Beach, VA	BANK OF AMERICA	American Sanctions 14	30\$	+ <input type="button" value=""/>
<input type="checkbox"/>	371555	AMEX	CREDIT		09/16	Yes	101	United States, 80123, Littleton, CO	BANK OF AMERICA	American Sanctions 14	30\$	+ <input type="button" value=""/>
<input type="checkbox"/>	371736	AMEX	CREDIT		03/17	Yes	101	United States, 60540, Naperville, IL	BANK OF AMERICA	American Sanctions 14	30\$	+ <input type="button" value=""/>
<input type="checkbox"/>	371564	AMEX	CREDIT		05/15	Yes	110	United States, 77081, Houston, TX	BANK OF AMERICA	American Sanctions 14	30\$	+ <input type="button" value=""/>
<input type="checkbox"/>	371554	AMEX	CREDIT		04/17	Yes	101	United States, 37027, Brentwood, TN	BANK OF AMERICA	American Sanctions 14	30\$	+ <input type="button" value=""/>
<input type="checkbox"/>	371242	AMEX	CREDIT	GREEN	06/17	Yes	101	United States, 98512, Olympia, WA	AMERICAN EXPRESS COMPANY	American Sanctions 14	30\$	+ <input type="button" value=""/>
<input type="checkbox"/>	371570	AMEX	CREDIT		10/16	Yes	101	United States, 97123, Hillsboro, OR	BANK OF AMERICA	American Sanctions 14	30\$	+ <input type="button" value=""/>
<input type="checkbox"/>	371381	AMEX	CREDIT		10/16	Yes	201	United States, 30328, Atlanta, GA	CITIBANK Dump or cc of this particular bank (BIN)	American Sanctions 14	24\$	+ <input type="button" value=""/>

The Cost



Global cybercrime cost businesses up to:
\$600 BILLION annually

Some estimate it will reach:
\$6 TRILLION by 2021

Payment Fraud

- Most people interact with their CU electronically
 - Wire transfers & ACH payments
 - Online banking
 - Member/business banking
- Account Take Over (CATO)
 - Compromise accounts/credentials that can move money

What Makes Social Engineering Successful?

“Amateurs hack systems, professionals hack people.”

Bruce Schneier

Social Engineering relies on the following:

- The appearance of “authority”
- People want to avoid inconvenience
- Timing, timing, timing...



<https://www.youtube.com/watch?v=jwqV5L9fr60>



Pre-text Phone Calls (Phishing by phone)

- “Hi, this is Randy from Comcast Business users support. I am working with Dave, and I need your help...”
 - Name dropping → Establish a rapport
 - Ask for help
 - Inject some techno-babble
- “I need you to visit the Microsoft Update site to download and install a security patch. Do you have 3 minutes to help me out?”
- Schemes result in losses from fraudulent ACH transactions,...



Physical (Facility) Security

Compromise the site:

- “Hi, Sally said she would let you know I was coming to fix the printers...”

Plant devices:

- Keystroke loggers
- Wireless access point
- CDs or Thumb drives



Strategies to Combat Social Engineering

- (Ongoing) user awareness training
- CIS 20 “First Five” – Layers “behind the people”
 - Inventory of Authorized and Unauthorized Devices
 - Inventory of Authorized and Unauthorized Software
 - Secure/Standard Configurations for HW & SW(hardening)
 - Continuous Vulnerability Assessment and Remediation
 - **Controlled Use of Administrative Privileges**
- VALIDATION → Periodic testing
 - People, Rules, Tools, and Spaces

Email Phishing Objectives

Goals:

- Gain access to network resources, financial accounts, or business email account (BEC)
- Convince target to do something

Malware infection via:

- Links to malicious website containing drive-by malware
- Email Attachments (ZIP, RAR, HTA, JAR, etc....)
- Downloading malware from a website

Gain information by:

- User credentials submitted into a compromised website
- Ask the user

Types of Email Phishing

Traditional Email Phishing

A hacker sends an email to a large number of people (from hundreds to millions), hoping a few will take the bait.

Spear Phishing

A specific target is identified and a custom message is sent.

Whaling and Persuasion Attacks

A specially crafted message is sent to the executives or upper management of a business.

Spear Phishing Success Factors

- With so much money at stake hackers are putting in more effort to increase the likelihood that the emailed link will be followed:
 - “Spoof” the email to appear that it comes from someone in authority
 - Create a customized text that combines with the spoofing to create pressure to act quickly (without thinking)

Persuasion Attacks

- CEO asks the CFO...
- Common mistakes
 1. Use of private email
 2. "Don't tell anyone"

- <http://www.csoonline.com/article/2884339/malware-cybercrime/omahas-scoular-co-loses-17-million-after-spearphishing-attack.html>

Omaha's Scoular Co. loses \$17 million after spearphishing attack

Fraudsters convinced an Omaha company to send \$17.2 million to a bank in China



By [Maria Korolov](#) | [Follow](#)

CSO | Feb 13, 2015 4:20 PM PT

Fraudsters targeting an Omaha company last summer used extremely well-targeted emails to convince its controller to send a series of wires totaling \$17.2 million to a bank in China.

First, there were emails, supposedly from the CEO, saying that Scoular was buying a company in China. The emails weren't from the CEO's official email address, and, moreover, warned the controller not to communicate about the deal through other channels "in order for us not to infringe SEC regulations."

The emails also instructed the controller to get the wire instructions from an actual employee of the company's actual accounting firm, KPMG. Plus, the phone number provided in the email was answered by someone with the right name.

[MORE ON CSO: How to spot a phishing email](#)

Since Scoular was, in fact, discussing expanding in China, the controller fell for the emails and sent off the money.

Ransomware

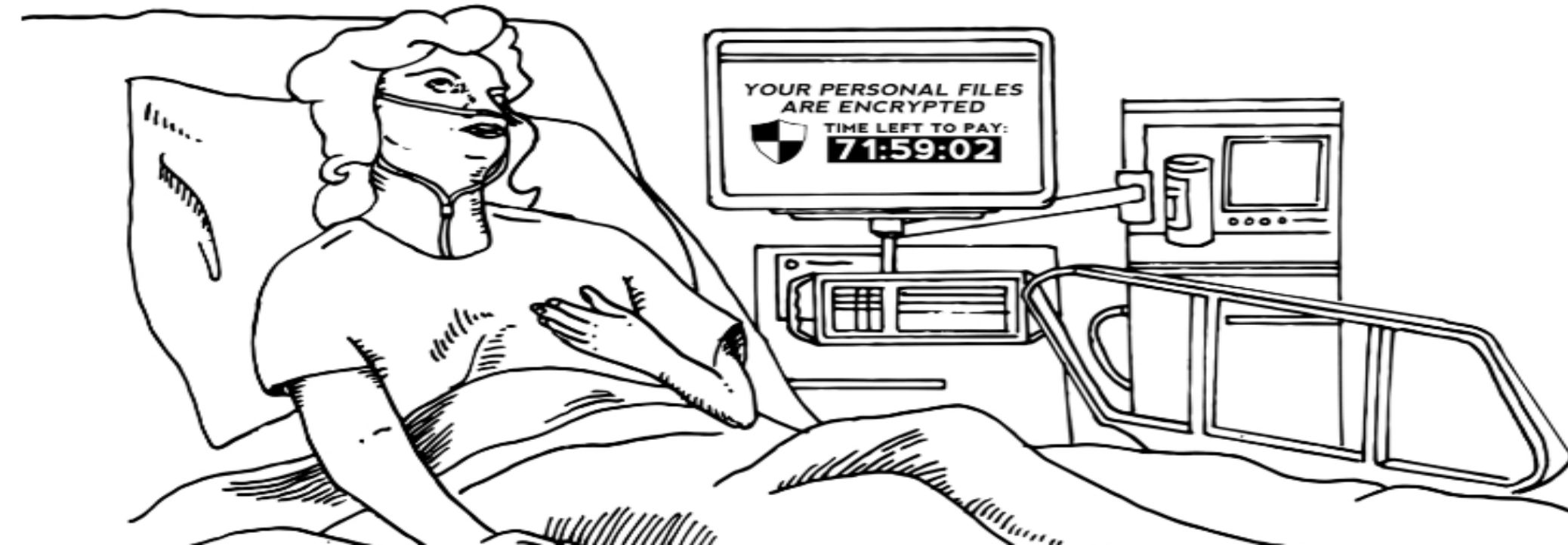


- Cryptolocker, Locky, WannaCry, etc.
- Encrypts all data, holds in “ransom” for \$\$
 - Data on local machine and on network
 - System files and back up files
- Can affect non-Windows OS (e.g. Mac)
- Starting to see BEC and compromised RDP as the “entry point”

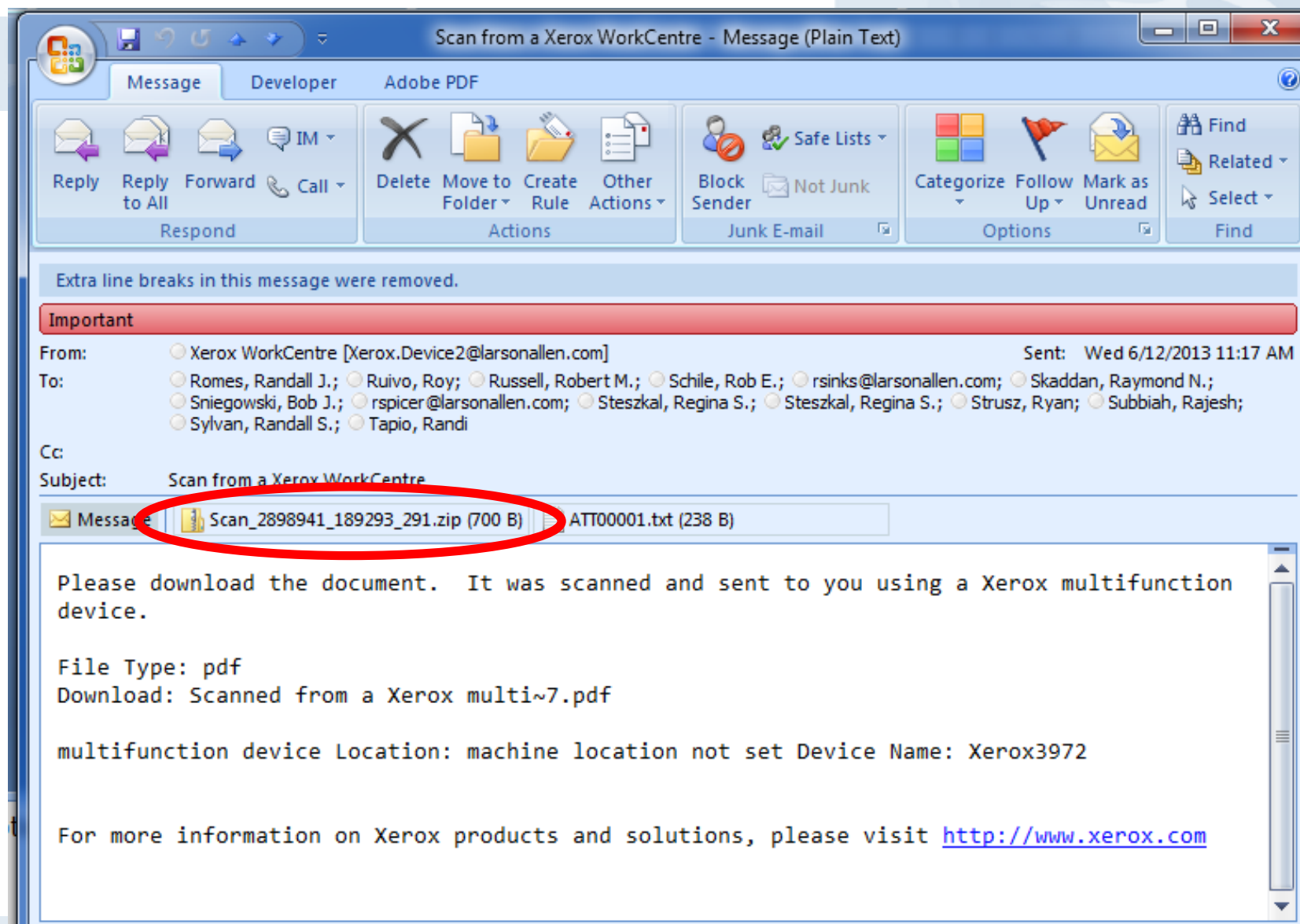
Ransomware

Hospital ransomware: A chilling wake-up call

Hollywood Presbyterian was forced to pay up, just like everyone else.

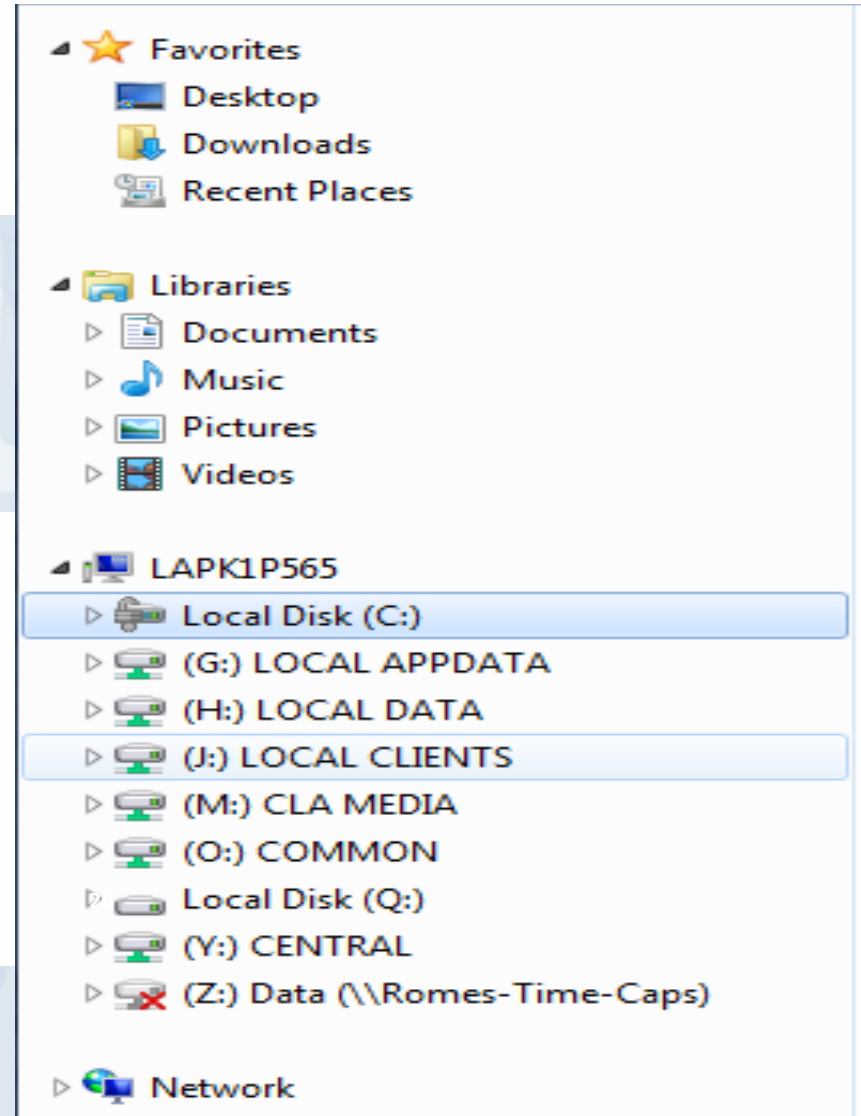


Ransomware



Ransomware

- Malware encrypts everything it can interact with



Ransomware Defensive Strategies

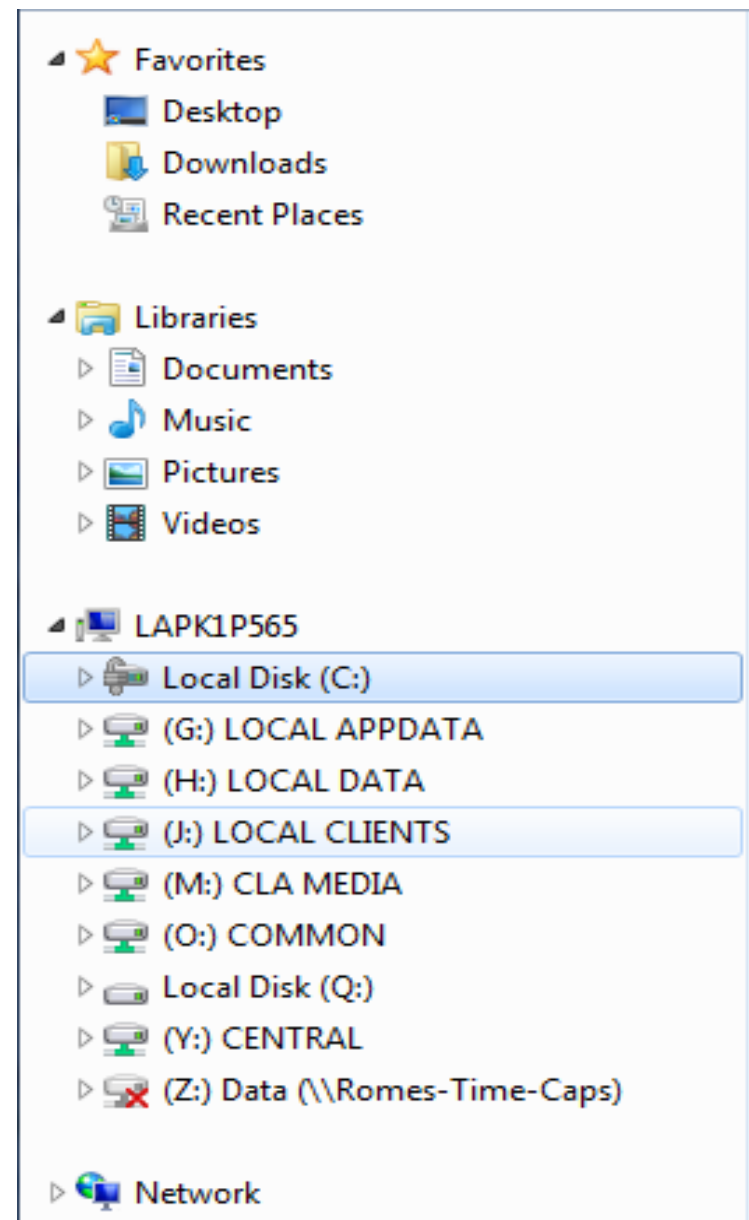
- Filtering capabilities
 - Removal of Ad's - web proxy
- Users that are aware and savvy
 - Benefits of “Phishing services”

21



Defensive Strategies

- Current Operating Systems
- Updated Security Patches***
- Working backup and restore capabilities



Ransomware Safeguards

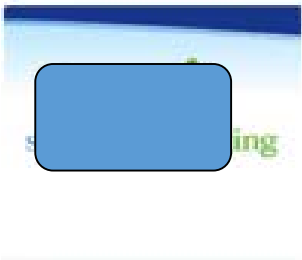



- Audit file permissions where backups are stored.
 - Identify which users could encrypt backups if they were to become infected.
 - Storage location of back ups should be very restrictive – read only access even for most administrators.
 - Backups should be done with a service account.
 - You could also restrict the backup network access temporally similar to a bank vault.
 - That could be done with a simple script that would disable the port during the day and then re-enable just before the backup starts.

Performing Reconnaissance

Secure <https://www.linkedin.com/company-beta/71555515/>

in Search Home My Network Jobs Messaging Notifications

 **Group**
Hospital & Health Care • 51-200 employees • CA

 1 person from your school was hired here. [See all 51 employees →](#)

[See jobs](#) [Follow](#) 56 followers

PREMIUM
▲ 17% change in the Accounting function in the last 6 months. [Get the full picture](#)

Performing Reconnaissance

Showing 428 results



William Murray, CPA • 2nd
Principal at CliftonLarsonAllen
Cedar Rapids, Iowa Area
Current: ...CliftonLarsonAllen (CLA... cliftonlarsonallen.com.



18 shared connections

[Connect](#)



Alex Hengel • 2nd
CPA, Senior at CliftonLarsonAllen
St. Cloud, Minnesota Area
Current: Senior at CliftonLarsonAllen



11 shared connections

[Connect](#)



Bill Vincent, CPA • 2nd
Principal at CliftonLarsonAllen LLP
Cedar Rapids, Iowa Area
Current: Principal, CPA at CliftonLarsonAllen



6 shared connections

[Connect](#)



Jo Eyberg, CPA • 2nd
Partner - Tax at CliftonLarsonAllen
St. Joseph, Missouri Area
Current: CliftonLarsonAllen is... www.cliftonlarsonallen.com.



3 shared connections

[Connect](#)



Robert Bollig, CPA • 2nd
Tax Manager at CliftonLarsonAllen, LLP
La Crosse, Wisconsin Area
Current: CliftonLarsonAllen is... www.cliftonlarsonallen.com.



13 shared connections

[Connect](#)

Job results for cliftonlarsonallen.com 659 results

[See all](#)

Attacking

Let's Go Phishing

- Determine what you want
 - Remote access program
 - Credential harvesting
- Impersonate an internal employee
 - Most SPAM filters don't block this by default
 - Much higher success rate

Attacking

From: Ed [REDACTED]
To: Anderson, David J
Cc:
Subject: Webmail upgrade

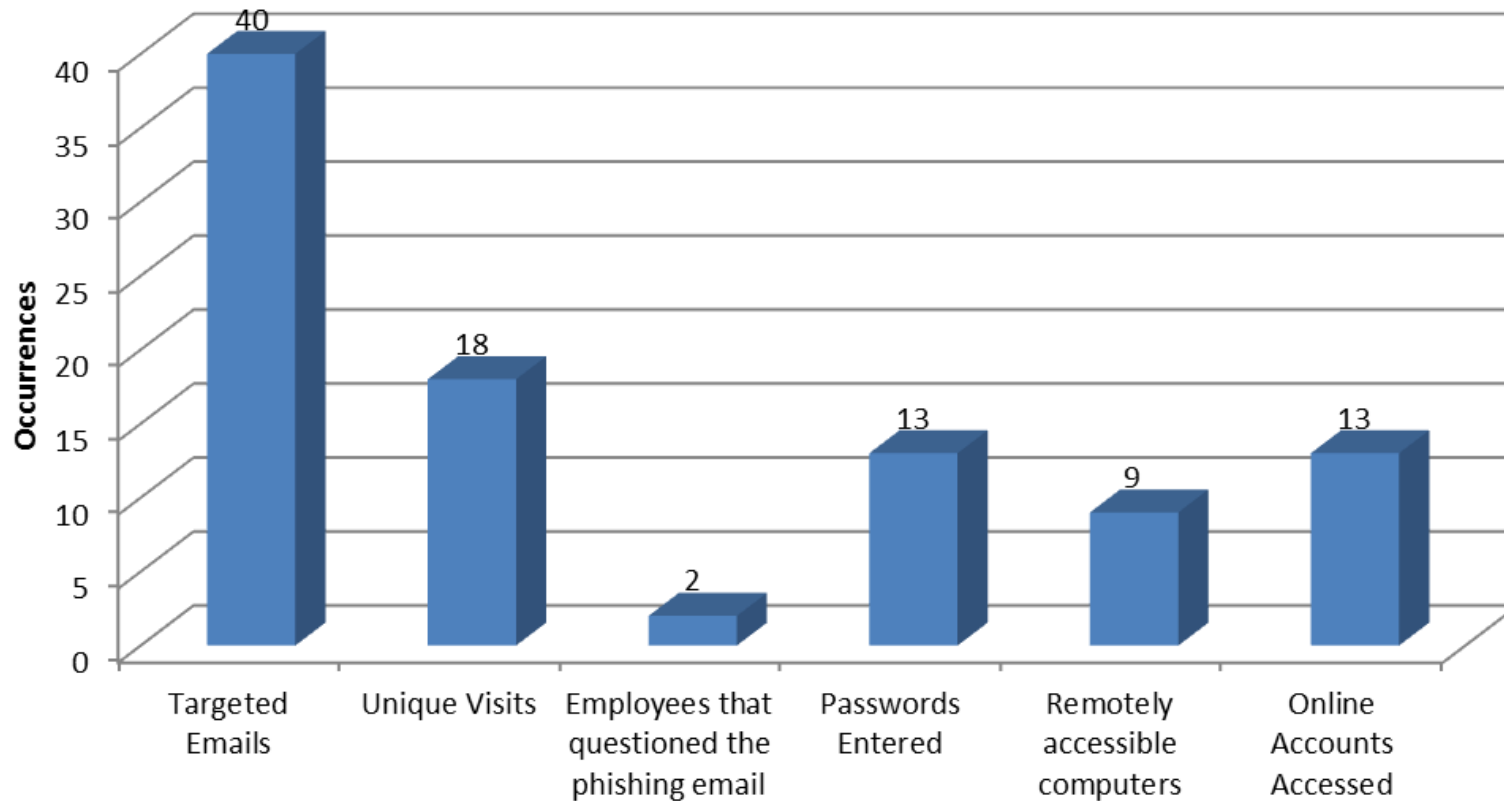
We have performed an upgrade to our mail system and are looking at updating access to webmail. We need users to log into the webmail portal in order to activate their account. Once you log in, you should receive a message that your email account has "been confirmed." If you get this message, the upgrade worked. If you receive an error, please let IT know and we will look into the issue.

Webmail site: [https://\[REDACTED\]/owa](https://[REDACTED]/owa)

Thanks,
Ed

Attacking

Phishing Results



What Does The Internet Perimeter Look Like (The Attack Surface)

- Externally Exposed Services
 - Webmail
 - VPN
 - Remote Desktop Protocol (RDP)
 - Helpdesk Portal
 - VMware Desktop
 - Lexmark Diagnostic Viewer
 - Other applications exposed to the Internet

Attacking

← → ↻ https://.issgs.net ☆

Microsoft®
Outlook® Web App

Exchange Email Account Update

This is a public or shared computer
 This is a private computer

Domain\user name:

Password:

Sign in

Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.

Cisco AnyConnect Secure Mobility Client

VPN: Connected to webvpn.
webvpn. Disconnect

00:00:50

Virtual Private Network (VPN)

Preferences Statistics Route Details Firewall Message History

Connection Information

State:	Connected
Tunnel Mode (IPv4):	Tunnel All Traffic
Tunnel Mode (IPv6):	Drop All Traffic
Duration:	00:00:50

Address Information

Client (IPv4):	172.30.
Client (IPv6):	Not Available
Server:	209.23.

Bytes

Sent:	12883
Received:	26400

Frames

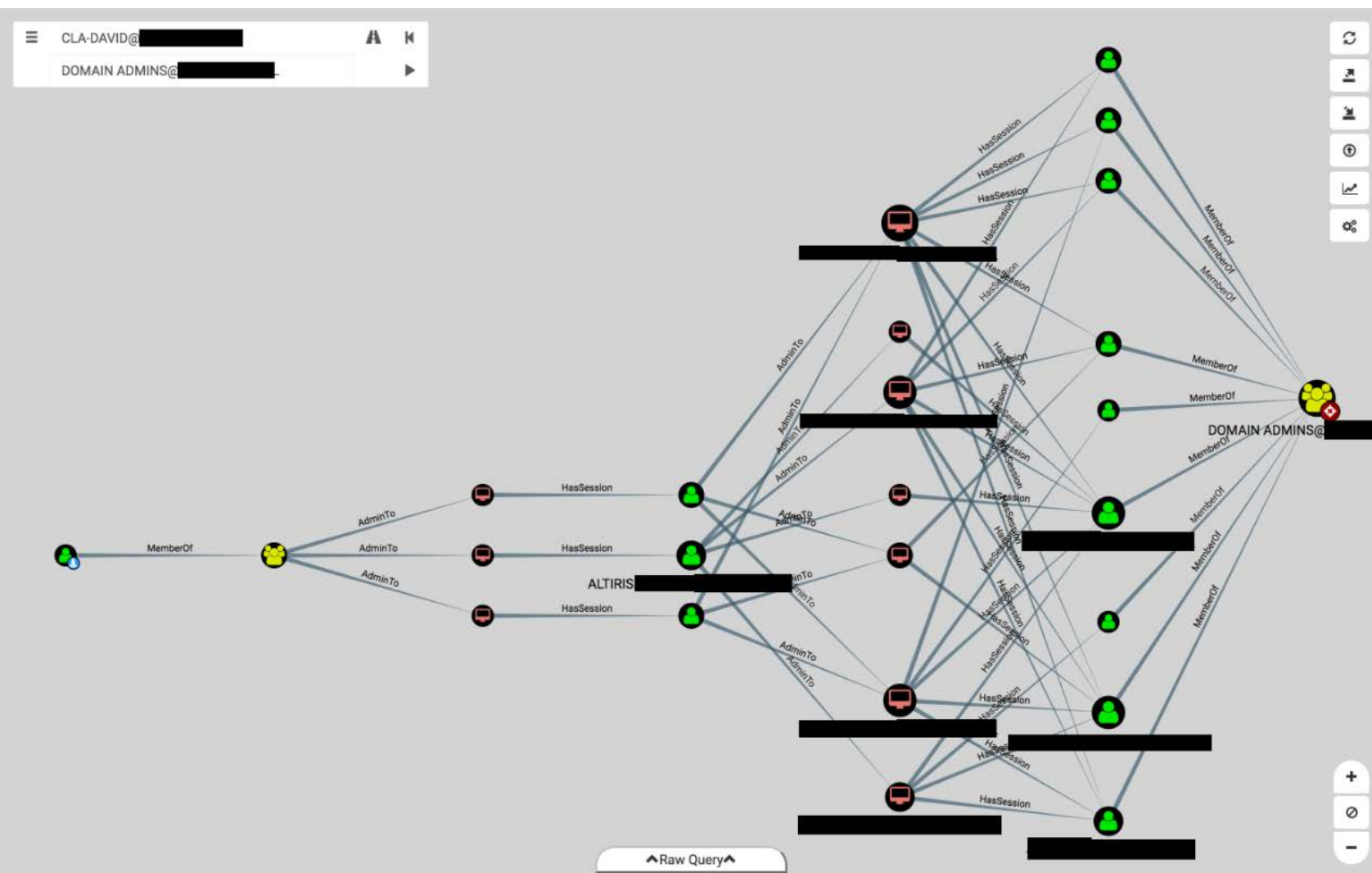
Reset Export Stats...

We Are Inside – Now What Do We Do

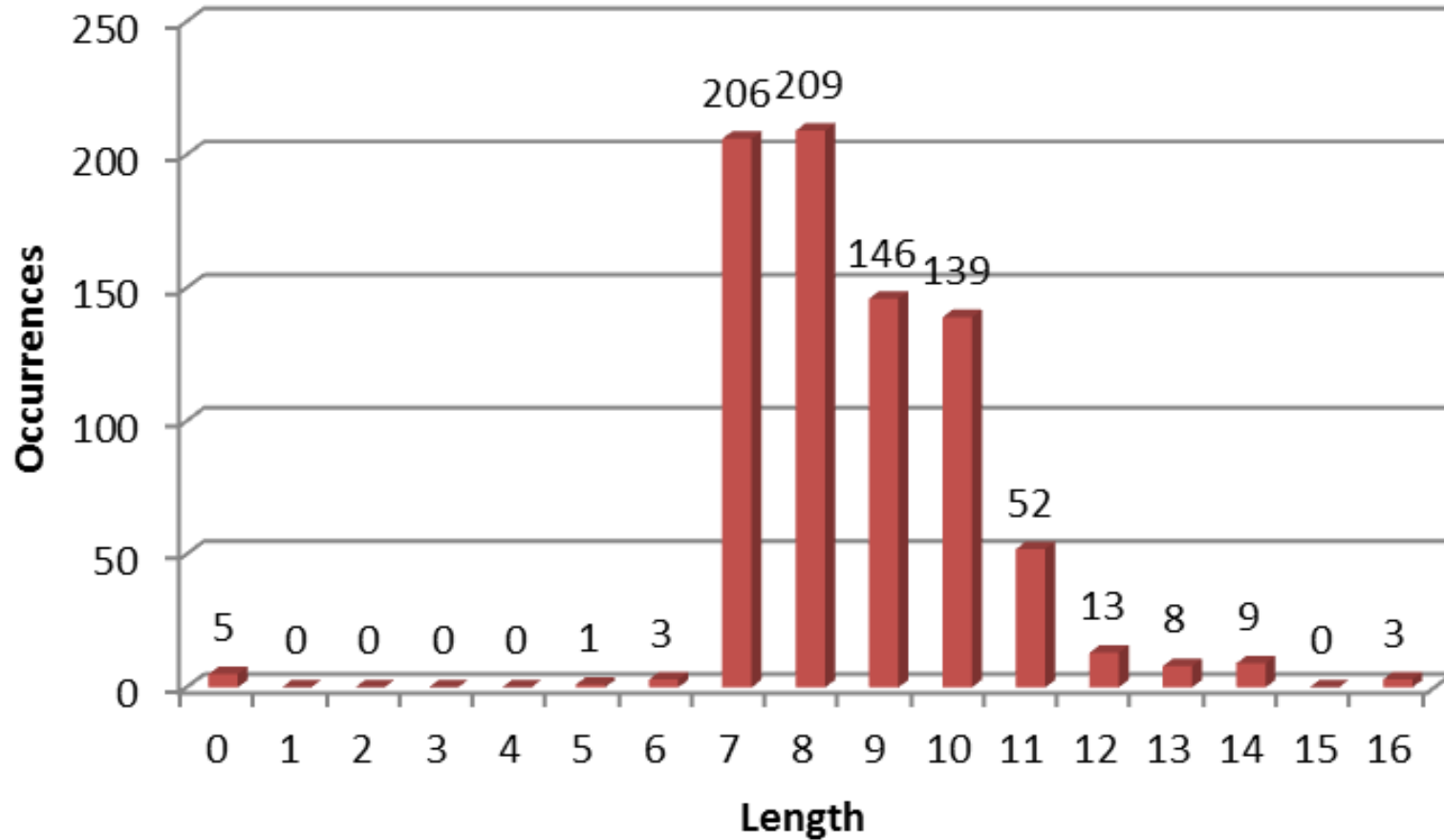
Internal network access... now what?

- Find sensitive information
 - Most employees have direct access to sensitive info
 - File shares and applications that are too open
- Elevate privileges
 - Often find administrative privilege issues
 - Abuse weak password policies

We Are Inside – Now What Do We Do



Password Cracking (I mean auditing...)



Password Cracking (I mean auditing...)

Password Audit	Total
Number of passwords audited	855
Passwords cracked	794
Passwords that were all letters	63
Passwords that were all numbers	5
Passwords that were an English word	20
Passwords that were a word with numbers appended to it	200
Passwords that were the same as the username	6
Passwords that do not meet Windows complexity	584

Carbanak - Biggest Bank Heist EVER

- \$1B over 2 years
- Average \$10M per bank.
- 2 to 4 months per bank
- Methods: Online Banking, Swift, ATMs
- Attackers primarily in Russia, Ukraine, China
- Banks primarily Russia, Europe, United States

<http://krebsonsecurity.com/2016/07/carbanak-gang-tied-to-russian-security-firm/>

18 Carbanak Gang Tied to Russian Security Firm?

JUL 16

Among the more plunderous cybercrime gangs is a group known as “Carbanak,” Eastern European hackers blamed for **stealing more than a billion dollars** from banks. Today we’ll examine some compelling clues that point to a connection between the Carbanak gang’s staging grounds and a Russian security firm that claims to work with some of the world’s largest brands in cybersecurity.

The Carbanak gang derives its name from the banking malware used in countless high-dollar cyberheists. The gang is perhaps best known for **hacking directly into bank networks using poisoned Microsoft Office files**, and then using that access to force bank ATMs into dispensing cash. Russian security firm **Kaspersky Lab estimates** that the Carbanak Gang has likely stolen upwards of USD \$1 billion — but mostly from Russian banks.

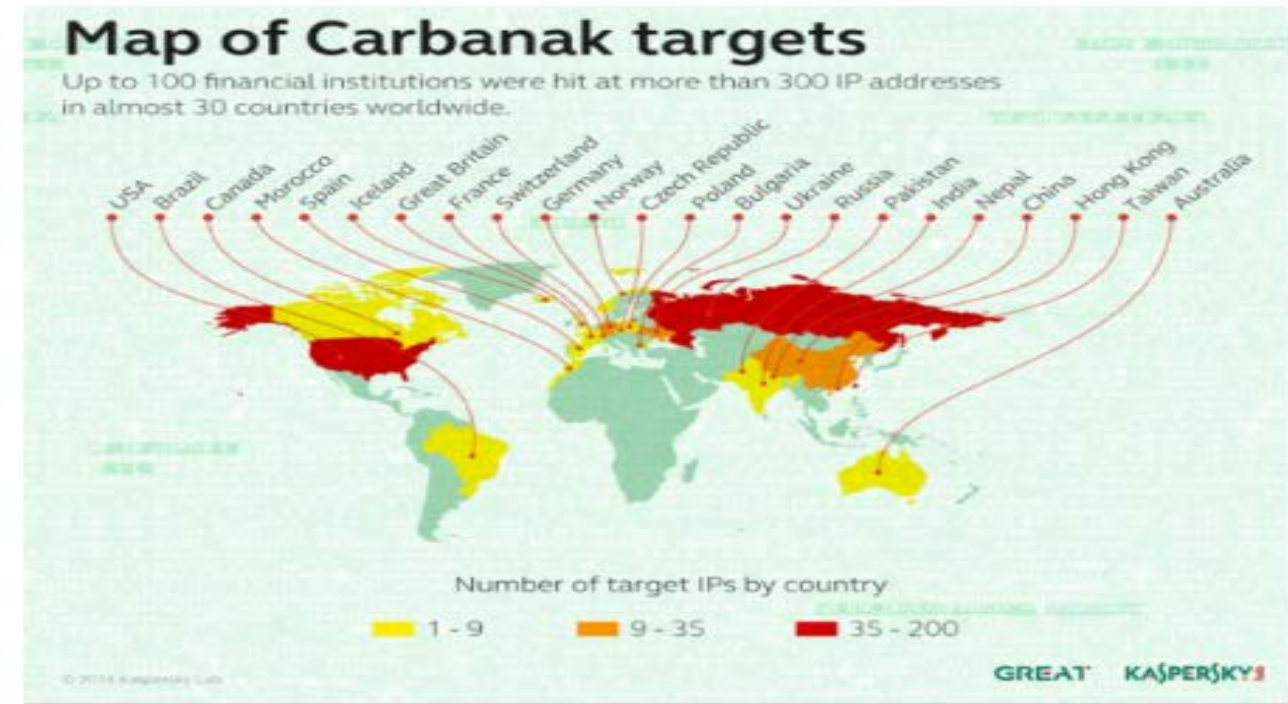


Figure 9. Geographical distribution of targets according to C2 data

Backend Payment Systems Carbanak - Biggest Bank Heist EVER

How the Carbanak cybergang stole \$1bn A targeted attack on a bank

1. Infection



100s of machines infected in search of the admin PC



2. Harvesting Intelligence

Intercepting the clerks' screens



3. Mimicking the staff

How the money was stolen



© 2015 Kaspersky Lab

GREAT KASPERSKY Lab

Backend Payment Systems - SWIFT

Ecuador Bank Hacked — \$12 Million Stolen in 3rd Attack on SWIFT System

Friday, May 20, 2016 Swati Khandelwal

81 Like 2.9K Share 924 Tweet 329 Share 123 share 1436



Bangladesh is not the only bank that had become victim to the cyber heist. In fact, it appears just a part of the widespread cyber attack on global banking and financial sector by hackers who target the backbone of the world financial system, SWIFT.

Yes, the global banking messaging system that thousands of banks and companies around the world use to transfer Billions of dollars in transfers each day is under attack.

A third case involving SWIFT has emerged in which cyber criminals have stolen about \$12 million from an Ecuadorean bank that contained numerous similarities of later attacks against Bangladesh's central bank that lost \$81 Million in the cyber heist.

Bangladesh Bank Attackers Hacked SWIFT Software

Attackers Used Malware to Steal \$81 Million, BAE Systems Says

Mathew J. Schwartz (@euroinfosec) · April 25, 2016 · 0 Comments

Twitter Facebook LinkedIn Credit Eligible Get Permission

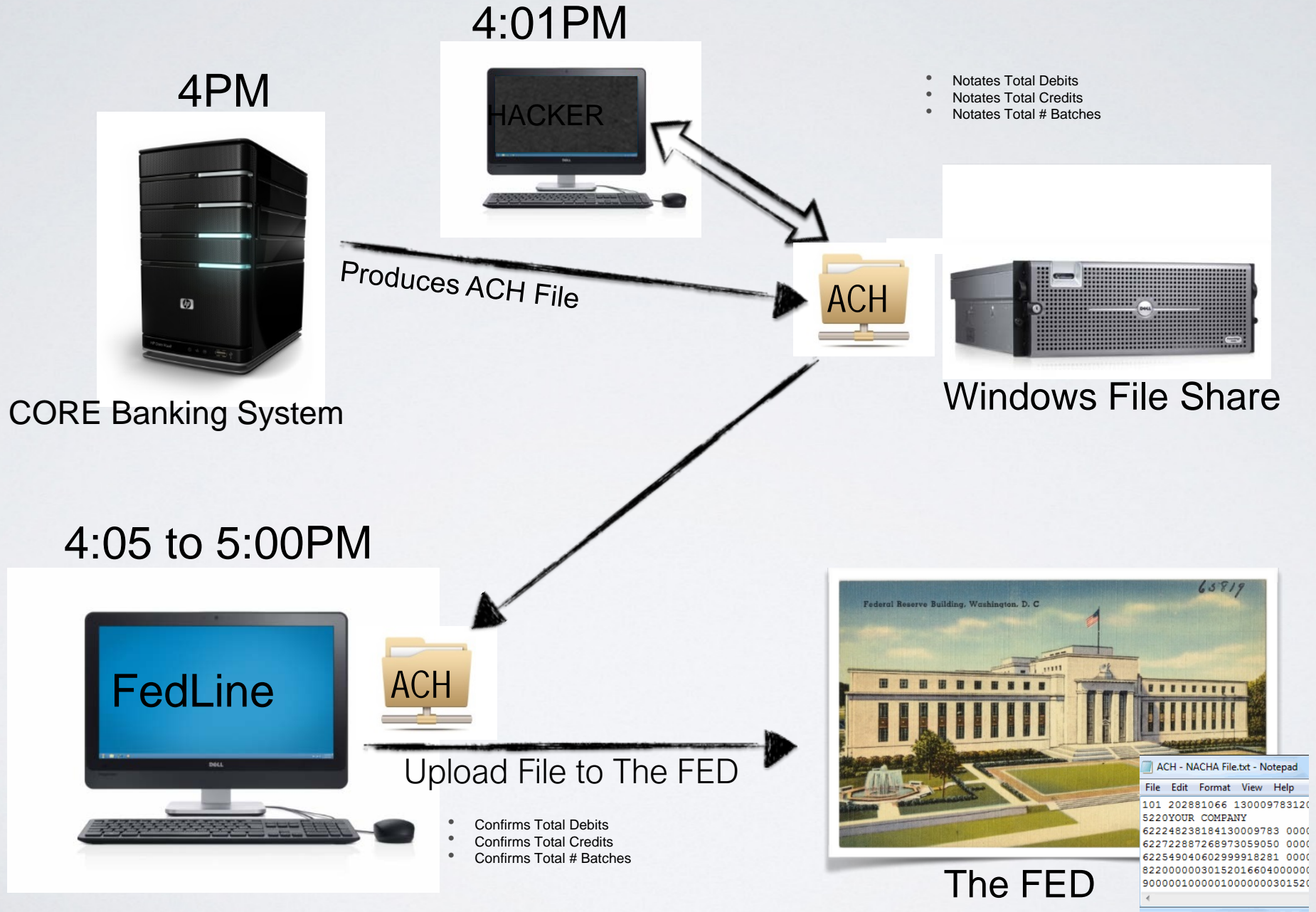
The attackers who stole \$81 million from Bangladesh Bank in February used malware that allowed them to hack into the bank's SWIFT software to transfer money, as well as hide their tracks, according to technology consultancy BAE Systems Applied Intelligence.

See Also: [Rethinking Endpoint Security](#)

The consultancy notes that it's found "custom malware" developed by an individual based in Bangladesh, which "contains sophisticated functionality for interacting with local SWIFT Alliance Access software running in the victim infrastructure."

SWIFT is a Belgium-based cooperative of 3,000 organizations that maintains a messaging platform that banks use to move money internationally. "SWIFT is aware of a malware that aims to reduce financial institutions' abilities to evidence fraudulent transactions on their local systems," a SWIFT spokesman tells Information Security Media Group. "Contrary to reports that suggest otherwise, this malware has no impact on SWIFT's network or core messaging services."

Backend Payment Systems - Is ACH Next?



Backend Payment Systems

ACH Fraud Potential

- All banks/credit unions that perform ACH originations are exposed.
- If Core/ACH outsourced, exposure is at vendor.
- Presence of ACH files awaiting transmission to processor.
- Files stored in Windows-protected storage.

- Potential Profit: Tens of Thousands to Tens of Millions.
- Why: Inherently weak and outdated file structure.
- What is keeping attackers from exploiting this vulnerability?
 - Knowledge and Current Success with Cardholder Data and Ransomware

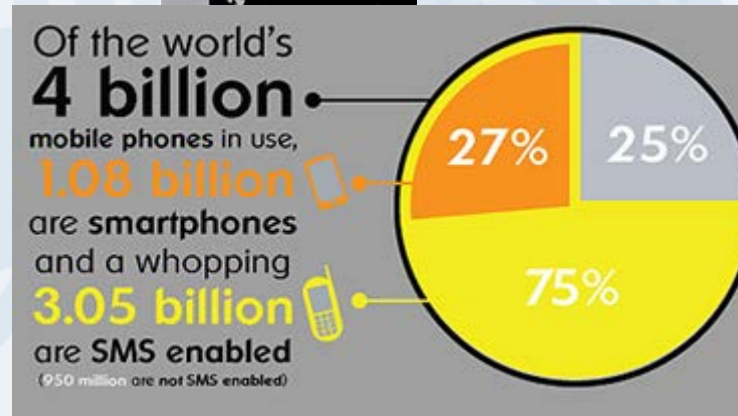
Backend Payment Systems

Action Required

- Protect high-risk files with a mechanism that requires access beyond Windows Administrator. (WORM or Linux)
- If ACH outsourced, relay concerns to vendor.
- Simulate breach and determine if your staff can detect and respond in a timely manner.
- Audit directory and file access. It is fairly common to find excessive employee ACH access within Core systems and network file shares.

Mobile Banking Basics

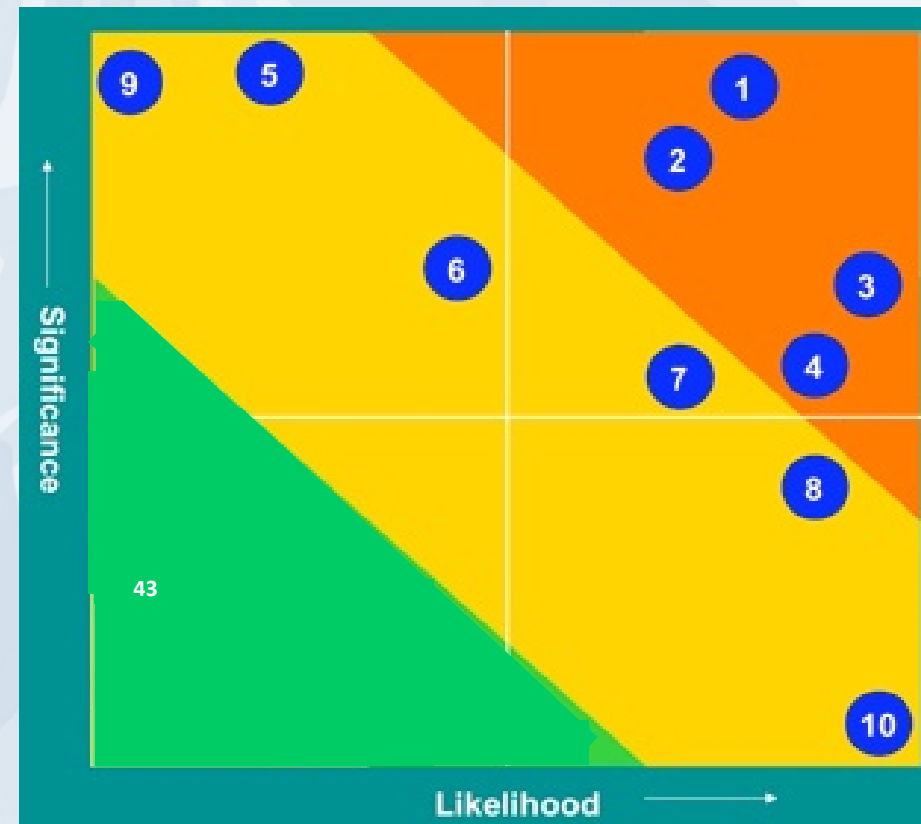
- Mobile Banking is here to stay...
- More people have (smart) phones than computers
- Mobile payments and deposits are common



Vulnerabilities, Risks, & Controls

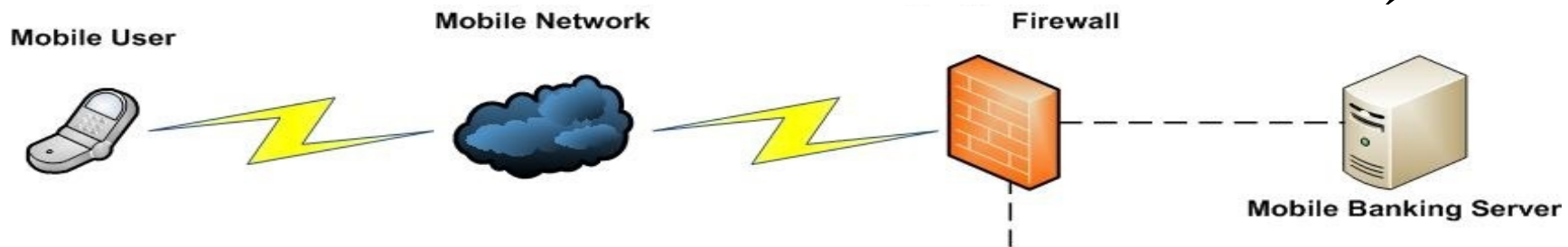
- Vulnerabilities and risks at each component
- Perform a risk assessment
 - Server Side Risks
 - (Vendor Risks)
 - Transmission Risks
 - Mobile Device Risks
 - Mobile App Risks
 - End User Risks

Risk Assessment Heat Map



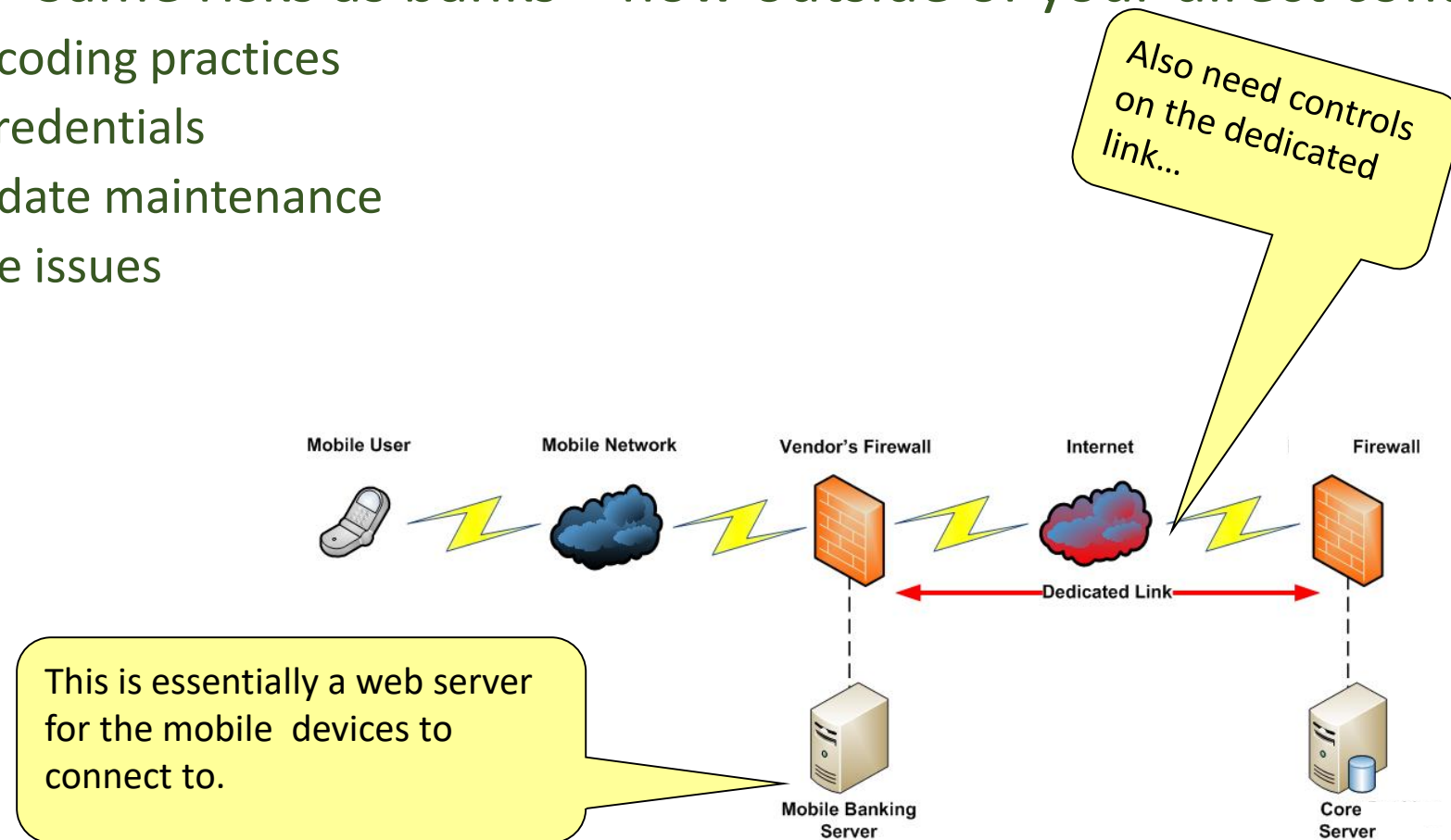
Vulnerabilities, Risks, & Controls

- **Server Side Risks** – Essentially the same as traditional Internet banking website risks
 - Insecure coding practices
 - Default credentials
 - Patch/update maintenance
 - Certificate issues



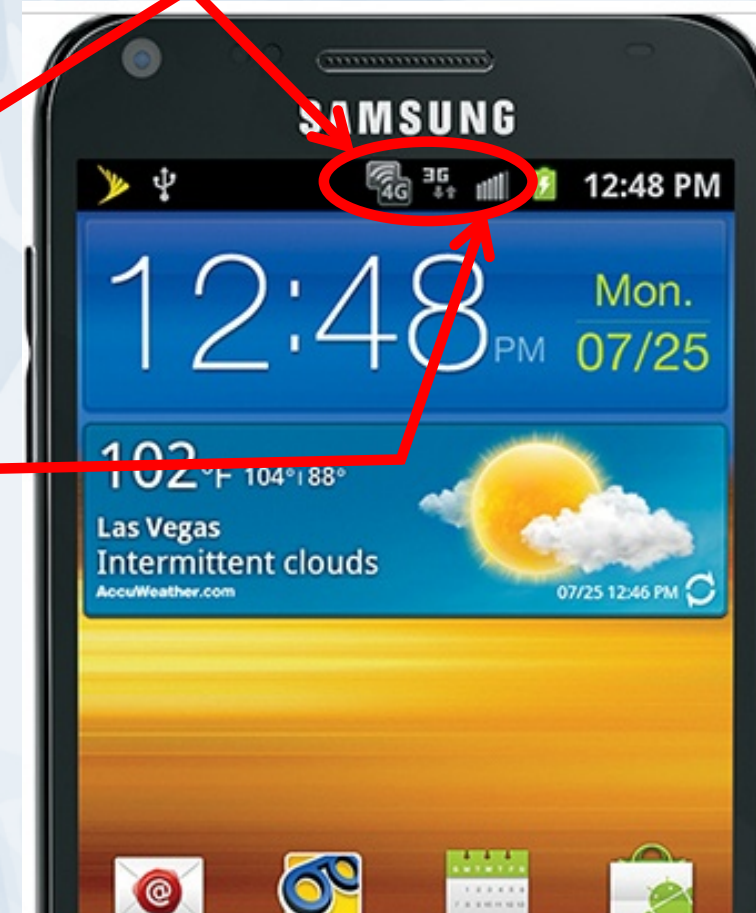
Vulnerabilities, Risks, & Controls

- **Vendor Risks** – Same risks as banks – now outside of your direct control.
 - Insecure coding practices
 - Default credentials
 - Patch/update maintenance
 - Certificate issues



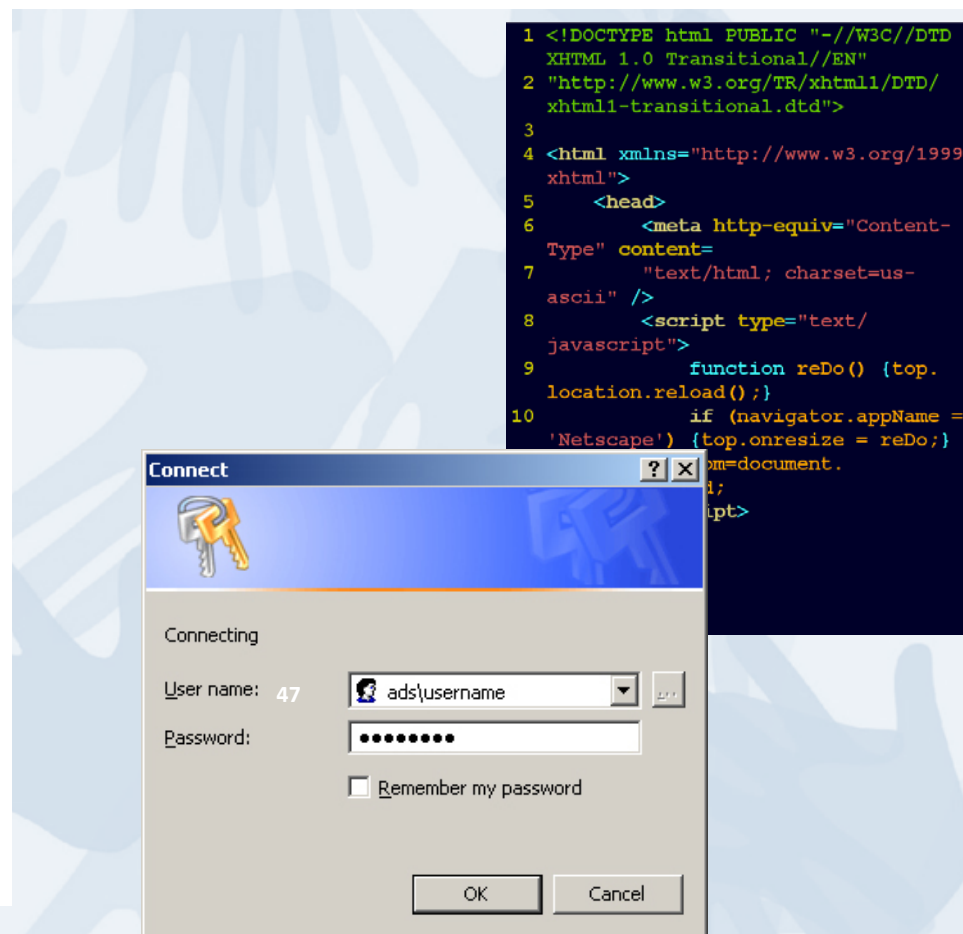
Vulnerabilities, Risks, & Controls

- Transmission Risks
 - Most mobile devices have always on Internet connection
 - Cellular (cell phone service provider)
 - Wifi (802.11 – home, corporate, “public”)
 - Need encryption



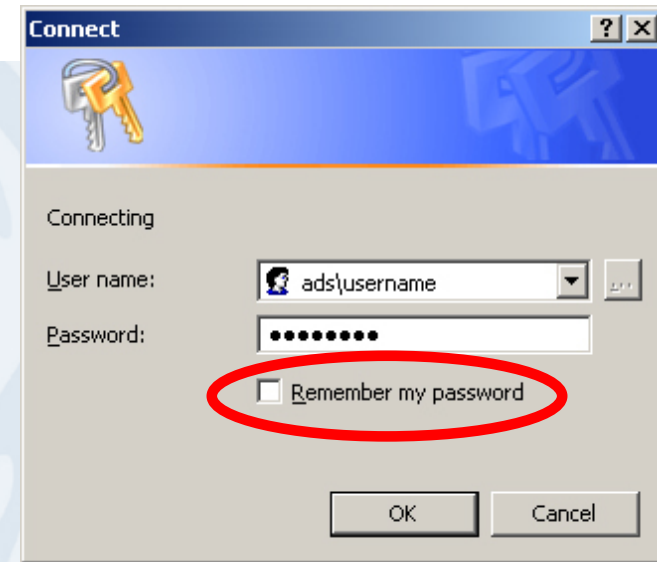
Vulnerabilities, Risks, & Controls

- Mobile App Risks
 - Secure coding issues
 - Installation of App
 - Use and protection of credentials
 - Storage of data
 - Transmission of data



Vulnerabilities, Risks, & Controls

- End User Risks
 - Lose the device
 - Don't use passwords, or use "easy to guess passwords"
 - Store passwords on the device
 - Jail break the device
 - Don't use security software
 - Use/don't recognize insecure wireless networks
 - Let their kids "use" the device



Vendor Due Diligence and Management

- All of the above – applies to your vendor(s)
 - Mobile banking application provider
 - Mobile banking hosting provider
- Contracts with SLA's
- SSAE18 reviews
- PCI Compliance validation
- Independent code review and testing
- FFIEC updates are clear: Need to hold service providers to YOUR standards... its YOUR data.

BYOD – what are you worried about?

Your List:

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.

My List:

1. Data leakage
2. Data theft
3. Ability for others to interact with the device
4. Loss of device
5. Storage of critical data
6. Internet of Things interconnectivity
7. Malware

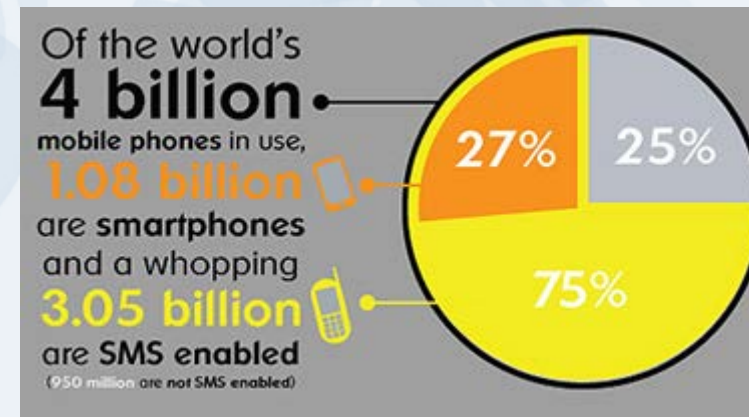
BYOD

- People, Rules, and Tools:

- Standards
- Data Classification
- Policies
- Incident Response
- Litigation Preparedness

- Why are we doing it?

- Is it cheaper?
- Because “they are doing it”
- Because it makes good business sense

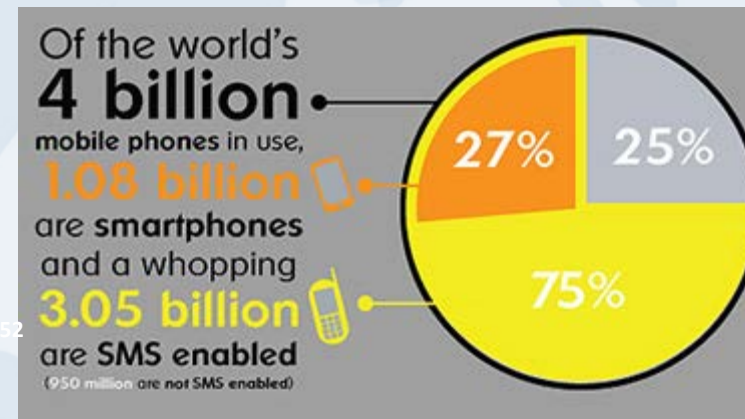


51

Control Strategies for BYOD

- Controls and Enterprise management of:
 - Acceptable use
 - Credentials
 - Login/Screen Saver

- What do you have at the bank?



Control Strategies for BYOD

Safeguards For Enterprises:

- On-device anti-malware
- On-device firewall
- SSL VPN clients to effortlessly protect data in transit, and to ensure secure and appropriate network access and authorization
- Mobile Device Management (MDM):
 - Centralized remote locate, track, lock, wipe, backup and restore facilities for
 - Centralized administration to enforce and report on security policies across the entire mobile device population

Control Strategies for BYOD

Safeguards For Enterprises - MDM:

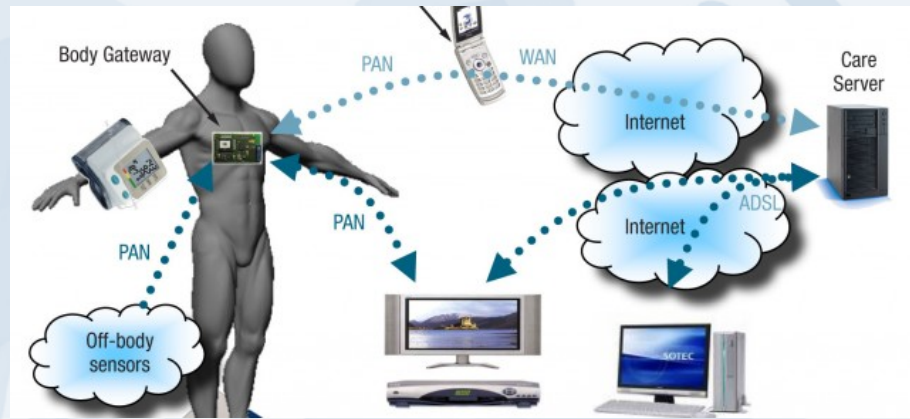
- Device monitor and control, such as the monitoring of messaging and control of installed applications
- A solution that integrates with network-based technologies, such as network access control (NAC), to ensure the security posture of mobile devices and determine appropriate access rights prior to allowing access to corporate resources
- Management capabilities to enforce security policies, such as mandating the use of PINs/passcodes
- Ability for an administrator to monitor device activity for data leakage and inappropriate use

Additional Trends to Watch

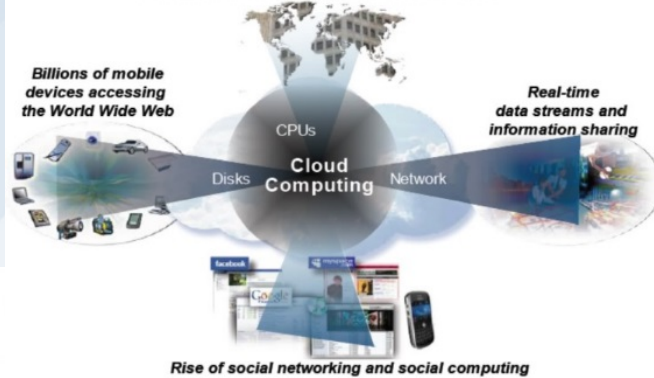
Internet of Things

- Growing 30% per year
- Gartner forecasts 21 billion devices by 2020
- Consumer devices account for 5.2 billion units in 2017, or 63% of the total
- Businesses devices account 3.1 billion units in 2017, or 37% of the total
- FI's collect a lot of information from customers through various channels
- Hacking could cause massive damage
- Weak default passwords unchanged

Raise Your Hand If...



Cloud Computing, Compute Model for a Smarter Planet Globalization and Globally Available Resources



INTRODUCING **echo dot**
Add Alexa to any room

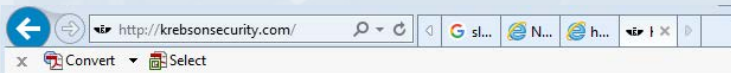
amazon tap
ALEXA-ENABLED PORTABLE SPEAKER
JUST TAP & ASK

Logos for various services: P, Spotify, iHeartRadio, UBER, wemo, 31, a, tunein, news, nue, PHILIPS, audible.

56

softer FIRMER
View Personal Preference™ Collection

Internet of Things (IoT)



Other — 45 comments

13 IoT Devices as Proxies for Cybercrime

OCT 16

Multiple stories published here over the past few weeks have examined the disruptive power of hacked “Internet of Things” (IoT) devices such as routers, IP cameras and digital video recorders. This post looks at how crooks are using hacked IoT devices as proxies to hide their true location online as they engage in a variety of other types of cybercriminal activity — from frequenting underground forums to credit card and tax refund fraud.



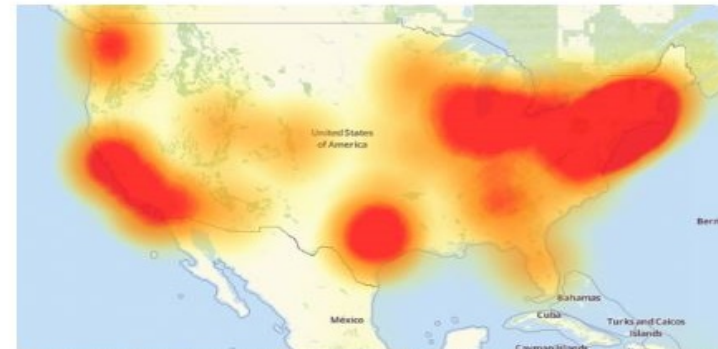
Recently, I heard from a cybersecurity researcher who'd created a virtual “honeypot” environment designed to simulate hackable IoT devices. The source, who asked to remain anonymous, said his honeypot soon began seeing traffic destined for **Asus** and **Linksys** routers running default credentials. When he examined what that traffic was designed to do, he found his honeypot systems were being told to download a piece of malware from a destination on the Web.

21 Hacked Cameras, DVRs Powered Today's Massive Internet Outage

OCT 16

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked “Internet of Things” (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet's top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.



A depiction of the outages caused by today's attacks on Dyn, an Internet infrastructure company. Source: Downtime.com.

At first, it was unclear who or what was behind the attack on Dyn. But over the past few hours, at least one computer security firm has come out saying the attack involved **Mirai**, the same malware strain that was used in the record 620 Gpbs attack on my site last month. At the end September 2016, the hacker responsible for creating the Mirai malware released the source code for it, effectively letting anyone build their own attack army using Mirai.

Mirai scans the Web for IoT devices protected by little more than factory-default usernames and passwords, and then enlists the devices in attacks that hurl junk traffic at an online target until it can no longer accommodate legitimate visitors or users.

According to researchers at security firm **Flashpoint**, today's attack was launched at least in part by a Mirai-based botnet. **Allison Nixon**, director of research at Flashpoint, said the botnet used in today's ongoing attack is built on the backs of hacked IoT devices — mainly compromised digital video recorders (DVRs) and IP cameras made by a Chinese hi-tech company called **XiongMai Technologies**. The components that XiongMai makes are sold

Everything Can Talk to Everything....

Android Malware Used to Hack and Steal a Tesla Car

By [Catalin Cimpanu](#)

November 25, 2016

06:05 AM

3



By infecting a Tesla owner's phone with Android malware, a car thief can hack and then steal a Tesla car, security researchers have revealed this week.

Previous attempts to hack Tesla cars attacked the vehicle's on-board software itself. This is how Chinese security researchers from [Keen Lab](#) have managed to hack a Tesla Model S last month, allowing an attacker to control a car from 12 miles away.

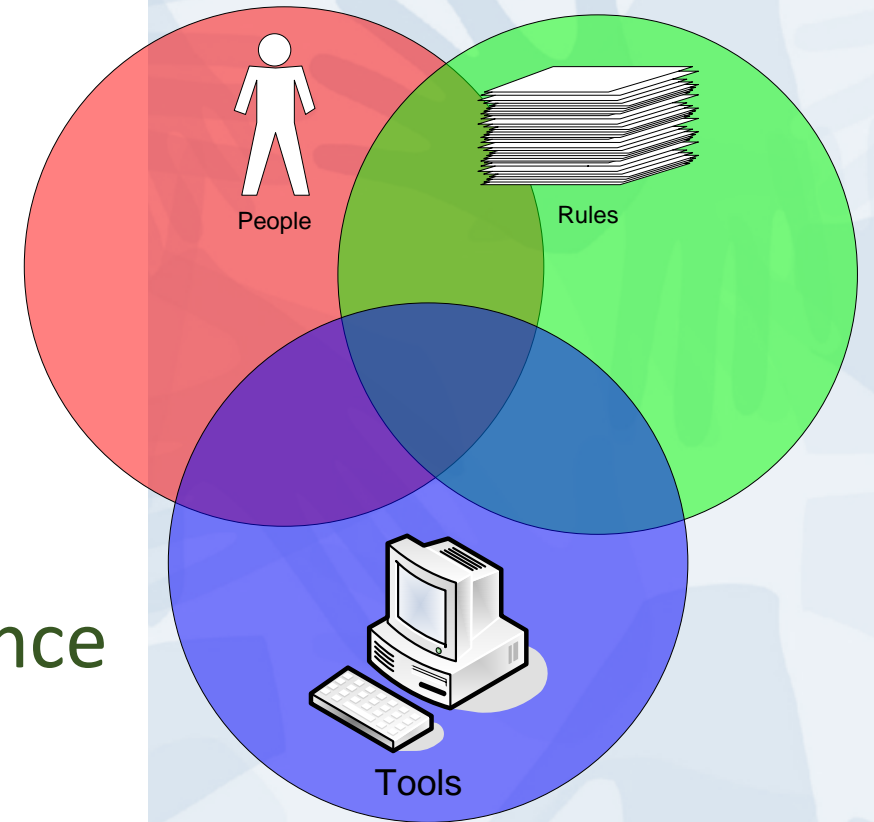
Security experts from Norwegian security firm [Promon](#) have taken a different approach, and instead of trying complicated attacks on the car's firmware, they have chosen to go after Tesla's Android app that many car owners use to interact with their vehicle.

Internet of Things Banking



Policies

- People, Rules and Tools
 - What do we expect to occur?
 - How do we conduct business?
- Standards Based, Disciplined, Change Management, operating from a Governance or Compliance framework:
 - FFIEC
 - PCI – DSS
 - CIS Critical Controls



Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

<https://www.cisecurity.org/controls/>

Defined Standards

- Harden your systems and applications
 - Principal of Minimum Access and Least Privilege
 - Turn off the services/components you do not need
 - Change the defaults
- CIS offers vendor-neutral hardening resources
<http://www.cisecurity.org/>
- Microsoft Security Checklists
<http://www.microsoft.com/technet/archive/security/chklist/default.aspx?mfr=true>
<http://technet.microsoft.com/en-us/library/dd366061.aspx>
- Software/Application Provider “Implementation Guide”

Operational Discipline

- Disciplined Change Management
- Consistent Exception Control & Documentation
 - Should include risk evaluation and acceptance of risk
 - Risk mitigation strategies
 - Expiration and re-analysis of risk acceptance



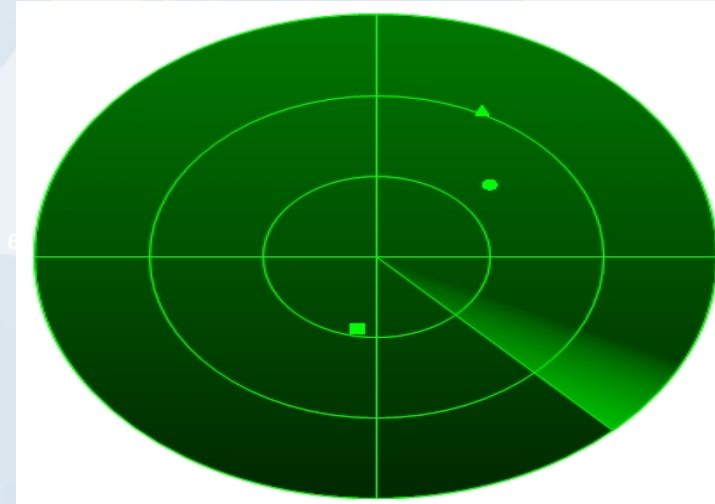
Vulnerability and Patch Management Standards

- Define your standard
 - Internet facing critical updates will be applied within ___ Days
 - Internal system critical updates will be applied within ___ Days
- Manage to your standard
- Document and manage your exceptions



Vulnerability Management Monitoring

- Monitoring
 - System logs and application “functions”
 - Accounts
 - Key system configurations
 - Critical data systems/files
- Scanning
 - Patch Tuesday and vulnerability scanning
 - Rogue devices

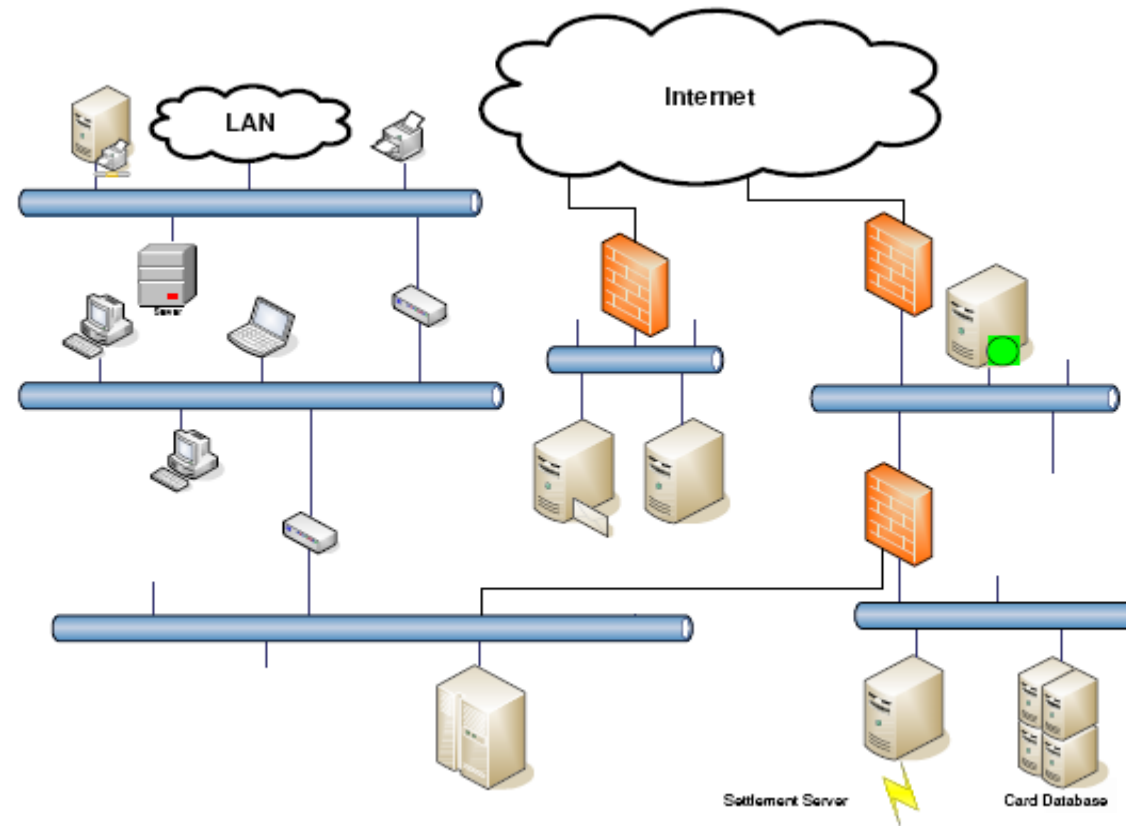


Know Your Network

Know What “Normal” Looks Like

Alignment of centralized audit logging, analysis, and automated alerting capabilities (SIEM) & DLP

- Infrastructure
- Servers & Applications
- Data Flows
- Archiving vs. Reviewing





**Lee Painter, Principal
CyberSecurity
CISSP, CRISC, HCISPP, CCSFP
lee.painter@claconnect.com
309.202.9531**