Winter Executive Forum 2017

JANUARY 17-20, 2017
LOEWS DON CESAR ST. PETE BEACH, FLORIDA

A Berkshire Hathaway Company

Cyber Security at Gen Re

Presented by Scott Speaker

January 18, 2017

Agenda

- Cyber Security Risks –
  Current State, Threat Actors, Is it really that easy?
- Aligning Business Risks with Appropriate Controls
- Security Framework
- Security Awareness
- Layers of Defense
- A couple of tips …

Major U.S. Data Breaches

2015

🟥 Anthem, Inc.
February
78.8M records (personal information)

🟥 UCLA Health
July
4.5M records (personal information and medical records)

🟥 Premera Blue Cross
March
11M records (personal information)

🟥 Excellus Blue Cross Blue Shield
September
10M records (personal information and financial data)

🟥 CareFirst Blue Shield
May
1.1M records (personal information)

🟥 Systema Software
September
1.5M records (medical records)

🟧 OPM
May
22M records (personal information)

🟦 T-Mobile / Experian
October
15M records (personal information)

🟥 MIE / NoMoreClipboard
June
4M records (personal information)

🟩 Scottrade
October
4.6M records (personal information)

🟧 OPM
June
4M records (personal information)

🟧 GA Secretary of State
November
6M records (personal information)

2016

🟥 21st Century Oncology
March
2.2M records (personal information)

🟥 Medstar Health
March
Ransomware disables systems

🟥 Premier Healthcare
March
205k records (stolen laptop)

🟥 Medical Colleagues of Texas
May
68k records (personal information)

🟩 Nordic Consulting Partners
May
1k records (employee error)

🟩 Pennsylvania Lumbermens Mutual Insurance Company
June
Unknown records (W2s)

🟧 IRS
February
700k records (financial information)

🟦 Dropbox
August
68M records (from 2012 Breach)

🟦 Verizon
March
1.5M records

🟩 State Farm
January
Unknown records

🟦 Yahoo
September
500M records

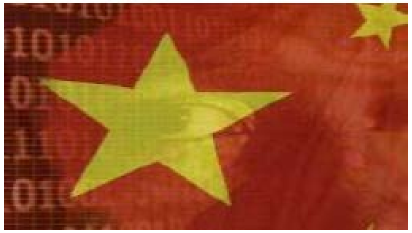
🟦 Yahoo
December
1B records

Source: Identity Theft Resource Center

🟥 Healthcare Insurance and Services 🟧 Government 🟩 Banking / Financial / Credit 🟦 Business Services

The Threats

Profiles of Threat Actors



Nation States

- Targeted and multi-stage
- Motivated by data collection
- Highly sophisticated with endless sources

Hactivists

- Targeted and destructive
- Unpredictable motivations
- Generally less sophisticated

Cyber Criminals

- Broad-based and targeted
- Financially motivated
- Getting more sophisticated

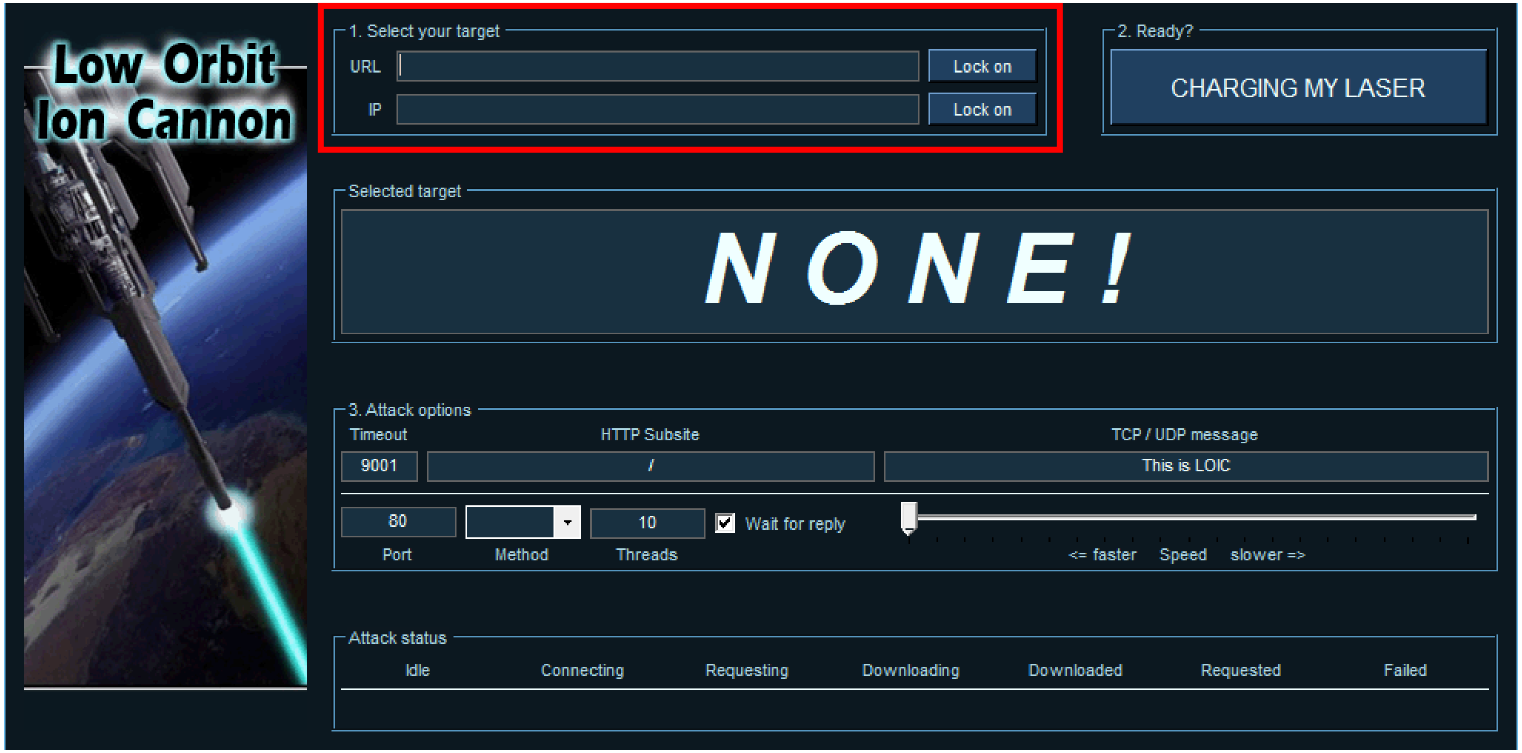
Insiders

- Targeted and destructive
- Unpredictable motivations
- Sophistication varies

Source: Carbon Black

It Is Really Easy

- Watch tutorial on Youtube: https://www.youtube.com/watch?v=_nPcysStRio
- Download LOIC from Sourceforge: https://sourceforge.net/projects/loic/
- Select website and execute …



Selected target: NONE!

Timeout: 9001
HTTP Subsite: /
TCP / UDP message: This is LOIC
Port: 80
Threads: 10
☑ Wait for reply

Source: Fortune

Cyber Security Risks at Gen Re

Ranking

Business Risk	Rank
Loss of Protected or Privileged Records	1
Extortion	2
Theft	3
Loss of Information Integrity	4
Business Interruption	5

Reviewed likelihood, impact, and ranking of each with Risk Committees and management resulting in:

1. Risk alignment
2. Guidance for future security investments

Gen Re | Winter Executive Forum 2017

Aligning Business Risk with Appropriate Controls

Business Risk – Loss of Protection Records

Where the impact is greatest …

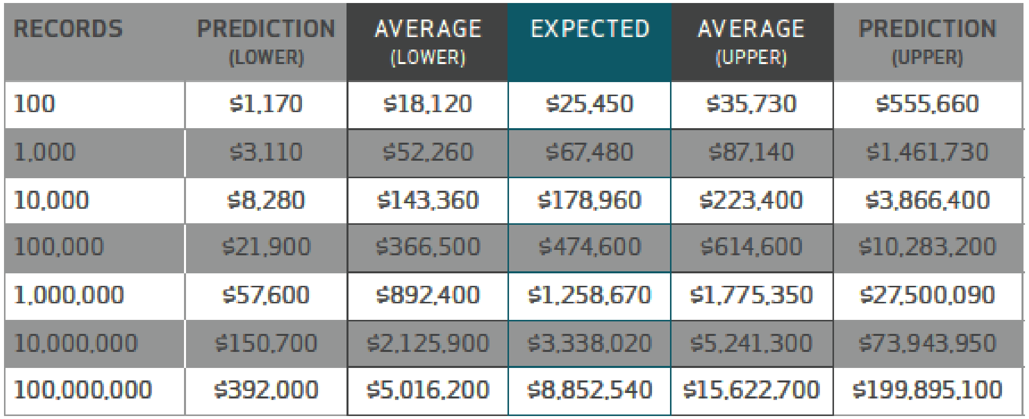
Where the information is easy to get

- The Dark Web
- “Insurers see 317% rise in data breaches”
- Human error accounts for over 60% of incidents

Where the money is . . .

- $1 for Social Security or Credit Card Numbers
- $10 for Partial Health Credentials
- $50 for Electronic Health Records

Where would Willie Sutton go today?



RECORDS	PREDICTION (LOWER)	AVERAGE (LOWER)	EXPECTED	AVERAGE (UPPER)	PREDICTION (UPPER)
100	$1,170	$18,120	$25,450	$35,730	$555,660
1,000	$3,110	$52,260	$67,480	$87,140	$1,461,730
10,000	$8,280	$143,360	$178,960	$223,400	$3,866,400
100,000	$21,900	$366,500	$474,600	$614,600	$10,283,200
1,000,000	$57,600	$892,400	$1,258,670	$1,775,350	$27,500,090
10,000,000	$150,700	$2,125,900	$3,338,020	$5,241,300	$73,943,950
100,000,000	$392,000	$5,016,200	$8,852,540	$15,622,700	$199,895,100

Source: fortune.com

Vignette 1 – Loss of Protection or Privileged Records

Data Breach – Consultant

- Consultant uses a personal USB thumb drive to install password hacking tools in an effort to extract data.
- IT systems scan the drive and create alerts.
- Consultant is confronted and denies wrongdoing.
- Forensic investigation conducted to determine if data was transferred to the USB drive – external firm is engaged.

Business Controls

- Incident Response for:
  - Isolating impacted assets
  - Interacting with legal, HR and third parties
- Security Event & Incident Management (SEIM)
- Forensic company (pre-qualification)
- Encryption
- Data Loss Prevention

Business Risk – Extortion

How do you extort money without getting caught?

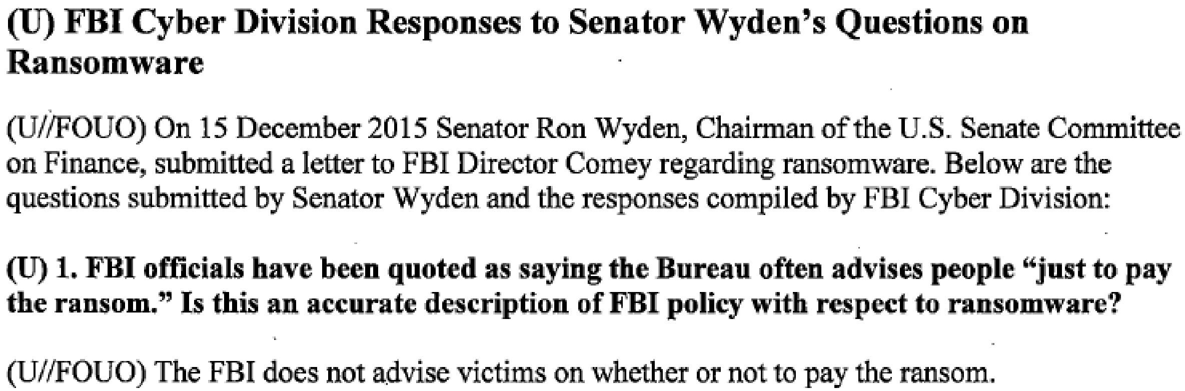
How does it work?

- User visits a malicious website or clicks on a malicious email and installs infected software.
- Malicious code encrypts personal data and files.
- Criminal demands ransom payment for encryption key.

What do they ask for?

- Payment, typically in the form of bitcoins.
- Range from $21-$700, with the average being just over $300.
- Estimated at $1B in 2016.

What does the Government say?



(U) FBI Cyber Division Responses to Senator Wyden's Questions on Ransomware

(U//FOUO) On 15 December 2015 Senator Ron Wyden, Chairman of the U.S. Senate Committee on Finance, submitted a letter to FBI Director Comey regarding ransomware. Below are the questions submitted by Senator Wyden and the responses compiled by FBI Cyber Division:

(U) 1. FBI officials have been quoted as saying the Bureau often advises people "just to pay the ransom." Is this an accurate description of FBI policy with respect to ransomware?

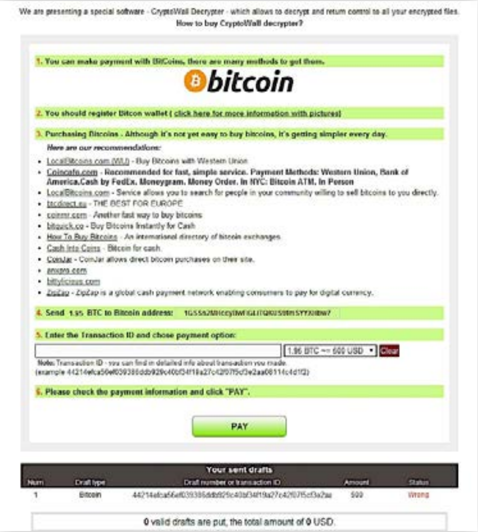
(U//FOUO) The FBI does not advise victims on whether or not to pay the ransom.

Source: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware; FBI

Vignette 2 – Extortion

Ransomware – TeslaCrypt 2.0

- Malicious attachment sent to an associate denoting a past due account balance with urgent remittance request.
- Within 10 minutes of clicking on the file attachment, all local and attached drives are encrypted (e.g., 20,000+ files).
- Payment request appears.



We are presenting a special software - CryptoWall Decrypter - which allows to decrypt and return control to all your encrypted files.
How to buy CryptoWall decrypter?

1. You can make payment with BitCoins, there are many methods to get them.

2. You should register Bitcon wallet (click here for more information with pictures)

3. Purchasing Bitcoins . Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
- Coincafe.com - Recommended for fast, simple service. Payment Methods: Western Union, Bank of America,Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person
- LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- btcdirect.eu - THE BEST FOR EUROPE
- coinmr.com - Another fast way to buy bitcoins
- bitquick.co - Buy Bitcoins Instantly for Cash
- How To Buy Bitcoins - An international directory of bitcoin exchanges.
- Cash Into Coins - Bitcoin for cash.
- CoinJar - CoinJar allows direct bitcoin purchases on their site.
- anxpro.com
- bittylicious.com
- ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

4. Send 1.95 BTC to Bitcoin address: 1G5S62MIccyIWfGLITQKU5ItH5YYXHBW7

5. Enter the Transaction ID and chose payment option:

1.96 BTC ~= 600 USD ▾ Clear

Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f18a27c42f07f5cf3e2aa08114c4d1f2)

6. Please check the payment information and click "PAY".

PAY

Your sent drafts				
Num	Draft type	Draft number or transaction ID	Amount	Status
1	Bitcoin	44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3a2ae	599	Wrong

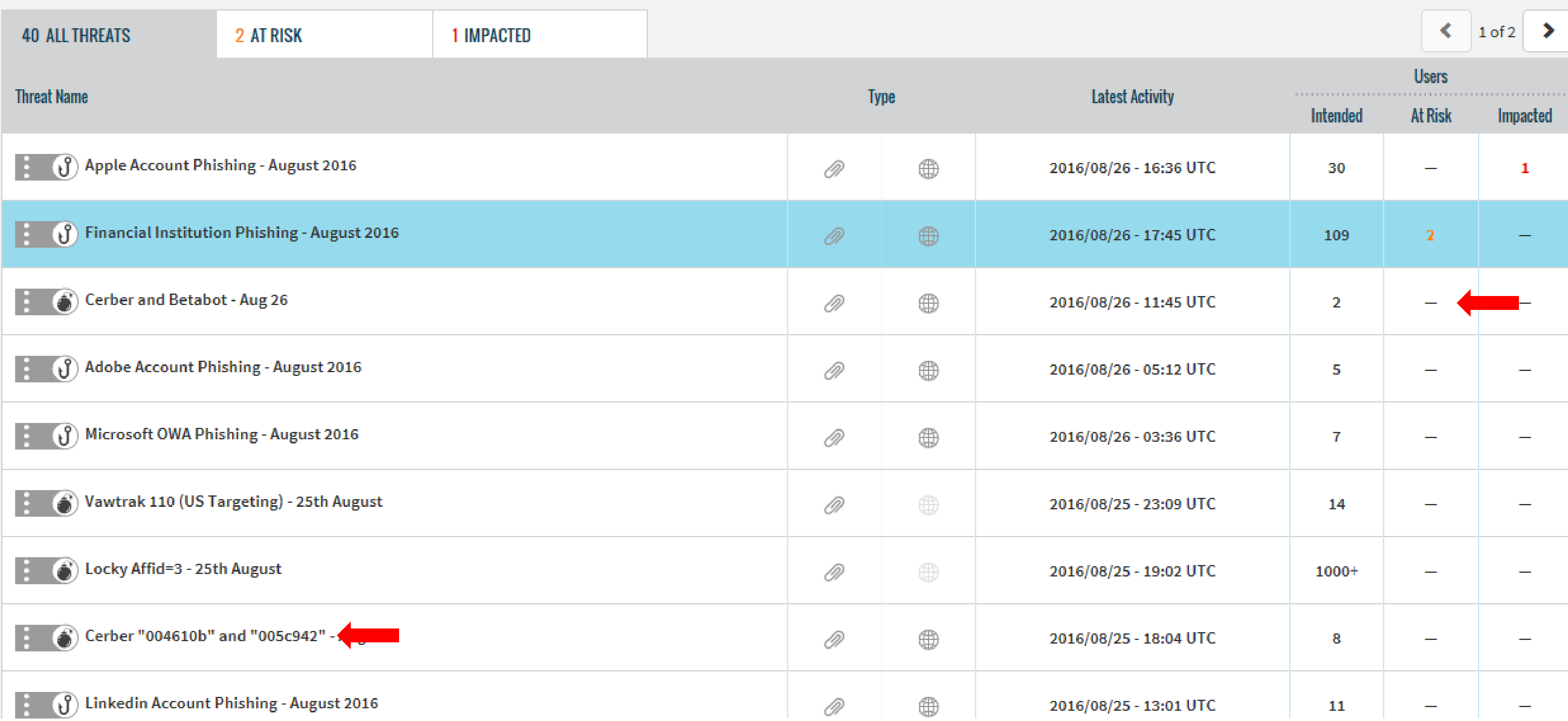
0 valid drafts are put, the total amount of 0 USD.

Business Controls

- Incident Response for isolating impacted assets
- Backup / Restore Capabilities
- Employee Awareness
- [External] designation on all emails received from outside the company
- URL and Attachment defenses
(i.e., sandboxing)

Source: https://www.isightpartners.com/2015/09/teslacrypt-2-0-cyber-crime-malware-behavior-capabilities-and-communications/

A Typical Day of Email Defense



Threat Name	Type		Latest Activity	Users		
				Intended	At Risk	Impacted
Apple Account Phishing - August 2016	📎	🌐	2016/08/26 - 16:36 UTC	30	–	1
Financial Institution Phishing - August 2016	📎	🌐	2016/08/26 - 17:45 UTC	109	2	–
Cerber and Betabot - Aug 26	📎	🌐	2016/08/26 - 11:45 UTC	2	–	–
Adobe Account Phishing - August 2016	📎	🌐	2016/08/26 - 05:12 UTC	5	–	–
Microsoft OWA Phishing - August 2016	📎	🌐	2016/08/26 - 03:36 UTC	7	–	–
Vawtrak 110 (US Targeting) - 25th August	📎	🌐	2016/08/25 - 23:09 UTC	14	–	–
Locky Affid=3 - 25th August	📎	🌐	2016/08/25 - 19:02 UTC	1000+	–	–
Cerber "004610b" and "005c942" -	📎	🌐	2016/08/25 - 18:04 UTC	8	–	–
Linkedin Account Phishing - August 2016	📎	🌐	2016/08/25 - 13:01 UTC	11	–	–

Source: ProofPoint

Business Risk – Theft

The Bangladesh Bank Heist

The Act …

- Hackers attempted to steal a total of $1 billion through 35 international money transfer orders.
- Five transactions, worth $101 million, were withdrawn from an account at the Federal Reserve Bank of New York, succeeded by using the Swift interbank messaging system to move cash into fake accounts.
- $81M Lost

How did it happen?

- Months of preparation
- False accounts, false IDs
- Theories still under investigation:
  - Malware
  - False internal network
  - Thumb Drive Virus

The fallout …

- Havoc through the exposure of crucial weaknesses in the global financial system
- Congressional hearings
- Political unrest between nations

Vignette 3 – Theft

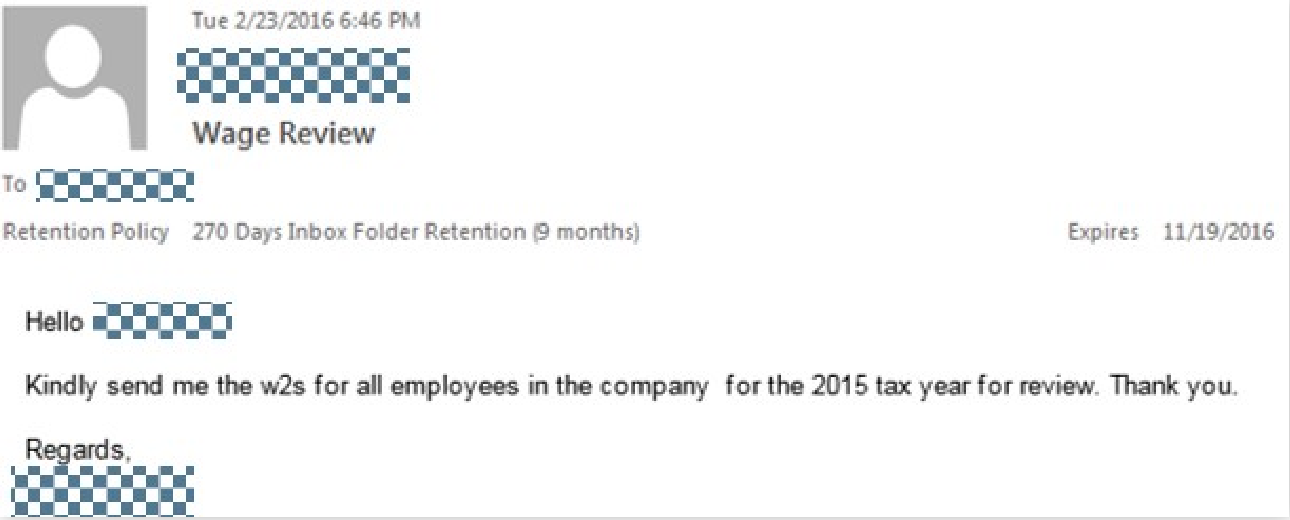
Business Email Compromise – Wire Transfer Fraud

- Cyber thieves research a company’s organizational structure and begin compromising systems via email.
- After analyzing emails for wire transfers, they register domains similar to the organizations they are targeting and open temporary bank accounts.
- Fraudulent emails are sent to both companies:
  - Company A – Redirect payment to a new bank account
  - Company B – Please excuse our delay
- Once monies are sent to the fraudulent bank account, the monies are withdrawn and all accounts (bank and domain) are cancelled.

Business Controls

- Employee Awareness
- Domain Registration Monitoring
- Email Imposter Controls
- Wire Transfer Policies

What Does an Impostor Email Look Like?



Tue 2/23/2016 6:46 PM

[redacted]

Wage Review

To [redacted]

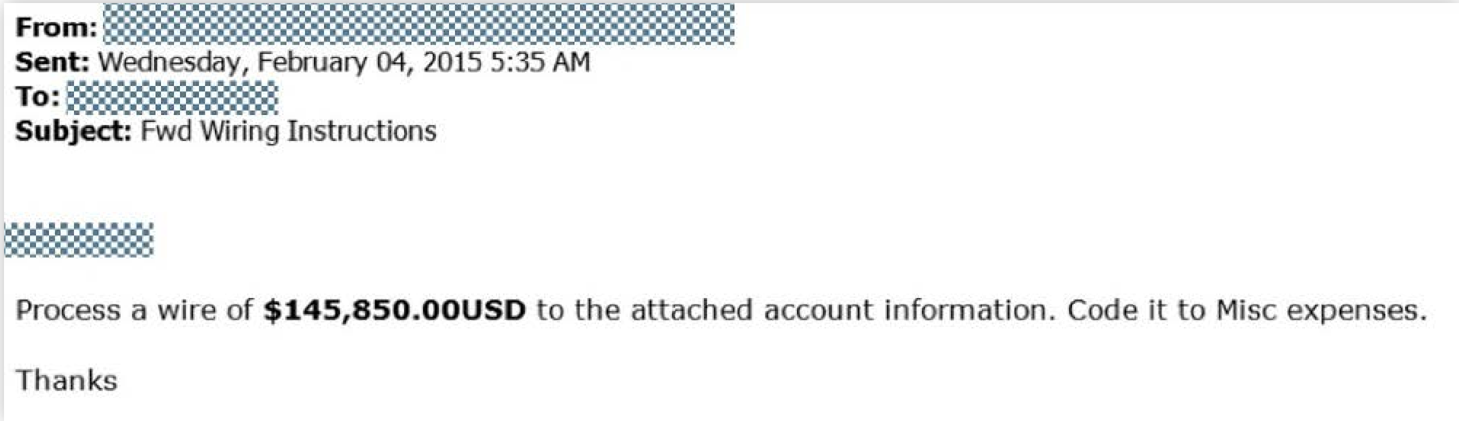
Retention Policy 270 Days Inbox Folder Retention (9 months) Expires 11/19/2016

Hello [redacted]

Kindly send me the w2s for all employees in the company for the 2015 tax year for review. Thank you.

Regards,

[redacted]



From: [redacted]
Sent: Wednesday, February 04, 2015 5:35 AM
To: [redacted]
Subject: Fwd Wiring Instructions

[redacted]

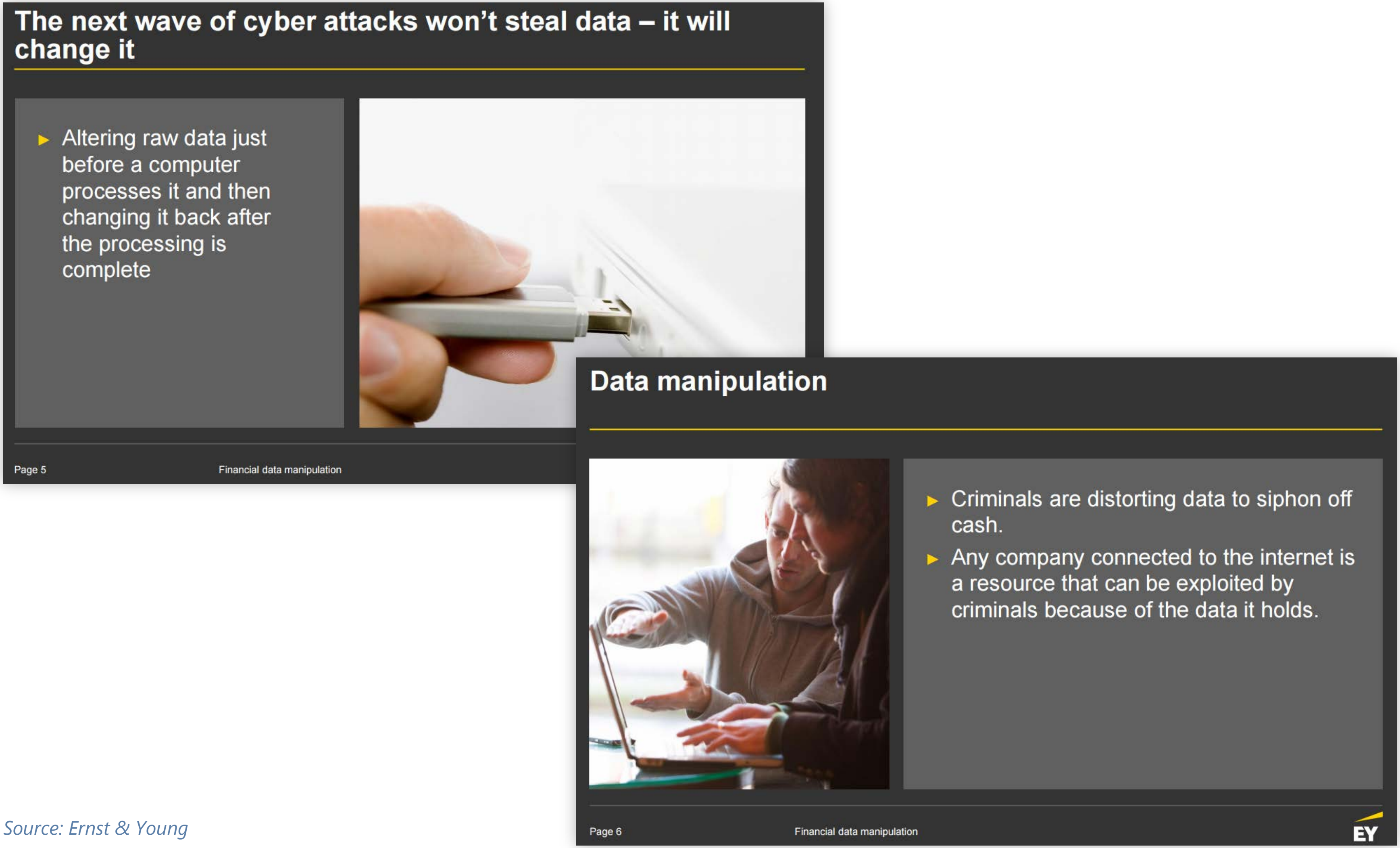
Process a wire of **$145,850.00USD** to the attached account information. Code it to Misc expenses.

Thanks

Source: ProofPoint

Business Risk – Loss of Information Integrity

Newest Cyber Threat



The next wave of cyber attacks won't steal data – it will change it

- Altering raw data just before a computer processes it and then changing it back after the processing is complete

Page 5 Financial data manipulation

Data manipulation

- Criminals are distorting data to siphon off cash.
- Any company connected to the internet is a resource that can be exploited by criminals because of the data it holds.

Page 6 Financial data manipulation

Source: Ernst & Young

Loss of Information Integrity

Data Manipulation

Scenario

- A threat actor, motivated by financial gain, decides to focus on a company that is about to release its quarterly results. The numbers are modified just before public release.
- In addition, CEO communications are modified (or created) to add credibility to the information.
- As the results are unexpected, the stock price is impacted and the threat actor profits from the temporary change in stock price.

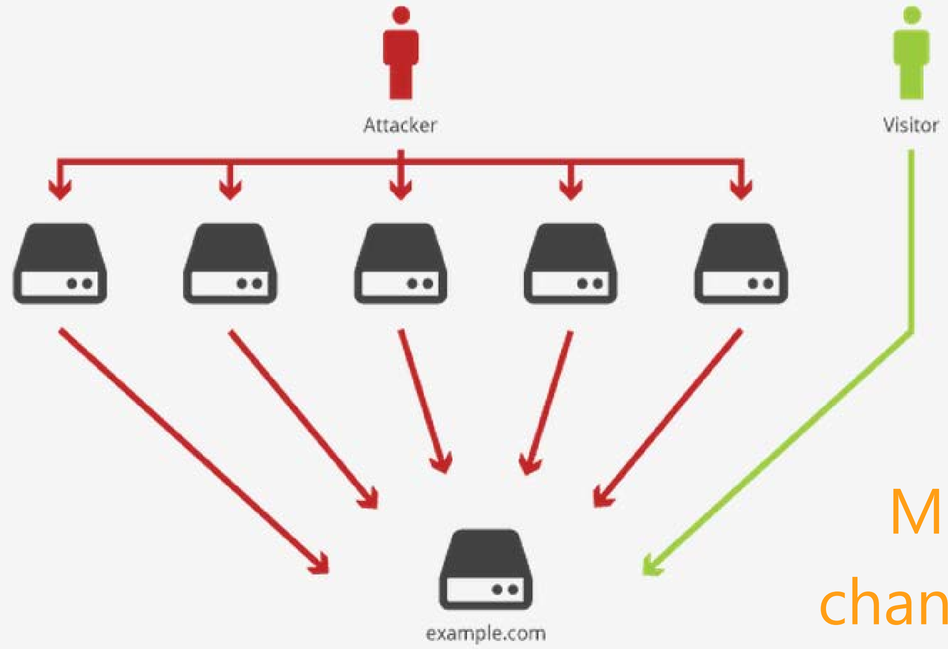
Variations

- Outsider or insider
- Widespread or targeted
- Creates or updates health records, account balances, records of ownership, or software
- Impacts past and/or current transactions, including transactions in backups
- Manipulates data on websites
- Used in combination with other methods

Business Risk – Business Interruption

Distributed Denial of Service (DDoS)

Globally distributed sites are used to flood our external network resources keeping our customers from accessing our external facing websites and anyone from working remotely through our VPN.



Motivation is often social change but could be financial.

DYN Attack is new approach to DDoS using Internet of Things (IOT)

Vignette 4 – Denial of Service Attack

Email Threat

PLEASE FORWARD THIS EMAIL TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE IMPORTANT DECISIONS!

- We are the Kadyrovtsy and we have chosen <REDACTED> as target for our next DDoS attack. All of your servers will be subject to a DDoS attack starting at Thursday the 12th of May.
- Right now we are running a small demo attack on <REDACTED IP> for 1 hour to prove that this is not a hoax.

What does this mean?

- This means that your website and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation amongst your users / customers as well as strongly hurt your Google rankings (worst case = your website will get de-indexed).

How do I stop this?

- We are willing to refrain from attacking your servers for a small fee. The current fee is 20 Bitcoins (BTC). The fee will increase by 20 Bitcoins for each day that has passed without payment.
- Please send the bitcoin to the following Bitcoin address: 1Eg5e3XVTe7wsiFbJx9eCdH4mWaNE9r54C

Business Controls

- Invoke Legal / Law Enforcement notification procedures
- Alert Internet Service Providers
- Increase network and website monitoring
- Rapid response team

Summary

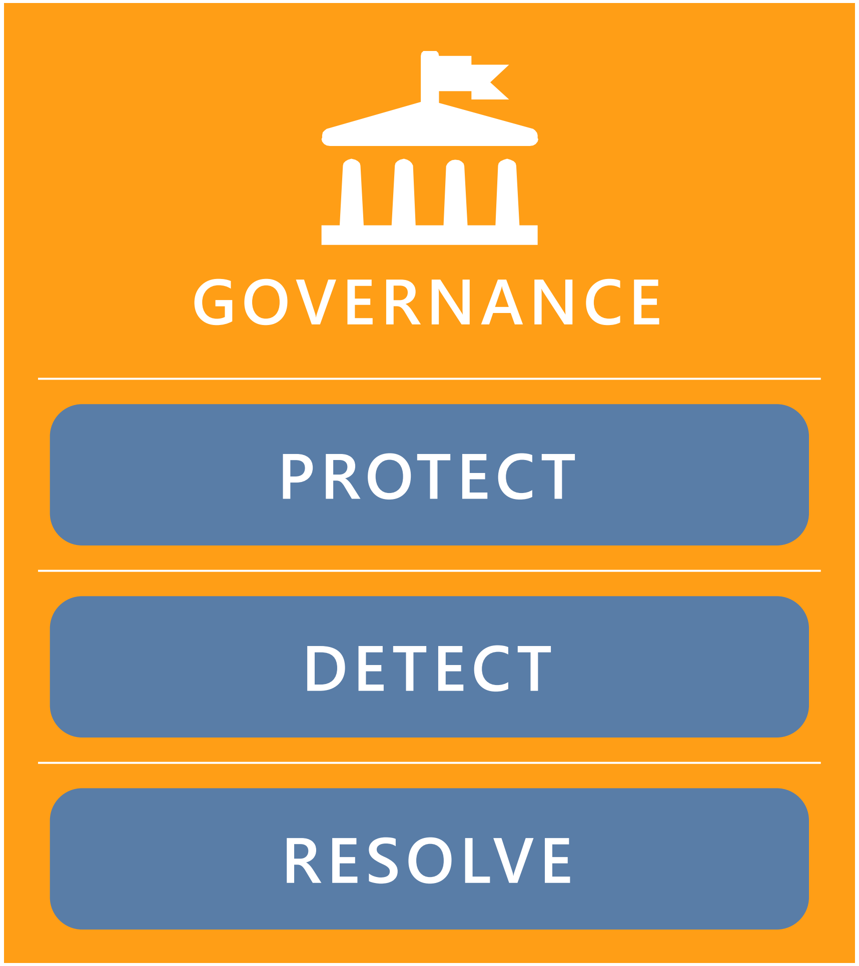
Cyber Security Risks at Gen Re

Ranking

Business Risk	Method	Likelihood	Impact	Rank
Loss of Protected or Privileged Records	Data Breach			1
Extortion	Ransomware			2
Theft	Business Email Compromise (BEC)			3
Loss of Information Integrity	Data Manipulation			4
Business Interruption	Denial of Service			5

Security Framework

Framework Overview



GOVERNANCE

PROTECT

DETECT

RESOLVE

Alignment with NIST Cyber Security Framework and join security groups (e.g., FS-ISAC and LOMA)

Minimize the number of security incidents

Identify potential and actual security incidents

Respond effectively to incidents

Framework Controls

PROTECT		DETECT	RESOLVE
Virus Control	Email/Spam Filtering	Pen Testing	24/7 SOC
Basic Access Management	Firewall	IDS/IPS	Incident Response
Content Filtering	Data Loss Prevention	Threat Processing	Scenario-based Training
Vulnerability Management	Privileged Access Management	Rights Monitoring	Denial of Service Defense
Encryption	Email Attack Protection	Security Assessments	Forensics
Data Classification	Security Awareness	Cloud Security	
Network Segmentation	Multi-Factor Authentication	Mobile Security	
IDAM & Single Sign-on	Network Access Control	Anomaly/End Pt. Detection	
Configuration Management & Hardening	Security Skills Training (IT)	Extranet Monitoring	

🟩 Implemented

🟨 Partially Implemented

🟥 Not Implemented Yet

Layer of Defense – Business Email Compromise

PROTECT		DETECT	RESOLVE
Virus Control	Email/Spam Filtering	Pen Testing	24/7 SOC
Basic Access Management	Firewall	🟩 IDS/IPS	🟩 Incident Response
Content Filtering	Data Loss Prevention	Threat Processing	Scenario-based Training
Vulnerability Management	Privileged Access Management	Rights Monitoring	Denial of Service Defense
Encryption	🟩 Email Attack Protection	Security Assessments	Forensics
Data Classification	Security Awareness	Cloud Security	
Network Segmentation	Multi-Factor Authentication	Mobile Security	
IDAM & Single Sign-on	Network Access Control	Anomaly/End Pt. Detection	
Configuration Management & Hardening	Security Skills Training (IT)	Extranet Monitoring	

🟩 Implemented
🟨 Partially Implemented
🟥 Not Implemented Yet

Calendar – 2016

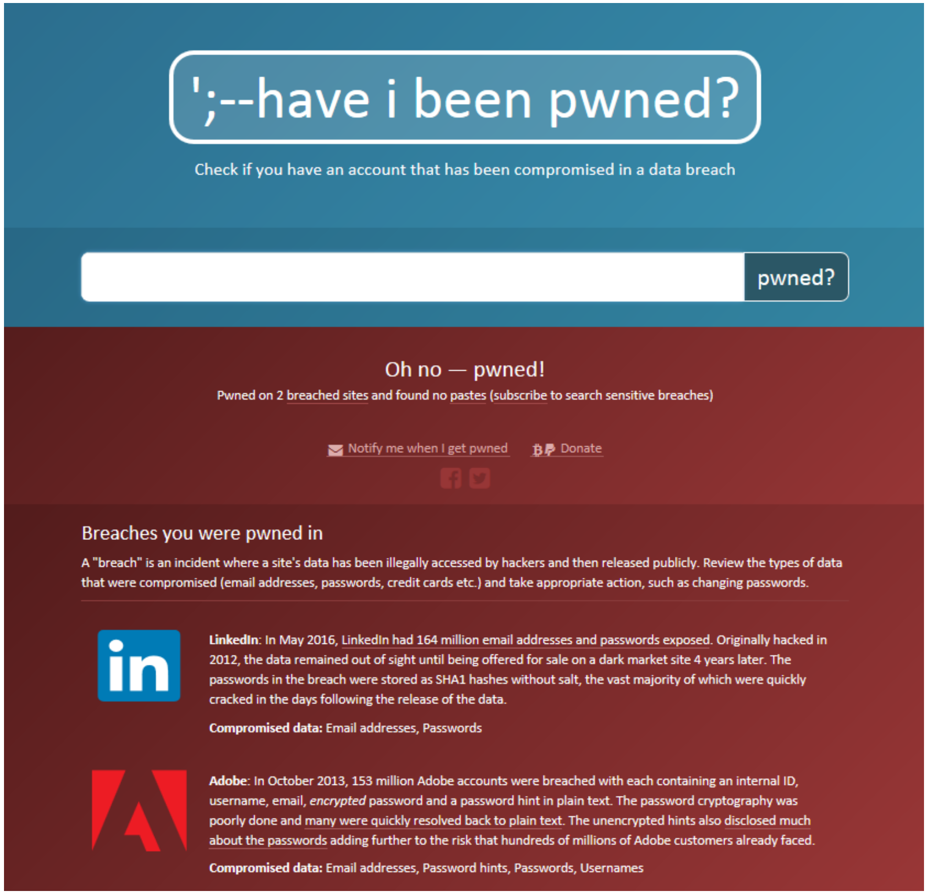
Gen Re Security Awareness

GISS GLOBAL INFORMATION SECURITY SERVICES

JAN	New Year's Security Resolutions Email for all
FEB	Wire Transfer Awareness
MAR	Training Session for IT Technical Leads
APR	Pilot new End User Computer Based Training
MAY	Security Spring Cleaning Email for all
JUN	Updated End User Policy SharePoint Site Email to all
JUL	Updated Gen Re + new Faraday and G2 Screen Saver
AUG	Passwords
SEP	Updated Business Owned Technology and Services Policy
OCT	Corporate Incident Response Plan Exercises
NOV	Updated IT Security Policy and Understanding Survey
DEC	Holiday Security Tips Email for all

Some Tips

Have my credentials been stolen?
https://haveibeenpwned.com



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

Oh no — pwned!

Pwned on 2 breached sites and found no pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

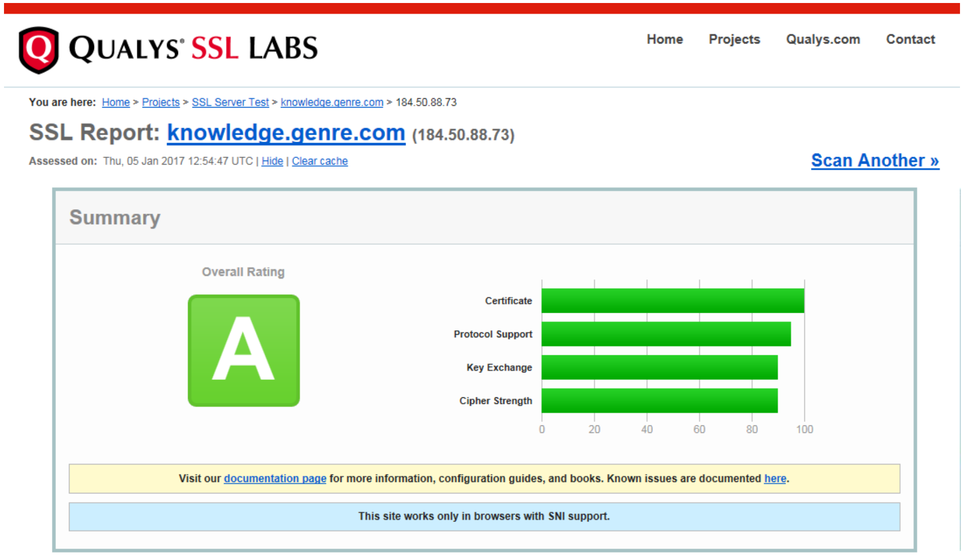
Compromised data: Email addresses, Passwords

Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

Source: Have I been pwned?

Some Tips – Is My Website Secure?



You are here: Home > Projects > SSL Server Test > knowledge.genre.com > 184.50.88.73

SSL Report: knowledge.genre.com (184.50.88.73)

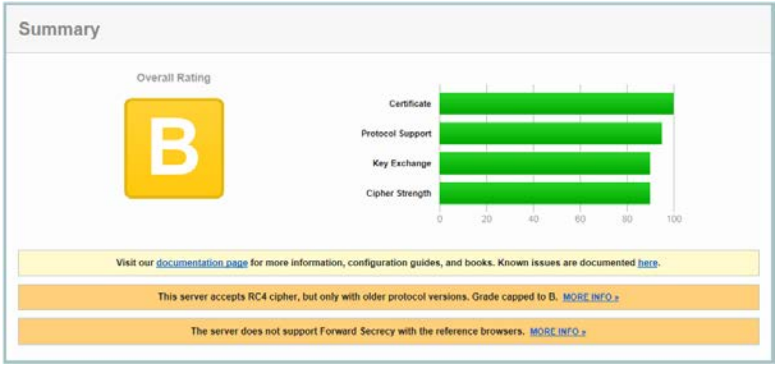
Assessed on: Thu, 05 Jan 2017 12:54:47 UTC | Hide | Clear cache

Scan Another »

Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

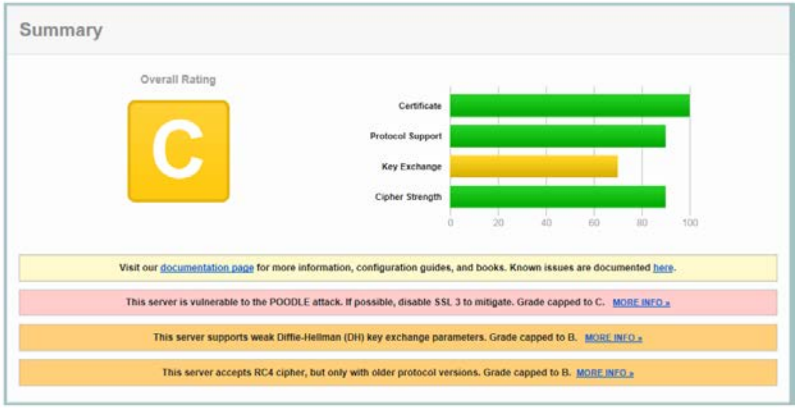
This site works only in browsers with SNI support.


Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server accepts RC4 cipher, but only with older protocol versions. Grade capped to B. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

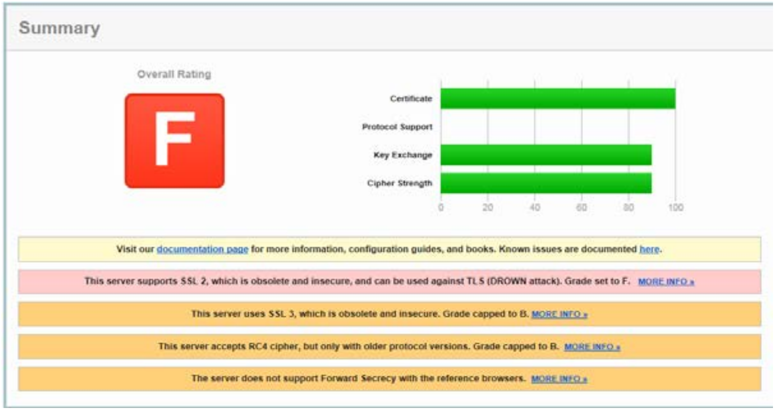

Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. MORE INFO »

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

This server accepts RC4 cipher, but only with older protocol versions. Grade capped to B. MORE INFO »


Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports SSL 2, which is obsolete and insecure, and can be used against TLS (DROWN attack). Grade set to F. MORE INFO »

This server uses SSL 3, which is obsolete and insecure. Grade capped to B. MORE INFO »

This server accepts RC4 cipher, but only with older protocol versions. Grade capped to B. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

Source: SSL Labs

Thank You