Cyber Crime and Financial Crime

Different Sides Of The Same Coin

Tyson Macaulay
Chief Technology Officer - Cyber
BAE Systems Applied Intelligence

SecTor Conference - Nov 13 2017
The sides of the metaphorical coin

- Two solitudes: Cyber Risk Management and Financial Risk Management

Chief Info (Sec) Officer

Compliance
Privacy
Reporting (Sox)
Safety (NERC CIP)

Crime/Espionage/Sabotage
Threat Intelligence
Info Sharing
Active analytics
Automated Interventions
Manual Interventions & Response

Chief Risk Officer

Compliance
Anti-Money Laundering (AML)
Know Your Customer (KYC)
Suspicious Activity Reporting (SARS)
Basel III (Capital reserves)

Crime/Fraud Detection
Passive Analytics
Manual interventions
Examples

Nepal bank latest victim in heists targeting SWIFT system
The topic
> FinCrime meets Cyber

Financial Crime regulation
- 1970 Banking Secrecy Act
- 1986 Money Laundering Control Act
- 1990 FINCEN
- 2000 SARS
- 2018 - Intersection

Cyber Security regulation
- 1983 Privacy Act
- 1988 Morris Worm
- 2002 ILOVEYOU virus
- 1998 PDD- 63
- 2004 PCI
- 2009 NERC CIP
- 2009 PSD2
- GDPR / C-59
- FINCEN
Regulators say FinCrime and Cyber risks are merging

> Framing the risks of FinCrime-Cyber intersection

- **United States Treasury**
  Office and Intelligence and Analysis
- **United States Treasury**
  Financial Crime Enforcement Network (FINCEN)
- **Bank of Canada**
  June 2017, Financial System Review
- **Gartner**
  April 2017, Managing Financial Crime
“Cybercrime can exploit new payment technologies for money laundering, but may also rely on low technology options...

Market manipulation fraud via computer intrusion involves criminals hacking into victims’ personal online brokerage accounts and using them to purchase shares of a targeted stock to inflate its price...

Recent cases demonstrate cybercriminals can avoid using money mules by transferring funds from hacked accounts to prepaid debit cards, and cashing out at an ATM”
### Source and destination information
- IP address and port information with respective date timestamps in UTC
- Uniform Resource Locator (URL) addresses
- Known attack vectors
- Command and control nodes

### Email content
- Subject user names
- Email addresses related to suspicious activities
- Social media accounts/screen names related to suspicious activities

### File information
- Filenames of files suspected to be infected with malware
- MD5, SHA-1, or SHA-256 hash information

### System modifications:
- System registry modifications
- Indicators of system compromise
- Common vulnerabilities and exposures
“Complex, interconnected information technology platforms have allowed the financial sector to deliver services to clients more efficiently. However, they have also created increased opportunities for a successful cyber attack on a single institution to spread throughout the broader financial system.”
“Traditional fraud systems do not have the data to detect new fraud trends, nor the quick reaction time needed to detect and mitigate sophisticated omnichannel fraud.”

“Defenses for AML, fraud and cyberthreats have similar data requirements, prompting some organizations to share data sources; however, detection systems and data quality requirements are different for each group resulting in many siloed data environments.”
Cyber to FinCrime CONOPS

**Threat Intelligence**

**Meta Data**
- Source Reputation
  - Address
  - Network
  - Domain
  - Geolocation
  - Anonymizer

**Indicator Type**
- Device IOCs
- Network type (mobile vs fixedline)
- Gateway (VPN, TOR)
- Darknet intelligence (stolen IDs, CC#, accounts)
- Blockchain / DLT SNA

**Source**
- Closed Source: Curated Threat Intel
  - Open Source (OSINT): Darknet Exposure Reports
  - Bulk Subscription feeds: AV/URL/Spam/VPN/ToR
### Compliance and Reporting Use-cases

**NetReveal – Case Management Systems**

#### Compliance Use Cases

<table>
<thead>
<tr>
<th>Category</th>
<th>Use Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privacy and Access (GDPR + PSD2)</strong></td>
<td>- API security</td>
</tr>
<tr>
<td><strong>KYC</strong></td>
<td>- ID Theft / Account takeover</td>
</tr>
<tr>
<td></td>
<td>- Blockchain SNA</td>
</tr>
<tr>
<td><strong>Suspicious Activity Reports (SARs)</strong></td>
<td>- AML reporting / Sanctions busting</td>
</tr>
<tr>
<td></td>
<td>- Malware events*</td>
</tr>
<tr>
<td></td>
<td>- Diversion attacks*</td>
</tr>
</tbody>
</table>

*Per FinCEN Advisory FIN-2016-A005*
Fraud use-cases

NetReveal – Case Management Systems

Fraud Use Cases

- Policy and Account Fraud and Compromise
- Policy Breach
- API and TTP security
- IoT compromise

BlockChain

- Ownership tracking
- Warranty and support conditions / status
- SNA
- Smart Contracts

Threat Intel

Account ID: Meta Data
Lawful Access and CSR

NetReveal – Case Management Systems

Lawful Access Use Cases

PEP (Politically Exposed Persons) tracking

Human Trafficking

Child Exploitation

Threat Intel

Account ID: Meta Data
The Vision - Cyber to FinCrime

Transactions
- Mobile
- Branch
- Call Centre
- Online
- Corporate Branch

Payment AML/Fraud Solution
- Ingest
- Detection
- Investigation
- Reporting

Cyber Intelligence
- Internet Portal Logs

Payment hub/Payment engine/Payment channel
- Ingest
- Block/Allow
Feedback loop – Fincrime to Cyber

Transactions
- Mobile
- Branch
- Call Centre
- Online
- Corporate Branch

Payment AML/Fraud Solution
- Reporting
- Detection
- Investigation

Cyber Intelligence
- Internet Portal Logs

Ingest
Thank You

Tyson Macaulay, CISSP, CISA
Chief Technology Officer – Cyber
BAE System

tyson.macaulay@baesystems.com
+1 (613) 292-9132
linkedin.com/in/tysonmacaulay
Future Capabilities


**Source and Destination Information:**
- IP address and port information with respective date timestamps in UTC
- Uniform Resource Locator (URL) addresses
- Attack vectors
- Command-and-control nodes

**System Modifications:**
- Registry Modification
- Indicators of Compromise (IOCs)
- Common vulnerabilities and exposures (CVEs)

**File Information:**
- Suspected malware filenames
  - MD5, SHA-1, or SHA-256 hash information
  - E-mail content

**Involved Account Information:**
- Affected account information
- Involved virtual currency accounts (case sensitive)

**Subject User Names:**
- E-mail addresses
- Social media account/screen names
**NetReveal + Threat Intelligence - Concept of Operations**

**Defined data specification:**
Standard format for all payment types to assure ease of deployment.

**Real-time feeds**
- Payments from all channels

**Batch data feeds (XML)**
- Customer referential data
- Account referential data
- PEP watchlists
  - Threat Intelligence Meta Data
    - Address / Network reputation and geolocation
    - Network / Device IOCs
    - Network type (mobile vs fixedline)
    - Anonymizer gateway (VPN, TOR)
    - Darknet intelligence

**Detect and respond:**
Profile customer data to risk rate payments, detect fraud, block payments and generate alerts.

**Automatic processes**
- Acquire
- Profile
- Scores
- Screen
- Interdict
- Alert

**Investigate and act:**
Investigate alerted payments, activity history and referential data, and make final decision on blocking or allowing the payment.

**Manual processes**
- Investigate
- Adjudicate
Threat Inputs to service

Inputs - BAE Systems Global SOC (GSOC)

- Highest pedigree sourcing
- Professionally engineered
- Targeted and Actionable
- Used internally by BAE
My Background

Professional

1993 – 2004
2 x start-up co.
1 x US Defence

Security Liaison Officer

Bell

CTO - Telecom Security

intel

CSO

Fortinet

BAE SYSTEMS

CTO Applied Intelligence

Thought

2006
Securing Converged IP Networks
Tyson Macaulay

2008
CRITICAL INFRASTRUCTURE津贴
Tyson Macaulay

2012
Cybersecurity for Industrial Control Systems

Tyson Macaulay and Bryan Singer

2016
RiIoT CONTROL

Volunteering

ISO

International Organization for Standardization

Security / IoT / Blockchain

Cira

BoD

Advisory

ISO

Professional

1993 – 2004
2 x start-up co.
1 x US Defence

Security Liaison Officer

Bell

CTO - Telecom Security

intel

CSO

Fortinet

BAE SYSTEMS

CTO Applied Intelligence

Thought

2006
Securing Converged IP Networks
Tyson Macaulay

2008
CRITICAL INFRASTRUCTURE津贴
Tyson Macaulay

2012
Cybersecurity for Industrial Control Systems

Tyson Macaulay and Bryan Singer

2016
RiIoT CONTROL

Volunteering

ISO

International Organization for Standardization

Security / IoT / Blockchain

Cira

BoD

Advisory

ISO