ASCO - IT Security for Intermediaries
Knowledge Sharing

November 2018



Agenda

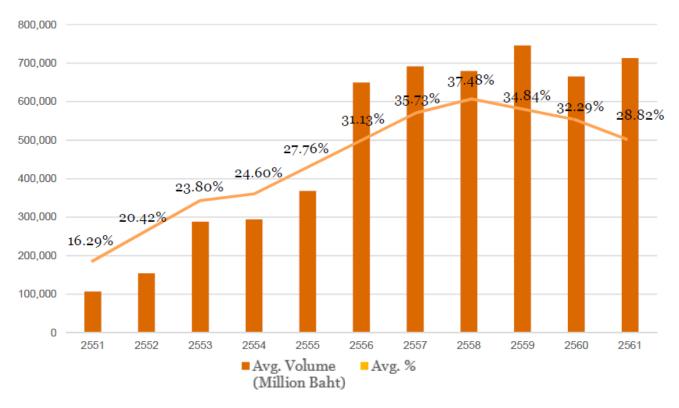
Why IT Security?

Cyber Resilience

Common Industry Observations

Why IT Security?

Contribution of Electronic Trading System



Why IT Security?

Penny Stock Pump-and-Dump Scheme

MARKETS | FINANCIAL REGULATION

Penny-Stock Promoter Pleads Guilty to Manipulating Companies

Gregg R. Mulholland could face up to 20 years in prison in 'pump and dump' scheme

By Christopher M. Matthews

May 9, 2016 4:05 p.m. ET

A penny-stock promoter pleaded guilty Monday to conspiring to manipulate stock: laundering more than \$250 million in profits, in what prosecutors have described at the largest-ever "pump and dump" schemes.

https://www.wsj.com/articles/penny-stock-promoter-pleads-guilty-to-manipulatingcompanies-1462824337



https://in.reuters.com/article/cyber-brokerages-hongkong-idINKBN15U0BA

Hired hackers key to JP Morgan, Fidelity breaches

By Reuters New York/San Francisco, 16 Nov 2015



hen US prosecutors this week charged two Israelis and an American fugitive with raking in hundreds of millions of dollars in one of the largest and most complex cases of cyber fraud ever exposed, they also provided an unusual look into the burgeoning industry of criminal hackers for hire.

The trio, who are accused of orchestrating massive computer breaches at JPMorgan Chase and other financial firms, as well as a series of other major offences, did little if any hacking themselves, indicate the federal indictments and a previous civil case.

brought by the US Securities and Exchange Commission.

https://www.itweb.co.za/content/nkLgB1Meg26v59N4

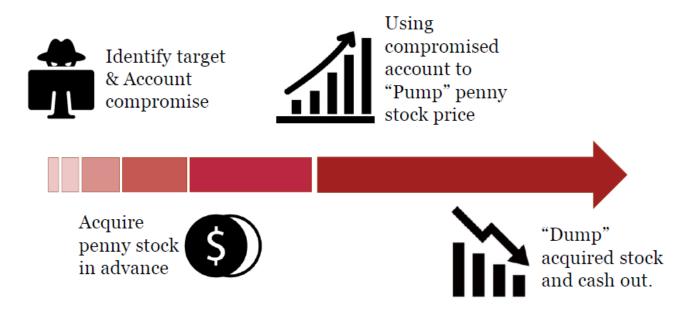
Crooked 'pump and dump' trades double to HK\$53m in Hong Kong

The discovery has prompted officials to warn the public to guard against hackers when using electronic devices.

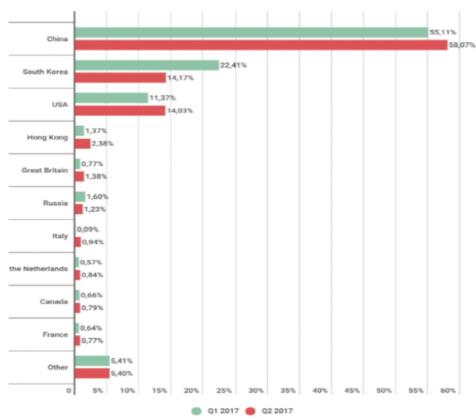
https://www.scmp.com/news/hong-kong/law-crime/article/1982323/crooked-pump-and-dump-trades-double-hk53m-hong-kong

Pump-and-Dump

How was money stolen from the account?



DDoS attacks



Hong Kong brokers are being repeatedly targeted by hackers

Five Taiwan brokerages report DDoS cyber attack threats, regulator says

Lloyds Banking Group Reportedly Hit by DDoS Attack

DDoS Attacks Slam Finnish Bank

Ukraine Blackout Redux: Hacking Confirmed

PYONGYANG LAUNCHES ATTACK AGAINST BITCOIN

DDoS attacks were registered in 86 countries in Q2, where the largest number of the attacks were aimed at China (58.07% of all of the attacks), which is 3 p.p. higher compared to the previous quarter. South Korea went down from 22.41% to 14.17% and retained second place nonetheless, while the USA rose from 11.37% up to 14.03%, almost catching up with South Korea.

Source: Kaspersky (https://securelist.com/ddos-attacks-in-q2-2017/79241/)

Cyber Resilience

It's all about risks

Control Maturity Inherent risk assessment Technologies Situation Awareness Delivery channels Identification Aspects Products and technology services to be assessed Organisational characteristics Governance Track records on cyber threats Inherent Risk Levels **Expected Maturity Levels** High Advanced Party Risk Managemen Medium Intermediate **Baseline**

Low

Cyber Resilience

The Cyber Resilience Framework

Internal Environment - Identification

- · IT asset identification
- Cyber risk identification and assessment

Governance

- Cyber resilience oversight
- Strategy and policies
- Cyber risk management
- Audit
- Staffing and training

Internal Environment – Response & Recovery

- · Response planning
- · Incident management
- Escalation and reporting

Situation Awarenego

Governance

Party Risk Mana

External Environment – Situation Awareness

Threat intelligence
 Threat intelligence sharing

Internal Environment - Protection

- · Infrastructure protection controls
- Access control
- · Data security
- Secure coding
- Patch management
- Remediation management

Internal Environment - Detection

- Vulnerability detection
- Anomalies activity detection
- Cyber incident detection
- Threat monitoring and analysis

External Environment – 3rd Party Risk Management

- · External connections
- Third party management
- Ongoing monitoring on third party risk

Cyber Resilience

Area of Focus

Cybersecurity management and supervision

Infrastructure security management

Protection of clients' internet trading accounts

- · Roles and responsibilities of cybersecurity management
- · Cybersecurity incident reporting
- Cybersecurity awareness training for internal system users
- · Cybersecurity alert and reminder to clients
 - Deploy a secure network infrastructure
 - User access management
 - Security controls over remote connection
 - Patch management
 - End-point protection
 - Unauthorized installation of hardware and software
 - Physical security
 - System and data backup
 - Contingency planning for cybersecurity scenarios
 - · Third-party service providers
 - Authentication
 - · Implement monitoring and surveillance mechanisms
 - · Prompt notification to clients
 - · Data encryption
 - Protection of client login passwords
 - Stringent password policies and session timeout controls

Common Industry Observations

IT Governance

3 line of Defences



Responsibilities

Responsible persons who govern and manage IT functions, also implement control monitor and report CEO CIO Business Executives Strategy Executives



Responsibilities

Ensure that compliance and controls requirements are met, also support implementation of IT policy and procedure, update and communicate IT risk and compliance issues. RM Committees Compliance



Responsibilities

Independent persons who evaluate and validate compliance and controls performance

Internal Audit

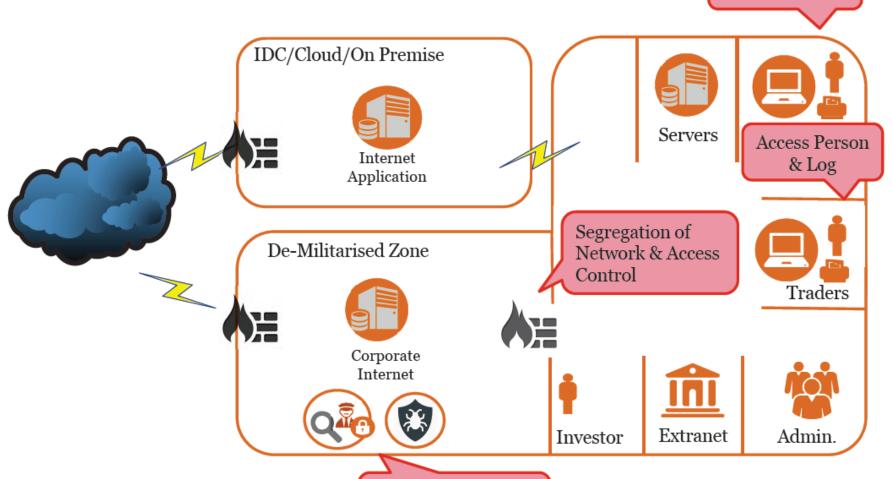
Board of director (Accountable)

Common Industry Observations Security Protect Cloud Security Management Use of network traffic Prove of security analysis tools IDC/Cloud/On Premise concept (IDS/IPS) (Penetration Test) Users Servers Internet Application Critical security patch De-Militarised Zone Traders Corporate Firewall Access Internet Rules Extranet Admin. Investor

Common Industry Observations

Security Protection

Social Media Control



ASCO - IT Security for Intermediaries

Data Classification & Data Handling

Q&A