RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: AIR-F03

Law Enforcement, The Secret Weapon in the CISO's Toolkit

John Fokker

Head of Cyber Investigations
McAfee - Advanced Threat Research (ATR)
@John_Fokker

Speaker

John Fokker

Head of Cyber Investigations ATR
McAfee

Previous roles:

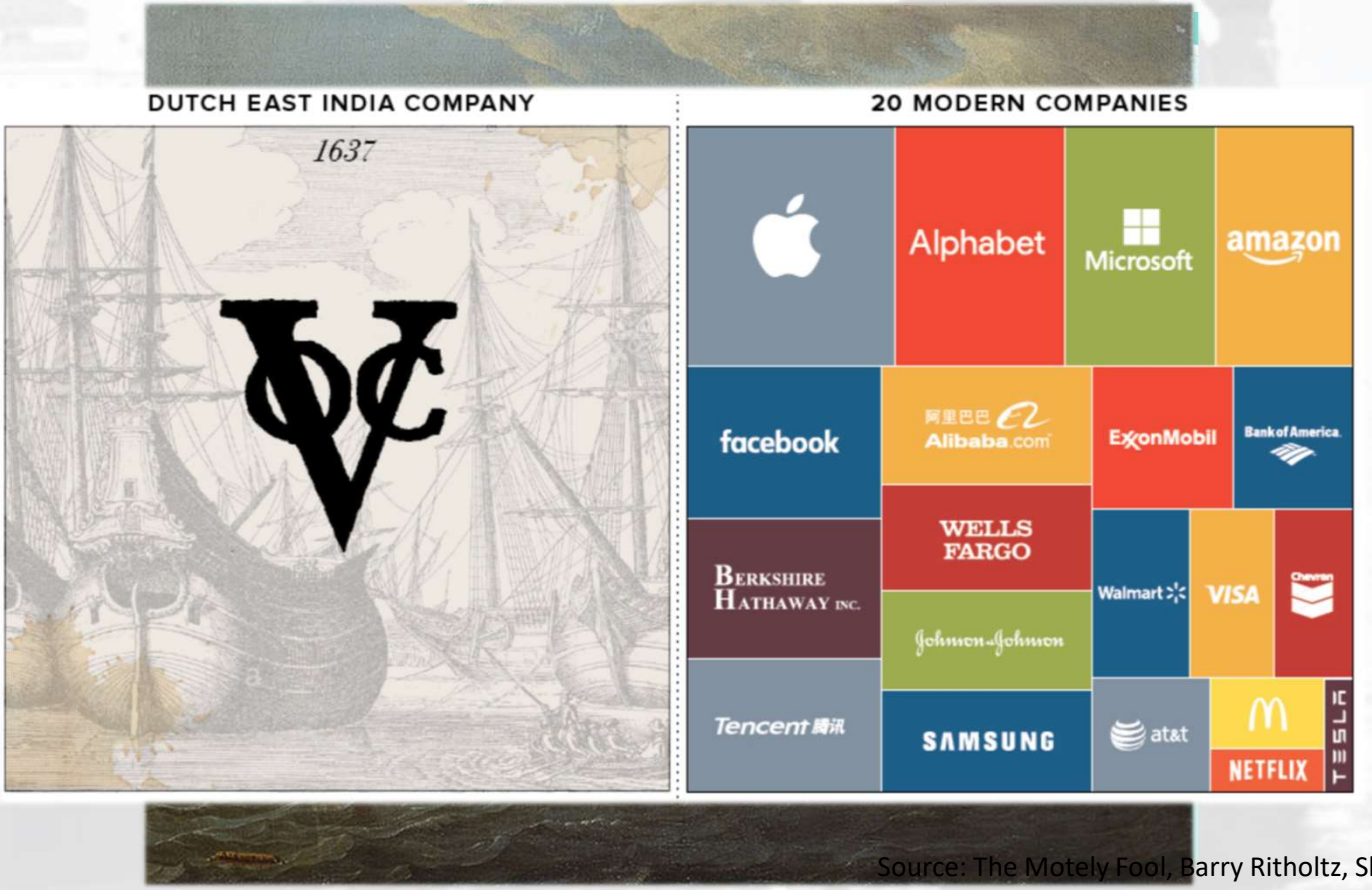
Technical supervisor -	Dutch High Tech Crime Unit
Digital Forensic specialist –	Dutch National Police
Special Forces Operator –	Dutch Marine Corps

Security at sea

How do military interventions at sea compare to Law Enforcement cybercrime interventions

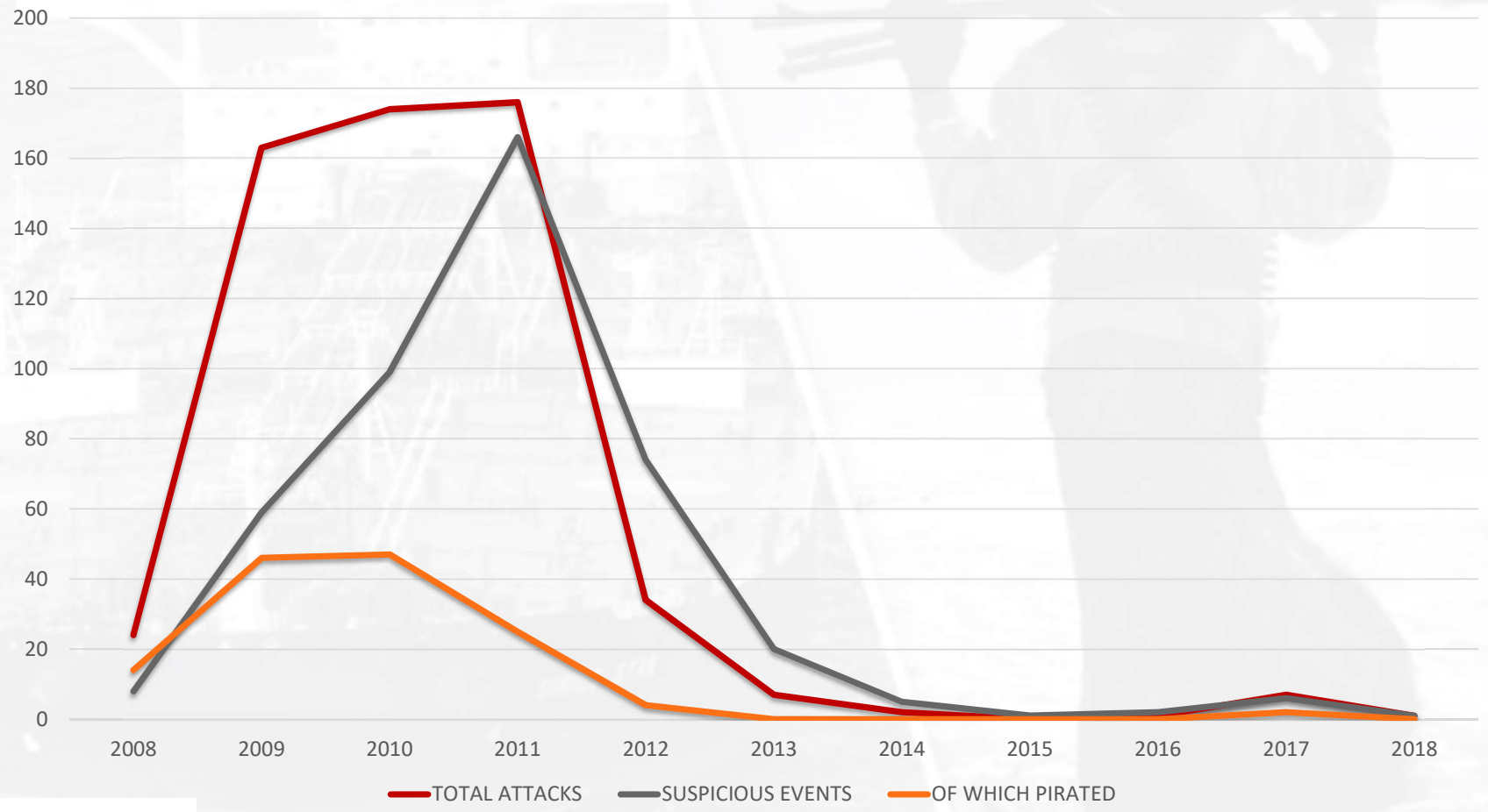
McAfee™
Together is power.

Security at Sea



Source: The Motely Fool, Barry Ritholtz, Sheridan Titman

Somali Piracy statistics

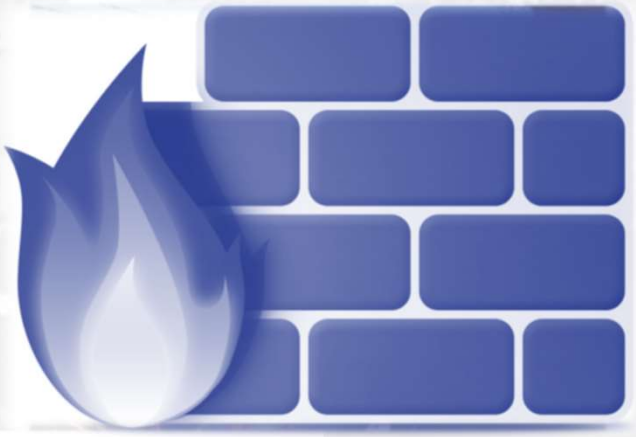


Source: EU Naval Force -Somalia

McAfee™
Together is power.

Safety Measures

FJJ4

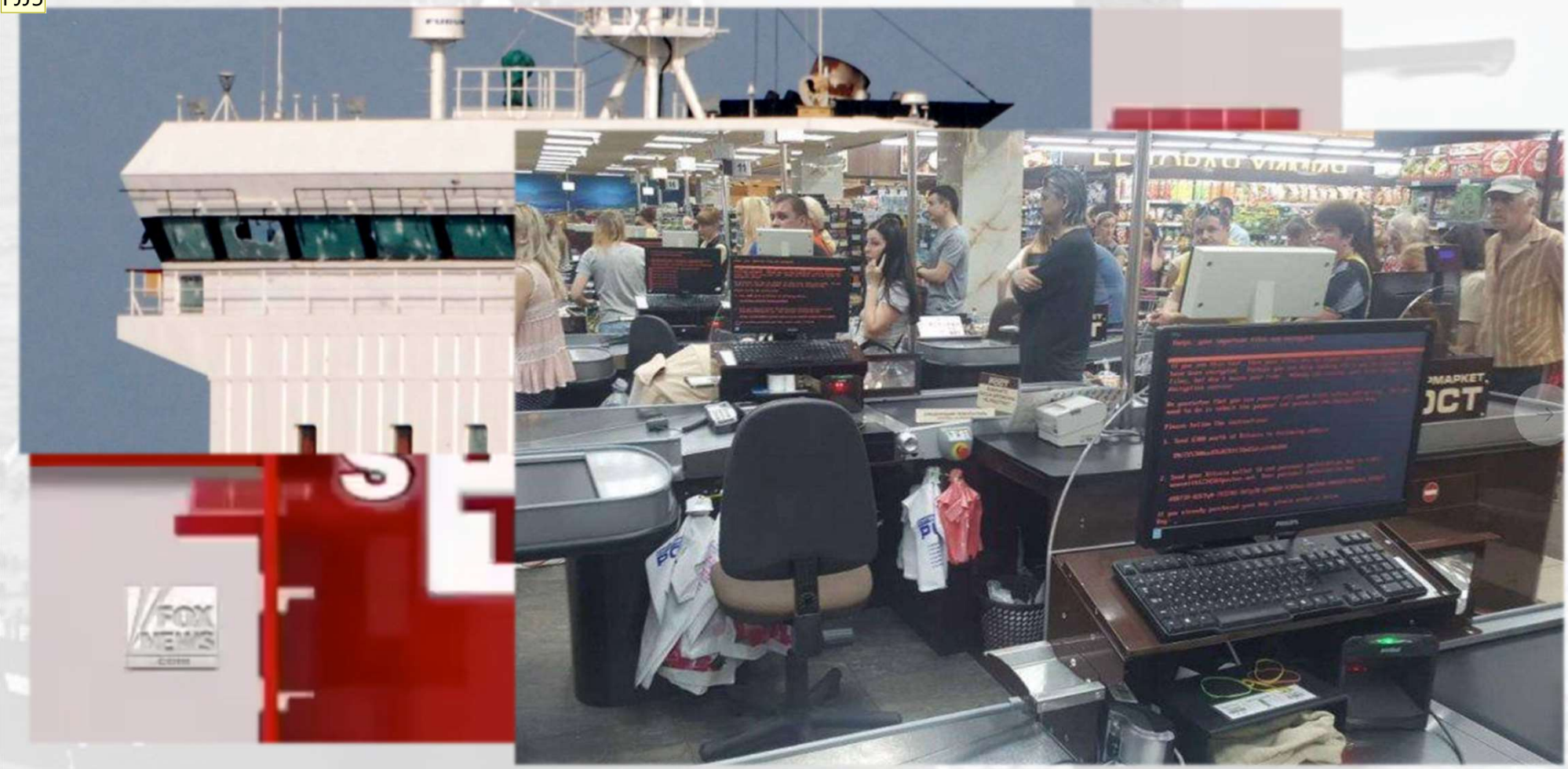


McAfee
Together is power.

Slide 7

FJJ4 Do you have a better picture for a Firewall?

Fokker J.E., John, 10/1/2018



McAfee™
Together is power.

Slide 8

FJJ5 Can some one make sure the sequence is running in order. So on click the video, then when finished disappear, on click the damaged bridge, on click disappear and then the ransomware in the store. On click disappear.
Fokker J.E., John, 10/5/2018

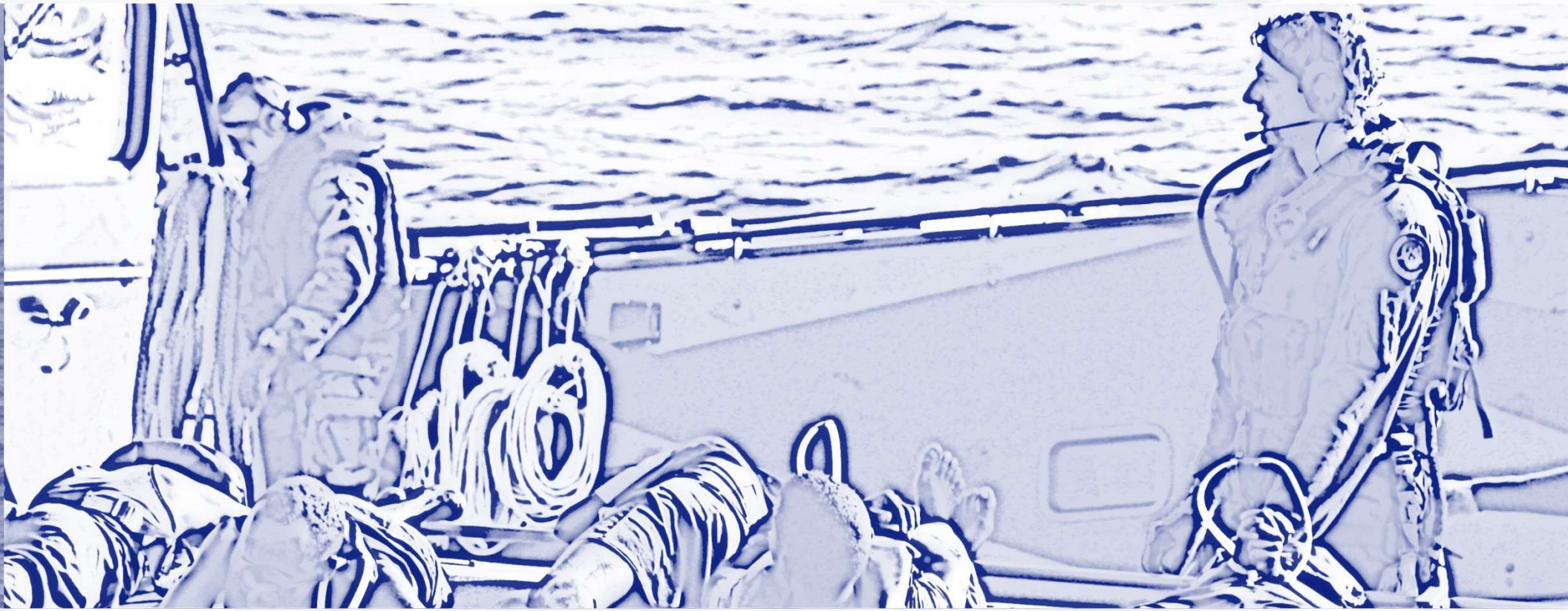
Pirate Threat Intelligence

Zooming in…

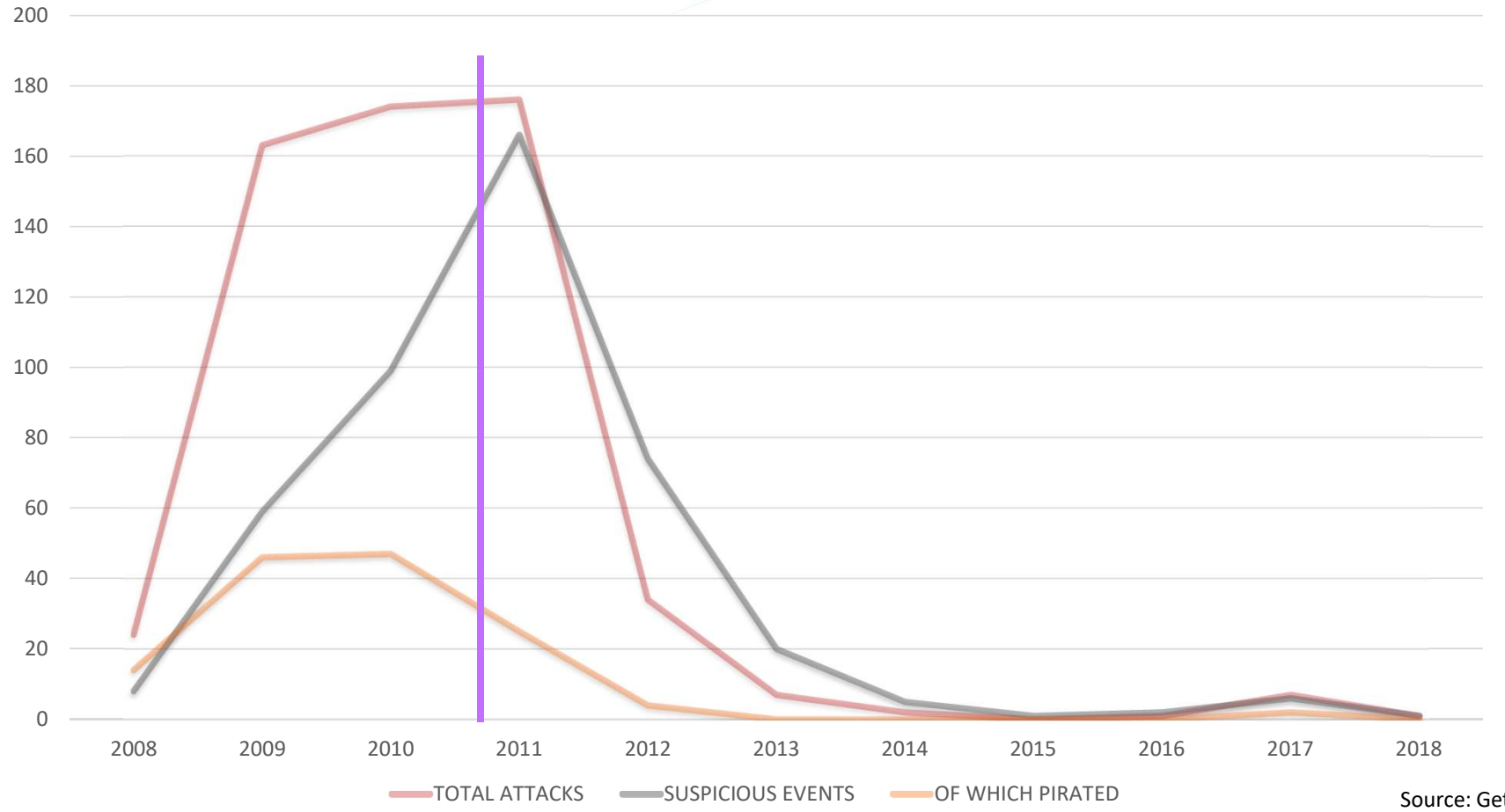

Pirate Camp Hobyo
US Dept of State Geographer
© 2018 Google
Image Landsat / Copernicus
© 2018 Basarsoft
Google Earth

Pirate Camp Hobyo

Change of Tactics: Disruption



Somali Piracy statistics



Source: EU Naval Force -Somalia

Source: Getty File Image

FJJ3

Un

React
Investig

Pro-a
Investig

38.96.*.*	US	California	San Diego	92101	Windows Server 2012 R2 Standard	16 GB	8.56 Mbit/s	5.99 Mbit/s			1.10.2018	11.00
					Avast 5		Win32:Malware-gen					

Slide 14

FJJ1 Please alter Icons to fit the McAfee approved icons. Unfortunately there are not enough Cybercrime related icons available:this is what the icons represent top left to right:1. Malware outbreak 2. Databreach. 3 Creditcard theft. 4 DDoS attack 5. Ransomware. 6. Spam BOTTOM left to right: 1. VPN service 2. Malware coding. 3. Data obfuscation . 4. Counter antivirus service. 5 Fake-ID 6 Domainregistration. 7. Bulletproof hosting. 8. Botnet traffic. 9. RDP market places. 9. Making fake credit cards. 10 Bitcoin tumbling 11. Money mules

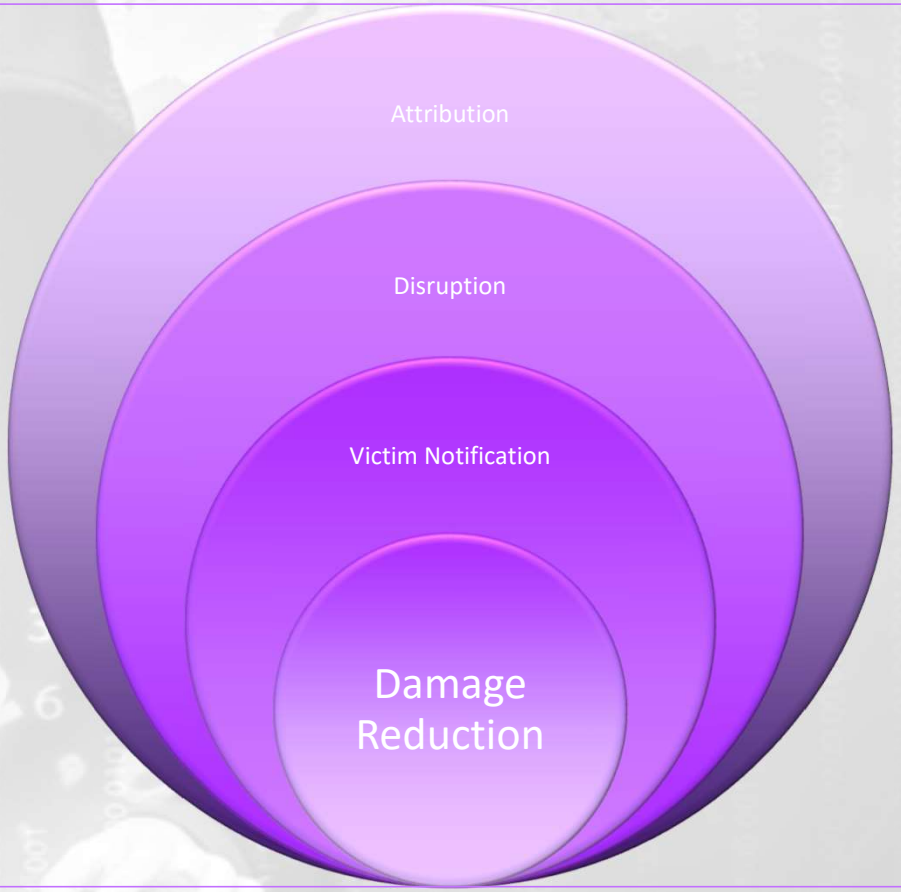
Fokker J.E., John, 10/1/2018

FJJ3 I would like an animation where the first screen shot of scan4you appears to come from the Counter antivirus Icon. The 2nd screen of UAS shop from the RDP log and the 3rd screen best mixer.io to come from the bitcoin logo

Fokker J.E., John, 10/1/2018

Investigation-as-a-Service,

Attribution is only one of the possible outcomes



Law enforcement engagement can help reduce incident response times

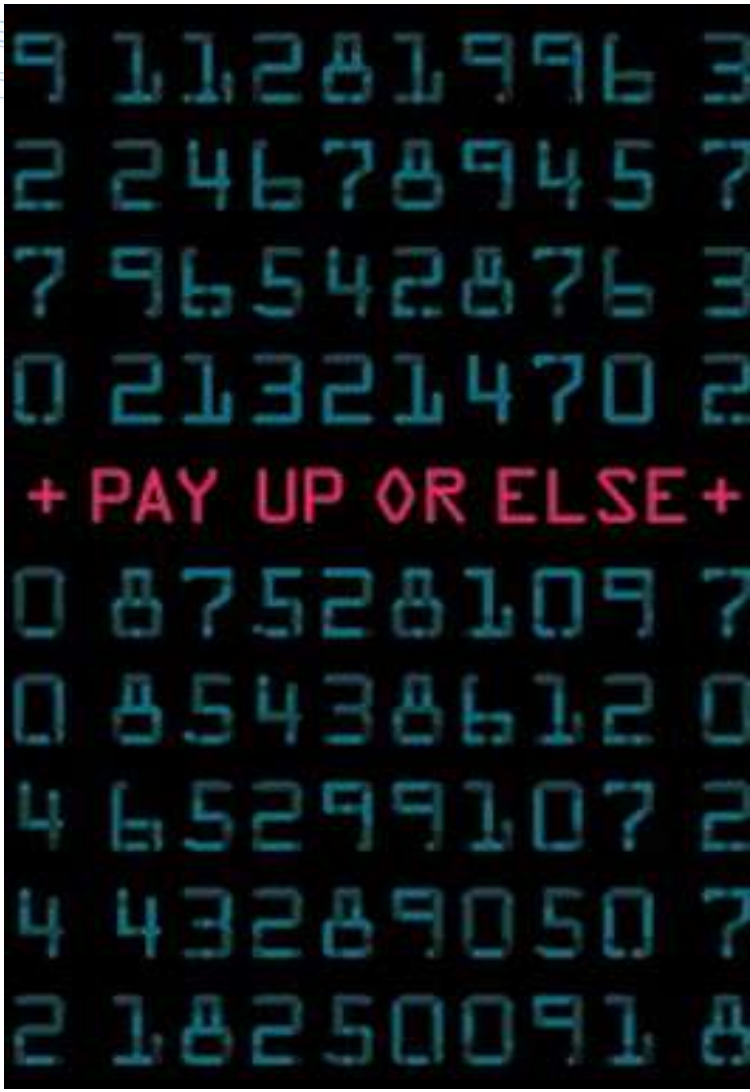
Case study: Data theft from a Billion dollar International company. The company is being extorted with the disclosure of sensitive data.

CISO'S QUESTIONS

- How did they get in?
- What data is gone? Were did it go?
- If we pay, will it stop?

Actions by Law Enforcement

- Seizing infrastructure involved
- Preserving valuable data
- **Established what was stolen and provided Strategic Intel.**



McAfee™
Together is power.

RSAConference2019

Law Enforcement as an offensive counter measure

Internet service provider under DDoS Attack

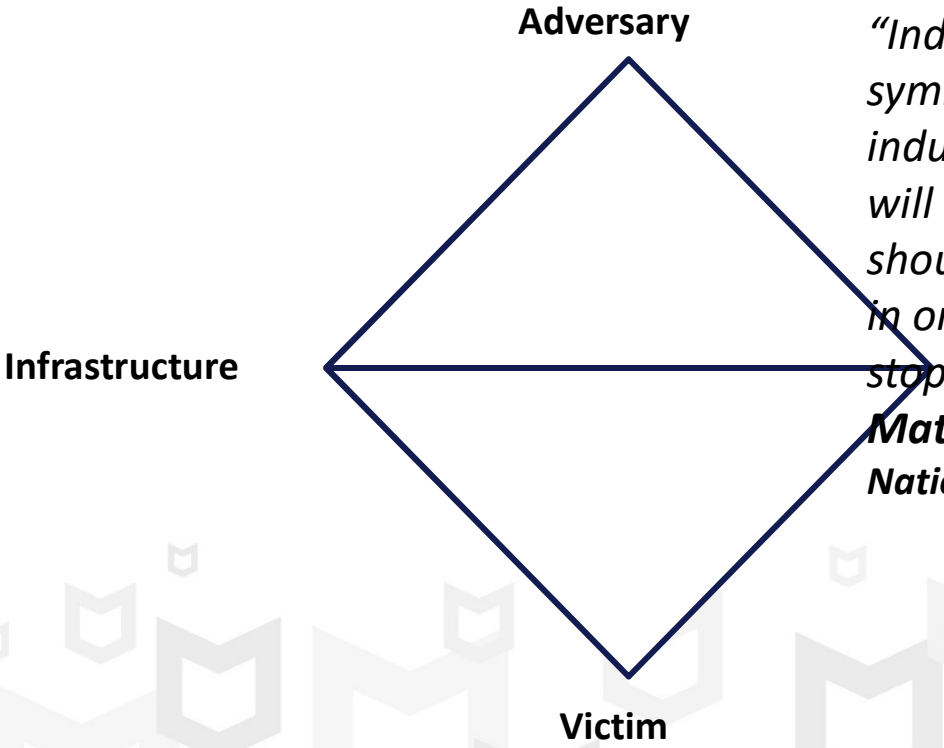
Aug 2015 the biggest cable company in the Netherlands was attacked, resulting in an internet outage for 2,5 million customers.

- Actors claiming to be Anonymous extorted the company
- Security team of Liberty Global did a emergency migration of infrastructure and system hardening
- International media attention
- Law enforcement served an deterrence and public reassurance.
- First arrests with in a week, in 1 month time the rest of the group.

LIBERTY GLOBAL

Ziggo

Intelligence sharing



"Industry and law enforcement working together should be a symbiotic exercise. Law enforcement should learn from industry where to focus limited government resources that will have the most impact on key threats, while industry should include government resources in their conversations in order to disrupt those conducting the threats, make them stop, and hold them accountable."

Matt LaVigna, President CEO,
National Cyber-Forensics and Training Alliance (NCFTA)

How do you get in contact ?

Infragard.org

"As a CISO you are going to meet with Law Enforcement sooner or later. That is why it's crucial to have a good relationship ahead of time, because when (not if) the bad stuff happens you won't have the time to choose who to talk to".

Darren Bennet, CISO, City of San Diego

NCFTA

NCFTA.net

McAfee
Together is power.

What if it's too late…

Local FBI field office

Local United States Secret Service (USSS) Field office

Internet Crime Complaint Center (IC3)

McAfee Advanced Threat Research

McAfee
Together is power.

Looking back

Takeaways
1. Reduce Incident response times through LEA partnership
2. Investigation-as-a-service, Attribution is just one of the many outcomes
3. LEA can act as an offensive countermeasure against Cyber threats

“Security is more powerful when Private sector and Law Enforcement are working together”

Might even apply to hunting pirates ;-)

“Apply” Slide

- Bullet point here (see slides 5 – 8 for instructions)
- Bullet point here
- Bullet point here

Presenter’s Company Logo – replace or delete on master slide

RSA Conference 2019


RSAConference2019