

INTERNATIONAL **DIRECTORS** SUMMIT 2019

The Trust Compass: Resetting the Course

14 & 15 OCT 2019 | Shangri-La Kuala Lumpur

CYBER VIGILANCE: HOW MUCH SHOULD WE KNOW?

By: Chris Sturgess

Why listen to me on Cyber Security?

- Joined the British Government
 - At 17 years old
 - Hacked for them for 15 years
- Includes National Cyber Security Centre
 - Get other Govt. hackers out of UK critical systems



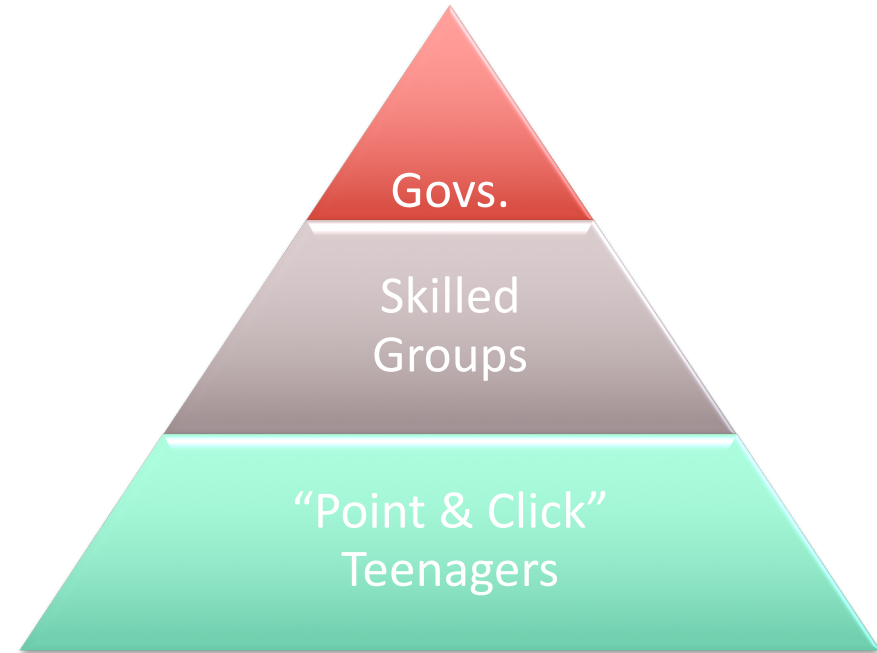
Clearwater Digital

- Maritime Intelligence Company
 - Cyber Security: Oil & Gas, Insurance, Shipping
 - Malaysia, Norway, London
- Clearwater Digital
 - Tech Startup
 - Cloud cyber security
 - Business Email Compromise & Invoice Fraud mitigation

clearwaterdigital.io

Summary – The Cyber Threat

- There are many different cyber threats
- You are more likely to face threats from
 - A bored teenager
 - A Nigerian fraud gang
- Lots of media focus on Government
 - Deal with the easier threats first



Risk Management Approach

- You will never be 100% secure or “hack proof”
- Risk management
 - What skill and capability is required
 - And how long did it take?
 - Did it take a teenager 2 hours or a government 4 weeks?
 - Don’t treat cyber security as just an “IT problem”
- Risk Impact
 - Will key stakeholders think you took ‘reasonable measures’?
 - Insurance Companies & Regulators

INTERNATIONAL **DIRECTORS** SUMMIT 2019

The Trust Compass: Resetting the Course

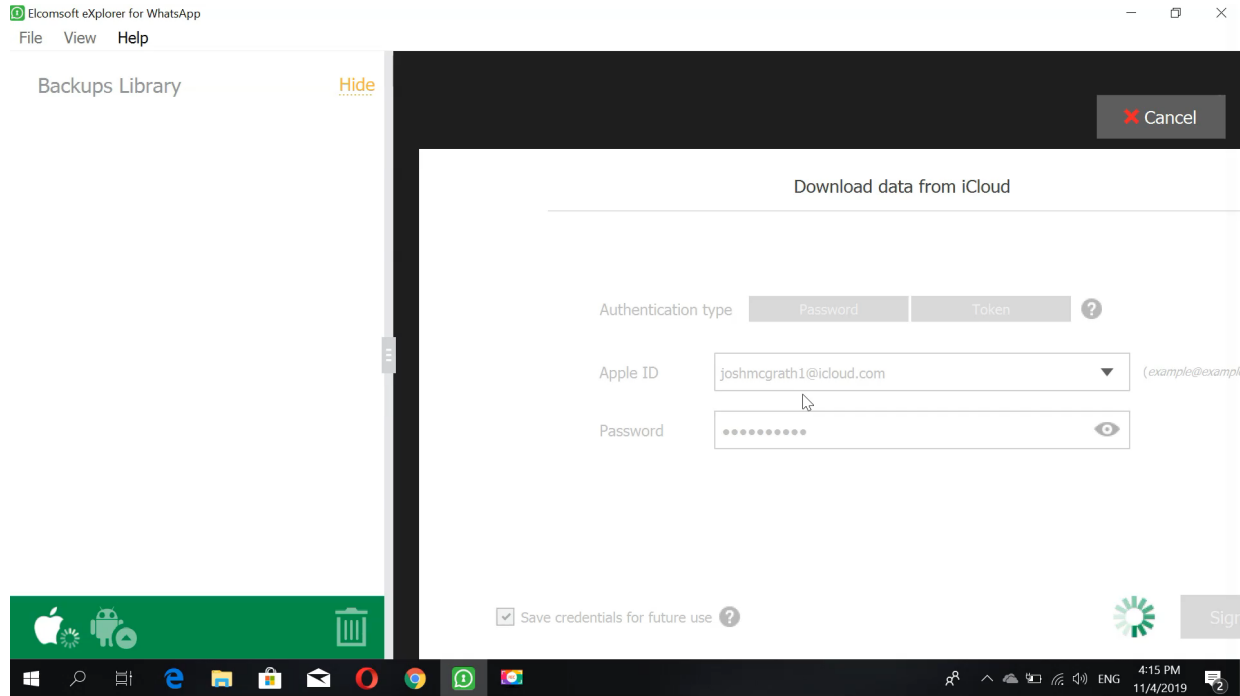
14 & 15 OCT 2019 | Shangri-La Kuala Lumpur

Demo – Hacking WhatsApp

Hacking tools – it's about money.



WhatsApp Hack



'Encrypted' Messaging Considerations

- Many use WhatsApp for business
 - It can be hacked
 - It can end up in court
- The board should always know
 - How is the data stored?
 - Where is it stored?
 - What legal jurisdiction does the company operate under?

DATA DILEMMAS

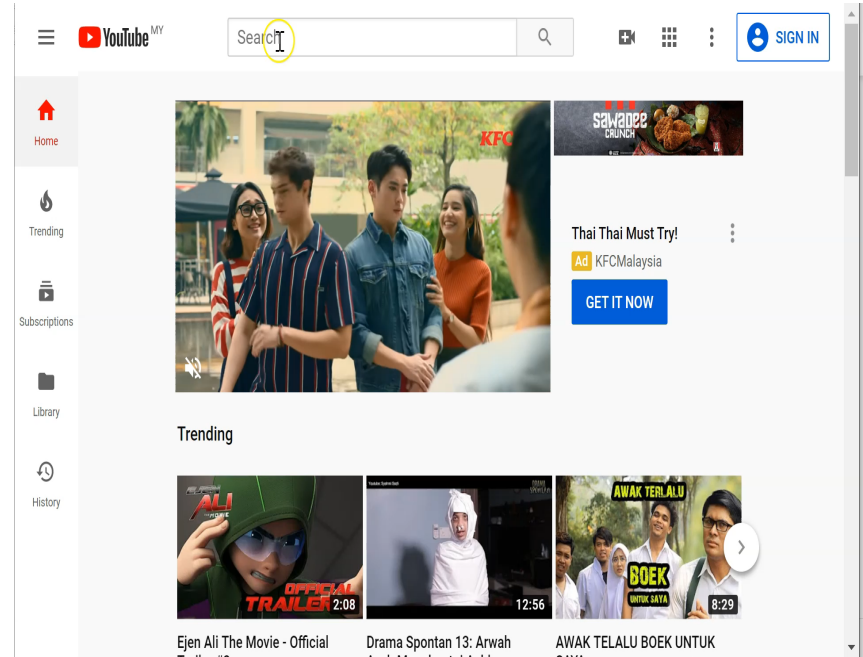
Apple's iCloud service in China will be managed by a data firm started by the government

Sony Film Executives Apologize for Racially Tinged Emails About Obama

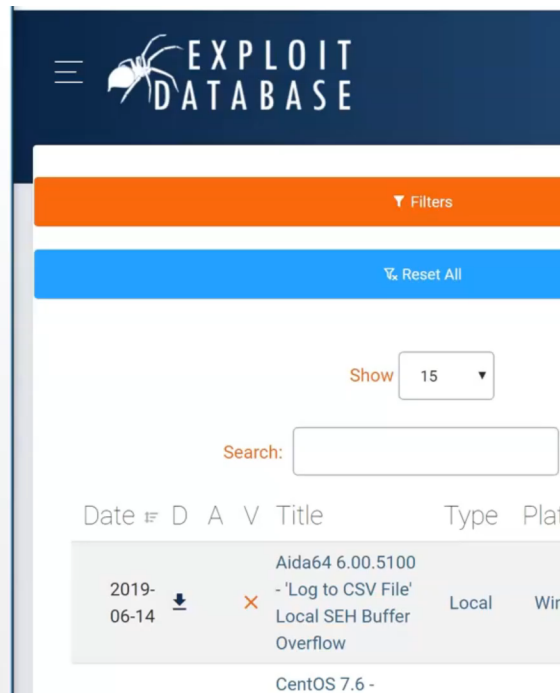
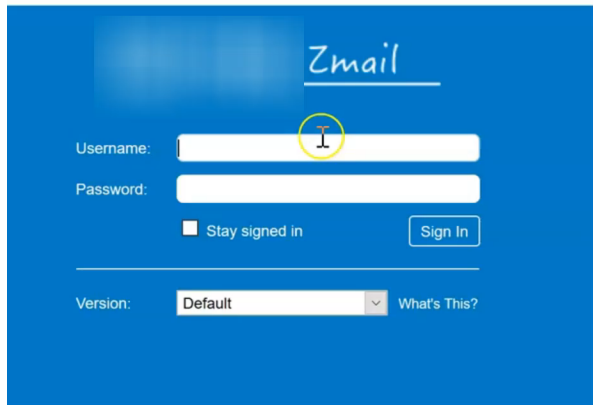
By Brooks Barnes and Michael Cieply

Teenage Hackers

- Simple hacks
 - Mostly following Youtube videos
 - Thousands of bored teenagers doing this every night
- Common scenario
 - Your system was secure on day one
 - 4 years later, not updated
 - Human error during a change
 - More common with move to cloud computing



Real World – Hacking corporate email in <5minutes



Teenage Hackers - Impact

- Often motivated by attention
 - May leak their hacks to the IT Media/Press
 - Dump personal data on the Internet
 - Highly embarrassing
- What if it's a 3rd party supplier?
 - Who do the journalists call?
 - Who gets the PR damage?

TECHNOLOGY

Personal data on 202 million Chinese job-seekers left exposed on insecure database

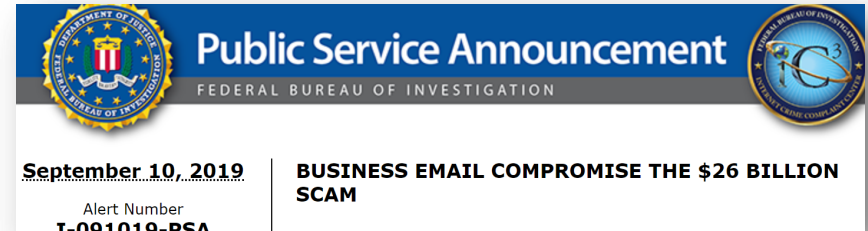
In early September, security researchers spotted that 30 million records from Malindo Air, as well as fellow Lion Air subsidiary Thai Lion Air, were posted on online forums. The files appear to have been left on a publically available online server.

Teenage Hackers – Mitigation?

- This is already happening to you
 - You just don't know if they are getting in or not!
- Recommendation
 - Develop a continuous vulnerability scanning programme.
 - Include your 3rd party provided IT systems if possible.
 - Integrate the findings into corporate risk management.
 - Fix embarrassing issues before someone else finds them.

Business Email Compromise (BEC)

- Hacking to steal money
 - Invoice Fraud
 - Salary Fraud
 - Mortgage Fraud
- Estimate \$300m dollars moved each month
 - Source: US Govt.
- Likely the biggest cyber risk to most orgs.



BEC – What’s the impact?

- 24 hours after you send the money, low chance of recovery
 - Difficult for police
- Can cause conflict with business partners
 - Who was hacked? Us or our supplier? Or both?
- Are you covered by your insurance provider?
 - Are you really sure?
 - Do they have a “**reasonable protection measures**” clause?

Who is behind Business Email Compromise?

- Need a country with 'relaxed' banking compliance
 - Nigeria
 - Eastern Europe
- Target English language transactions
 - South East Asia highly attractive

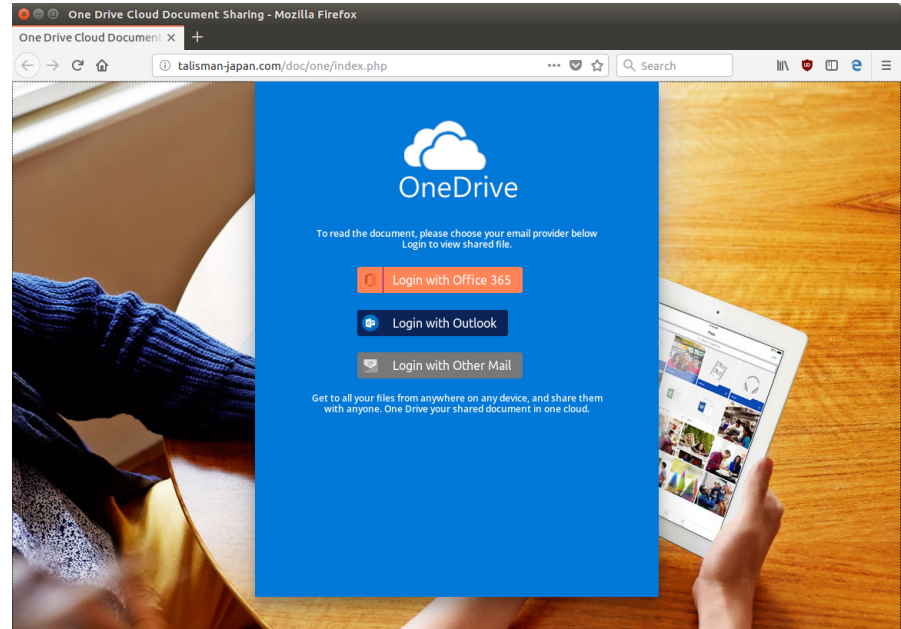


How do they target?

The image shows a screenshot of a LinkedIn profile for Shangri-La Hotels and Resorts. The profile header includes the LinkedIn logo, a search bar, and navigation icons for home, network, company, messages, and notifications. The main content area features a blue background image of a resort. The company logo is a gold shield with a white mountain range. The company name is "Shangri-La Hotels and Resorts" and the location is "Hospitality · Quarry Bay · 454,987 followers". The bio reads: "Welcome to Shangri-La Hotels and Resorts. A global luxury hotel group where ho from the heart is in our nature." Below the bio are buttons for "+ Follow", "Visit website", and "Messaging". A yellow circle highlights a cursor hovering over the company logo.

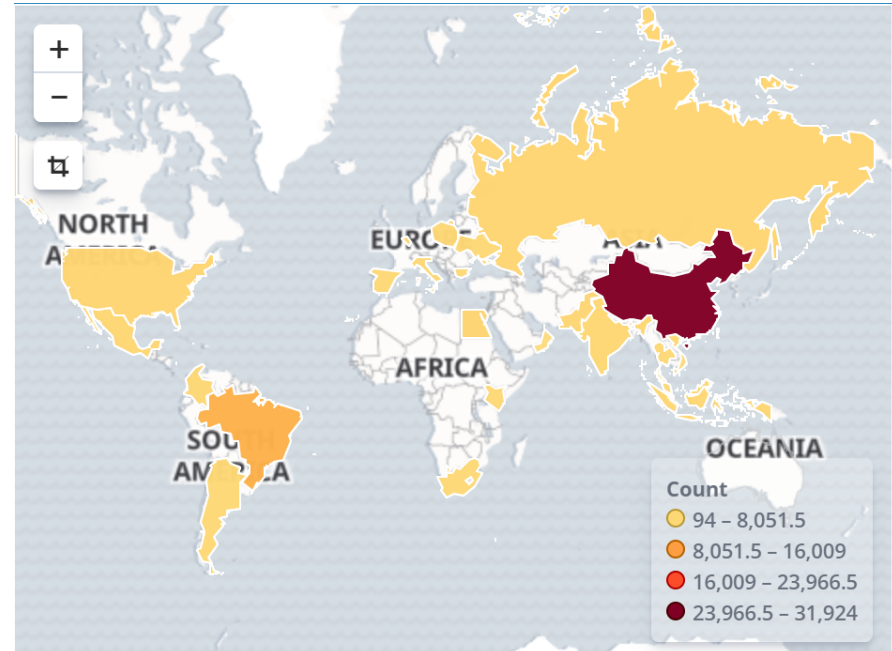
Phishing

- Phishing = Some type of malicious email
- Normally a fake login page
- They look very realistic
 - Clever people will fall for it
- Hacker has your password



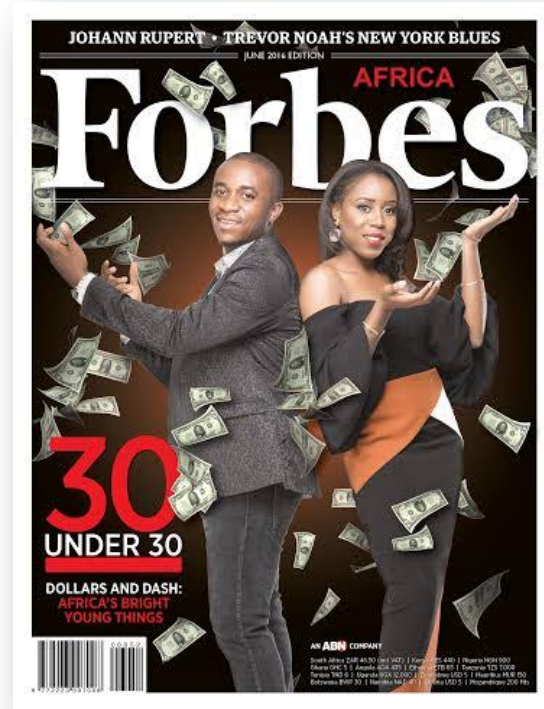
Automated Hacking

- We monitor Office365 & Gsuite for clients
 - 50,000 password hack attempts every week / every client
- Board visibility
 - How many of your finance staff are logging in from Nigeria today?
- How many staff have **Company2019!** as their password?
 - **Normally 2% <-> 8%**



Detection Case Study – Invictus Obi (Alleged*)

- US/UK Construction Company
- CFO's Office365 accessed at least 464 times from Nigeria
 - Email and OneDrive documents.
- Many hackers do not care about their footprint
 - They assume no one is watching
 - Often true!
- They lost approx. \$11M USD.



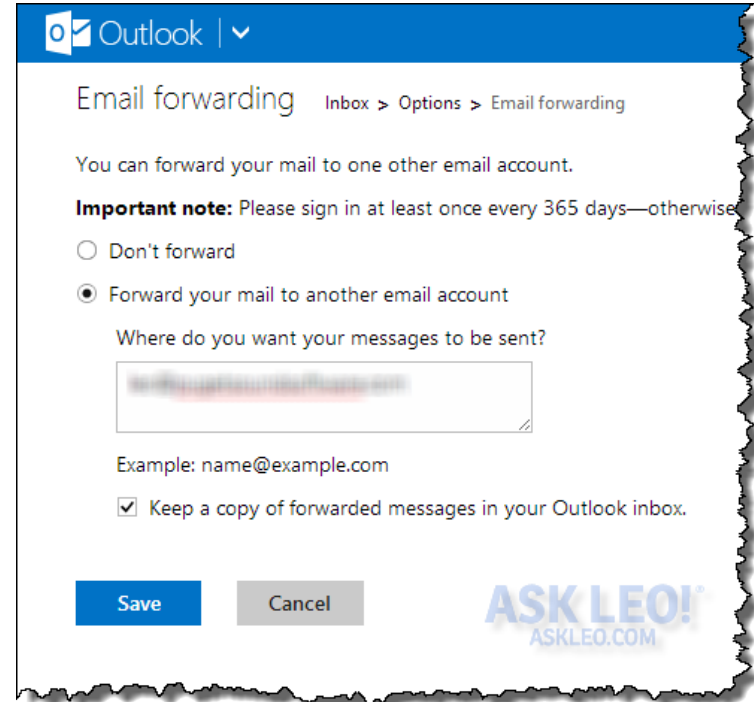
What information do they want?

- Control of the email accounts of **anyone** who
 - Handles financial transactions
 - Authorizes payments or invoices
 - They will download everything
- Use technology to **exploit Trust**
 - Pose as your employees
 - Manipulate the emails they can read

email that fraudulently acquired sensitive log-in details of their Chief Financial Officer (CFO). Posing as the CFO, the intruder then sent wire transfer requests to the Unatrac internal Finance team leading to several transfers amounting to \$11 million (N3.9 billion).

But we changed the passwords?

- Email Forwarding
 - All your CFO's email is automatically forwarded to a Hotmail account
 - There is no notification to the hacked employee
- Is this happening in your company?
 - Hackers
 - Employees sending company data to personal accounts

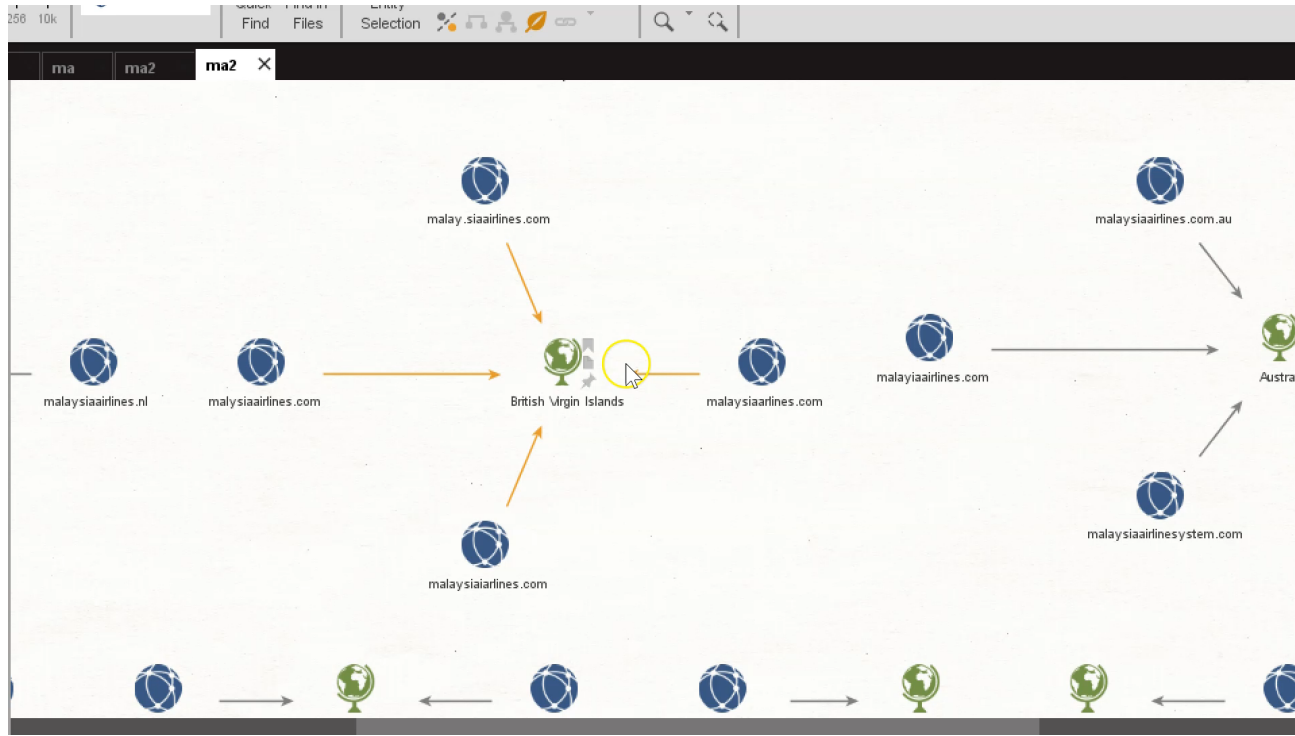


You kicked them out?

- They buy a misspelled version of your company domain
 - Easy, cheap and anonymous
 - E.G **malaysia-airlines.com**
- They already
 - Have documents and email signatures
 - Know your business processes
- The email your employees or your customers from fake domain
 - Ask to change bank account

```
Registrant Fax Ext: [REDACTED]  
Registrant Email: elvisstaff@outlook.com [REDACTED]  
Registry Admin ID: Not Available From Registry  
Admin Name: Elvis Staff [REDACTED]  
Admin Organization:  
Admin Street: 67 crecent ajegunle  
Admin City: ikeja  
Admin State/Province: Lagos  
Admin Postal Code: 100032  
Admin Country: NG  
Admin Phone: +234.80564863247
```

Real Life Example



Impacts – Business Email Compromise

- Would the banks stop this? KYC etc?
 - Often not
 - Scammers may use a Malaysian bank account
- Do you tell your customers if you are hacked?
 - Difficult decision for senior management.
- Did a supplier complain they have not been paid after a bank account change request?
 - Recommend you investigate for signs of intrusion into **your** network.

BEC - Key Corporate Considerations

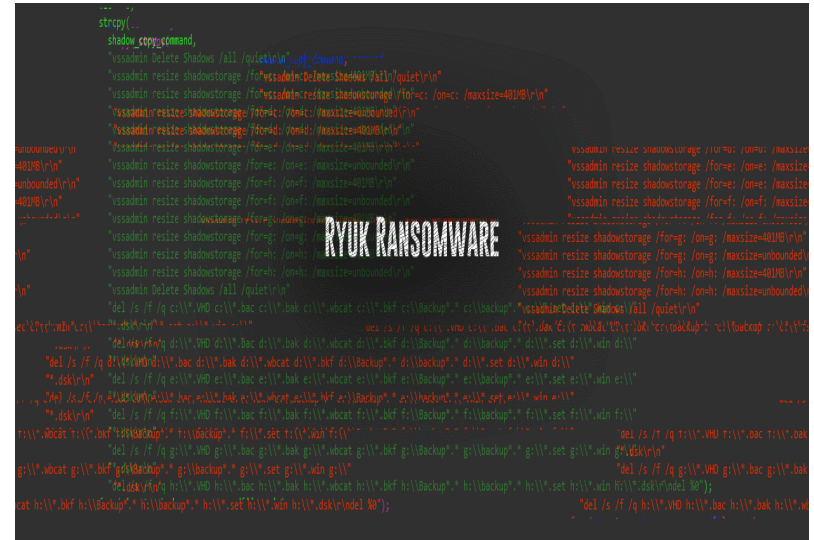
- Clever people will fall for phishing attacks
 - If people are scared to report internally, it helps the scammers.
- This is more than just **“IT’s problem”**.
 - Information sharing after a suspicious event can improve vigilance.
 - This more about people and trust than “just IT”.
- Never just change a password and forget about it.

BEC - Future Threat Landscape

- Most companies are moving IT to the cloud
 - Office 365 / Google Gsuite etc
- Every cloud-powered organisation has very similar technology
 - Easy for hacking groups to scale attacks
 - They don't have to spend time learning internal networks
- Do not assume moving to the cloud will solve all your security problems
 - Your personal email account will probably alert if you login from a home country
 - Your corporate Office365 will let your account be accessed from Nigeria without a warning

High Skill Hacking Groups

- The “ransomware” industry
- Ransomware?
 - All/Most your machines are encrypted
 - All/Most of your backups are encrypted
- Extortion demand
 - If you pay, you get a ‘key’ to unlock the data
 - 1-year tech support!



The image shows a screenshot of a ransomware script, likely written in PowerShell. The text is mostly red and white on a black background. A prominent watermark in the center reads "RYUK RANSOMWARE". The script contains various commands, including "steeply", "shadow streptomid", "ssadmin Delete Shadow /all /notclean /copy /comany", and several "ssadmin resize shadowstorage" commands with different parameters like "/formci", "/formc", "/formci /omaxsize=4096", and "/formci /omaxsize=unbounded". There are also "ssadmin Delete Shadow /all /quiet" commands. The script appears to be designed to manage shadow copies and perform encryption operations.



Famous Incidents

CYBER RISK

SEPTEMBER 6, 2018 / 3:13 PM / A YEAR AGO

U.S. charges North Korean hacker in Sony, WannaCry cyberattacks

Norsk Hydro ransomware incident losses reach \$40 million after one week

Who?

- Highly skilled hackers
 - Mostly Russian, Chinese and some Iranians
- Use the hacking techniques that invoice fraudsters use
 - Then some extra ones
- But they need less financial scamming skill
 - As they ask to be paid in crypto-currency

The New York Times

Obama and Xi Jinping of China Agree to Steps on Cybertheft

 REUTERS



TECHNOLOGY NEWS

AUGUST 7, 2019 / 2:31 PM / 2 MONTHS AGO

Chinese government hackers suspected of moonlighting for profit

How?

- Malware sent via email
 - Might only work < 0.5%
- Automatically emails the malware to everyone in your contact list
- If they can't get bank account logins
 - You are “traded” to a ransomware gang

A graphic with a blue and white background featuring a keyboard. The text is centered and reads: **TrickBot malware may have hacked 250 million email accounts**

**TrickBot malware may have hacked
250 million email accounts**

Including millions belonging to governments in the US, UK and Canada.

Execution

- They will take control of your IT staff accounts
 - Achieve full control over your IT network and backup system
 - If this takes too long, they will move on to someone else!
- Ransomware will encrypt everything at the same time
- You will come in to a extortion message
 - With a crypto-currency demand

Impact

- Many orgs assume their backups are tamper proof
 - Then are horrified when they are gone also
- Pay the extortion threat?
 - Speak to a lawyer.
- If you respond well, reputational damage may not be catastrophic.
 - Norsk Hydro (Norway) seen as responding well.

Ransomware - Mitigation Strategies

- What does your insurance provider think?
 - Do they class this as cyberwarfare?
- ‘Red Teaming’
 - **“Trust but verify”** board level approach to IT/suppliers
 - Emulate the attacker
 - Or get ask someone in to ask probing questions
- ‘Scenario Planning’
 - If this happens to us, how quickly can we get up and running?
 - Do we have a disaster response plan?

Ransomware – Mitigation Strategies (2)

- These are technically far more advanced than teenagers or cyber-fraudsters
 - Your IT network will need to have very good defenses
- Are you sure your data backups cannot be tampered with?
 - Did someone tell you it would be OK?
 - Or did you test it?
 - If your IT supplier tells you this, what do you have in your contracts?

Governments

- Most
 - Not interested in 99% of companies
 - Won't steal your money or break your IT

- Some
 - Might steal your money
 - Use you in a wider cyber conflict (Iran & Saudi)

4,563 views | Mar 11, 2019, 12:00pm

North Korean Hackers Have Raked in \$670 Million Via Cyberattacks



Lee Mathews Contributor

Security

Observing, pondering, and writing about tech. Generally in that order.

Shamoon malware destroys data at Italian oil and gas company

About a tenth of Saipem's IT infrastructure infected with infamous data-wiping Shamoon malware.

Governments (2)

- A few
 - Might steal your Intellectual Property for their own industries
- Not about aircraft designs anymore!

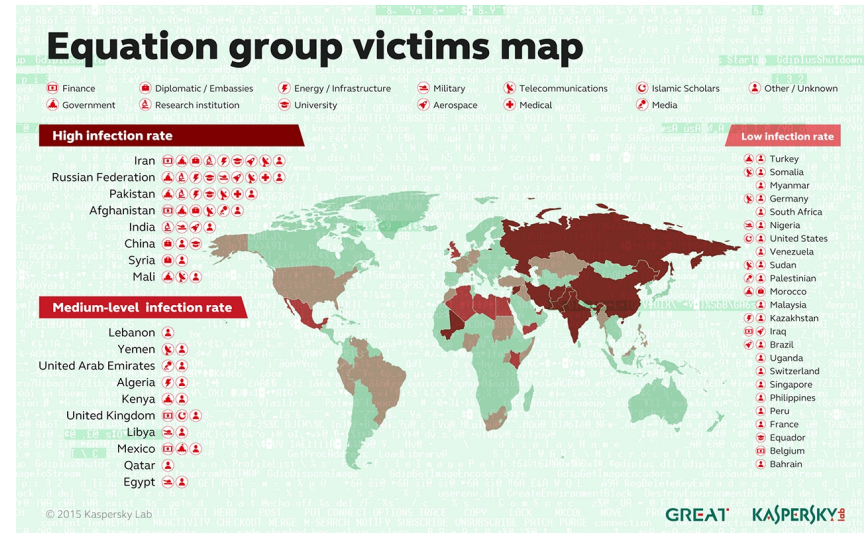
Cybersecurity

Vietnam ‘State-Aligned’ Hackers Are Targeting Auto Firms, FireEye Says

60 Minutes Investigates Chinese Cyber-espionage in Wind Industry

Government Hacking – Key Considerations

- If a Government is uses an expensive hacking tool, they risk
 - Getting attributed & losing the tool
- They will try to use the same tools as Teenagers & Nigerian Fraudsters first
 - I recommend you mitigate those threats first



Real World Government Case Study

ANDY GREENBERG

SECURITY 10.04.2018 01:41 PM

How Russian Spies Infiltrated Hotel Wi-Fi to Hack Victims Up Close



Further investigation revealed that one of the Russian intelligence officers operating in the Netherlands had also been active in Malaysia, targeting the investigation of the crash of Malaysia Airlines

Hacking on the Hotel WiFi

```
root@cpentest: /pentest/exploitation/responder
File Edit View Search Terminal Tabs Help
root@cpentest: /pentest/exploitation/gladius
SMB server [ON]
Kerberos server [ON]
SQL server [ON]
FTP server [ON]
IMAP server [ON]
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]

[+] HTTP Options:
Always serving EXE [OFF]
Serving EXE [OFF]
Serving HTML [OFF]
Upstream Proxy [OFF]

[+] Poisoning Options:
Analyze Mode [OFF]
Force WPAD auth [OFF]
Force Basic Auth [OFF]
Force LM downgrade [OFF]
Fingerprint hosts [OFF]

[+] Generic Options:
Responder NIC [wlan0]
Responder IP [192.168.1.2]
Challenge set [1122334455667788]
Don't Respond To Names ['ISATAP']

[+] Listening for events...
[*] [LLMNR] Poisoned answer sent to 192.168.1.5 for name LAPTOP-844N1RR6
[*] [LLMNR] Poisoned answer sent to 192.168.1.5 for name LAPTOP-844N1RR6
[*] [MDNS] Poisoned answer sent to 192.168.1.5 for name LAPTOP-844N1RR6.local
[*] [LLMNR] Poisoned answer sent to 192.168.1.5 for name LAPTOP-844N1RR6
```



Mergers & Acquisitions

- M&A is a very complicated IT problem
 - “temporary fixes” are done
- If your secure & modern IT network is ‘joined’ to another network
 - The hacker can just jump across

05 Target Hackers Broke in Via HVAC Company

FEB 14

Last week, **Target** told reporters at *The Wall Street Journal* and *Reuters* that the initial intrusion into its systems was traced back to network credentials that were stolen from a

Government Hacking – Key Considerations (2)

- Protect against the teenagers, fraudsters and ransomware gangs first
- Then you force the Governments to use their advanced tools
 - 95% of companies will not be reasonably expected to prevent this
- Then you need help from your Government.

Recommended Actions

- For these cyber threats
 - What insurance do you have and what clauses are there?
 - What is in place with your third-party suppliers?
 - When was your disaster recovery plan last practiced?
- Your data
 - Where is it? What legal jurisdiction?
 - Who's accessing it? Did your CFO really log in from Nigeria this morning?

Summary

- Key Questions
 - How long did it take the hackers?
 - What grade of skills and tools did they use?
 - Did it take a teenager 2 hours or a Govt. 4 weeks?
- What is your risk tolerance?
 - Key stakeholders – Board, Investors / Major Shareholders / Regulators
 - How good are our competitors?
 - Your Insurance provider
- Cyber Security is not just an “IT problem”

Questions?

<http://clearwaterdigital.io>

chris.sturgess@clearwaterdigital.io

INTERNATIONAL **DIRECTORS** SUMMIT 2019

The Trust Compass: Resetting the Course

14 & 15 OCT 2019 | Shangri-La Kuala Lumpur

THANK YOU