

CSM-ACE 2014

Cyber Threat Intelligence Driven Environments

Presented by James Calder

Client Services Manager, Singapore

CONTENTS

Digital criminality

Intelligence-led security

Shylock case study

Making threat intelligence work

Countering digital criminality

DIGITAL CRIMINALITY

Convergent trends in cyber and financial crime

RISKS IN CYBER SPACE



Dec 2013
Initial disclosure



Jan 2014
Full extent revealed



Feb 2014
Supply chain link



May 2014
Target CEO resigns

EVOLUTION OF FRAUD ATTACK METHODOLOGIES

"I've poured a glass of water down the back of the TV... but, I was told to do it by the man from the TV repair shop." - Woman from Europe

Insurance Claims
Benefit Fraud
Tax Evasion
Internal Fraud

Opportunistic

Individuals

First Party Fraud
Application Fraud
Tax Evasion
Benefit Fraud
Insurance Fraud

Planned

**Individuals
and Small Groups**

Staged / Induced Accidents
Tax Refund Fraud
Identify Theft
Insider Fraud
Social Engineering
First Party Fraud

Organised

**Teams
Skills for hire
Hierarchy**

Cyber Attack + Fraud
Phishing
Account Takeover

Automated

**Technology enabled
Highly scalable
International**

"After penetrating the computer network, the crime ring allegedly made more than 4,500 ATM transactions in about 20 countries around the world" - Fox news

Criminal Gains

Time / Confidence / Sophistication

THE ROLE OF CYBER IN ENABLING FRAUD

Definitions

Cyber-crime: Illegal or damaging acts in cyber-space (eg “hacking”, DDoS, information theft)

Cyber-enabled crime: Crimes facilitated or enhanced through use of cyber-space

Digital criminal: Organised criminals who specialise in stealing money using cyber techniques

	Fraud Challenge	Cyber Challenge
Definition	Fraud attacks are attacks against a business process	Cyber attacks are against information technology infrastructure
Method	Criminals seek to create or manipulate transactions.	Criminals seek to steal data or control/disrupt systems.
Threat Actor Goal	Financial Gain	Information Theft System Manipulation Economic Espionage Denial of Service



Intelligence-led security

Understanding threat intelligence

UNDERSTANDING THREAT INTELLIGENCE

THREAT DATA

- Malware signatures
- IOCs / IOAs
- Domain blacklists
- IP reputation lists
- Security mailing lists
- RSS feeds
- Open-source reports

THREAT CONTEXT

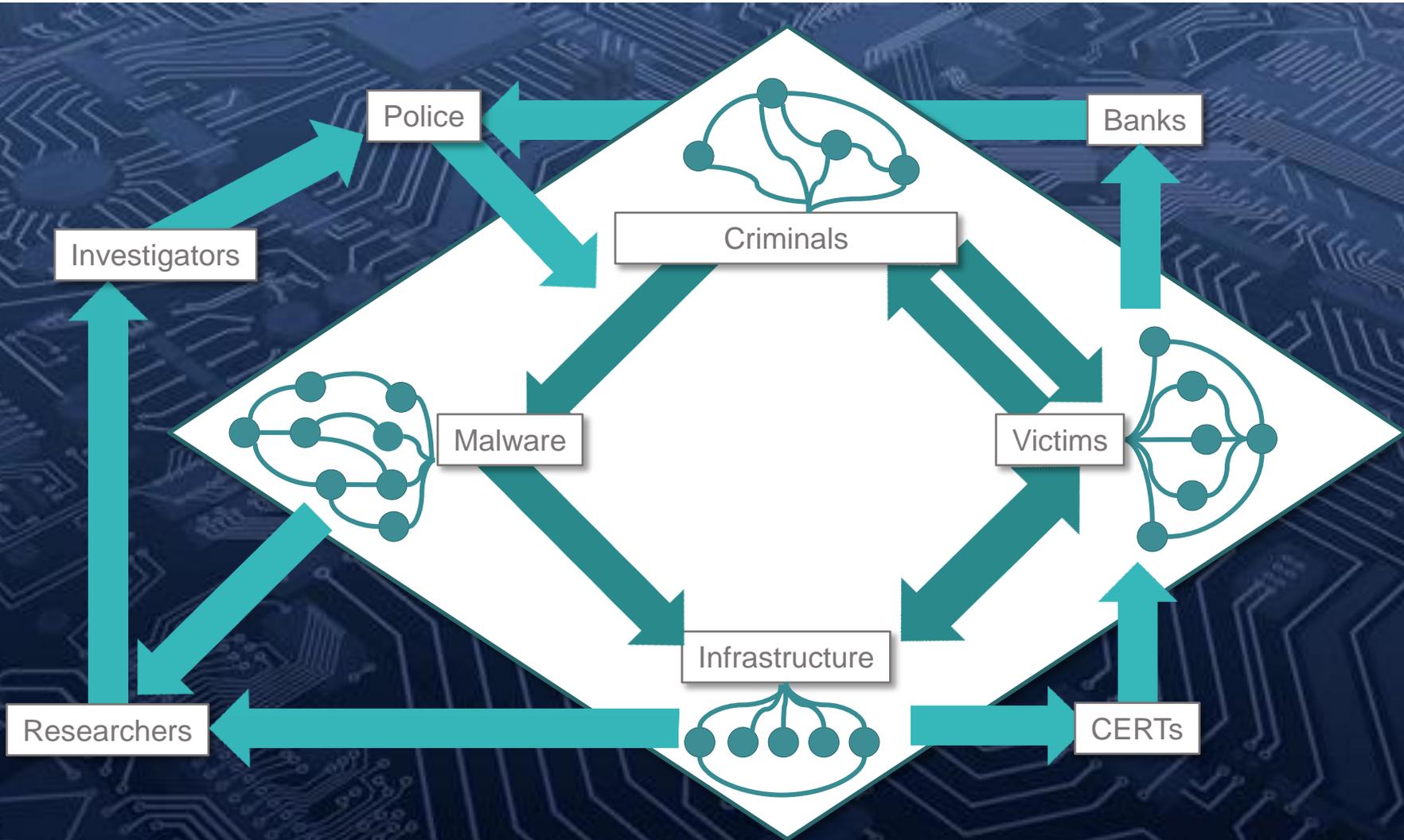
- Targets (sector / region)
- Motivation / Persistence
- Tools / Tactics / Procedures
- Attribution / Affiliation
- Socio-political context
- Business impacts
- Suggested mitigations

THREAT INTELLIGENCE

TECHNOLOGY FOCUSED RISK LANGUAGE

BUSINESS FOCUSED RISK LANGUAGE

DRIVES THE BUILDING OF INTELLIGENCE MODELS



SIX STEPS TO INTELLIGENCE-LED SECURITY

PERFORM THREAT ASSESSMENT

DETERMINE INTELLIGENCE REQUIREMENTS

BUILD COLLECTION SOURCES

OPERATIONALIZE THREAT INTELLIGENCE

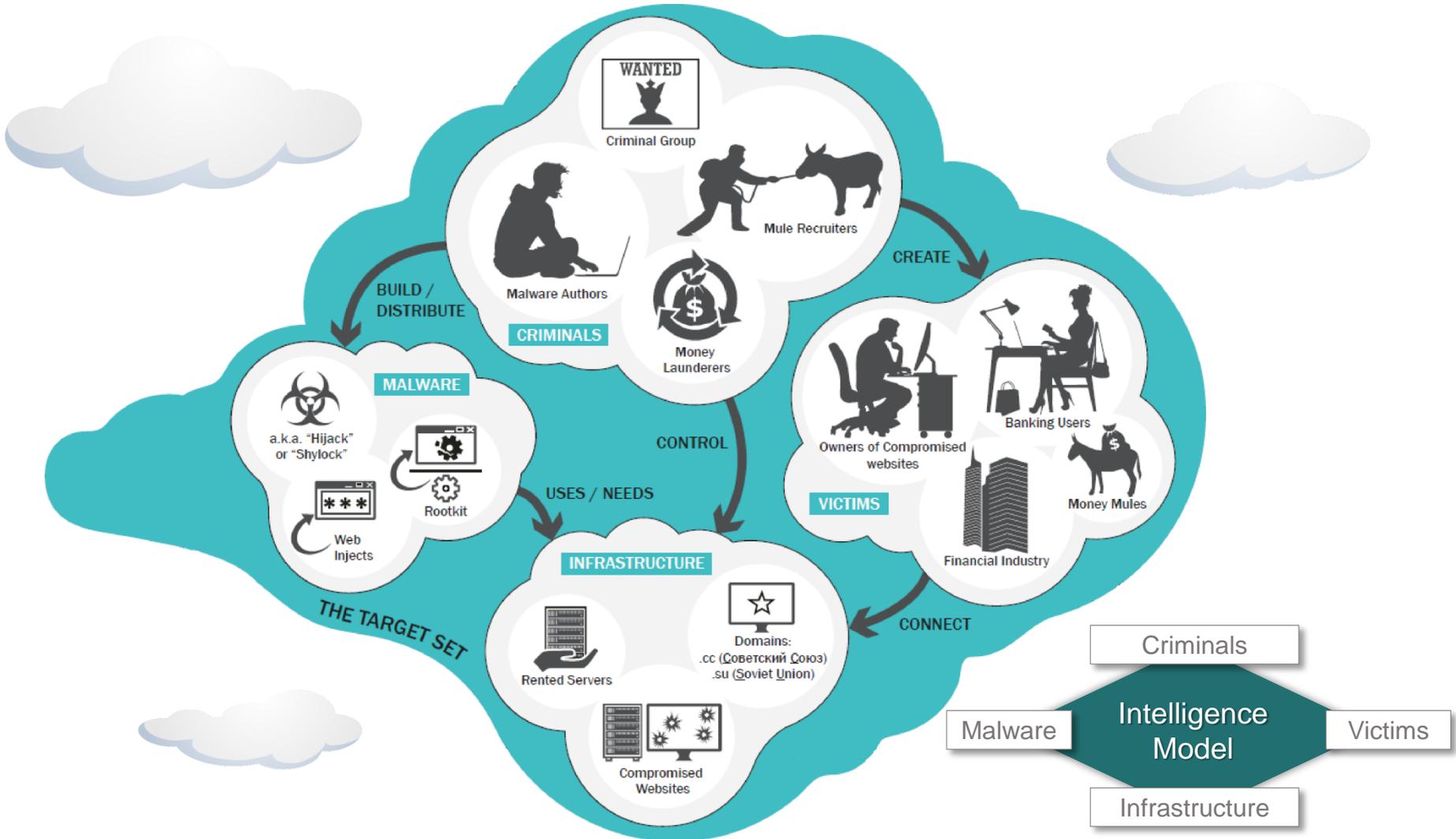
INTRODUCE SECURITY ANALYTICS

GAIN SITUATIONAL AWARENESS

Shylock Case Study

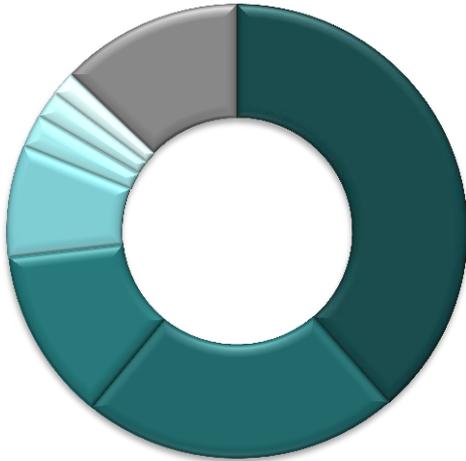
Use of threat intelligence to counter digital crime

SHYLOCK – A CYBER CRIMINAL INTELLIGENCE PROBLEM

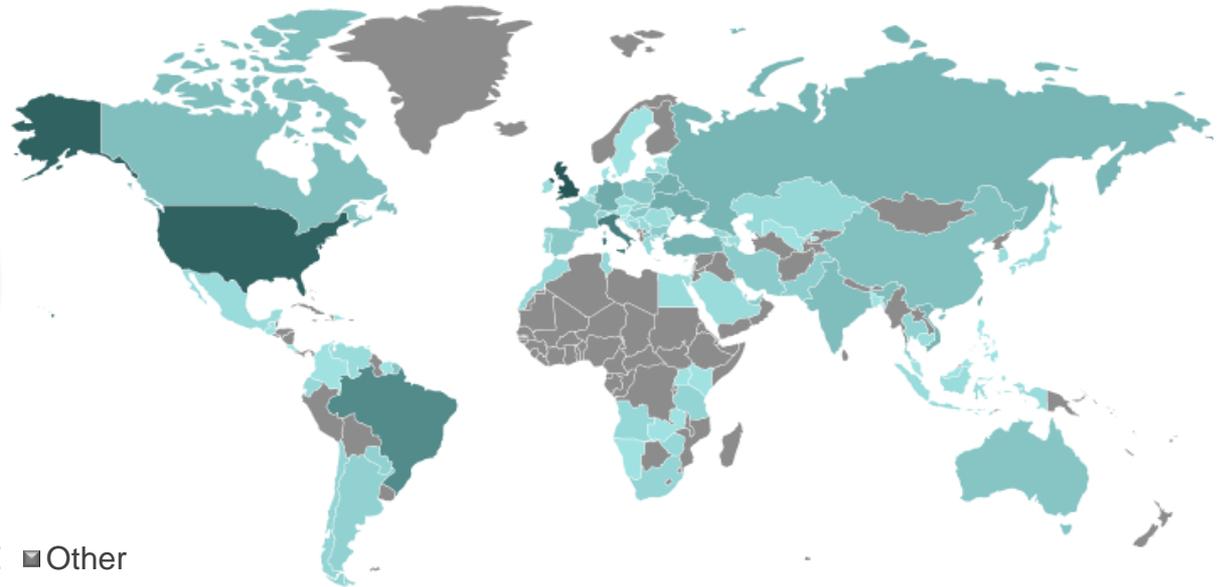


SHYLOCK FINANCIAL CRIME OPERATION

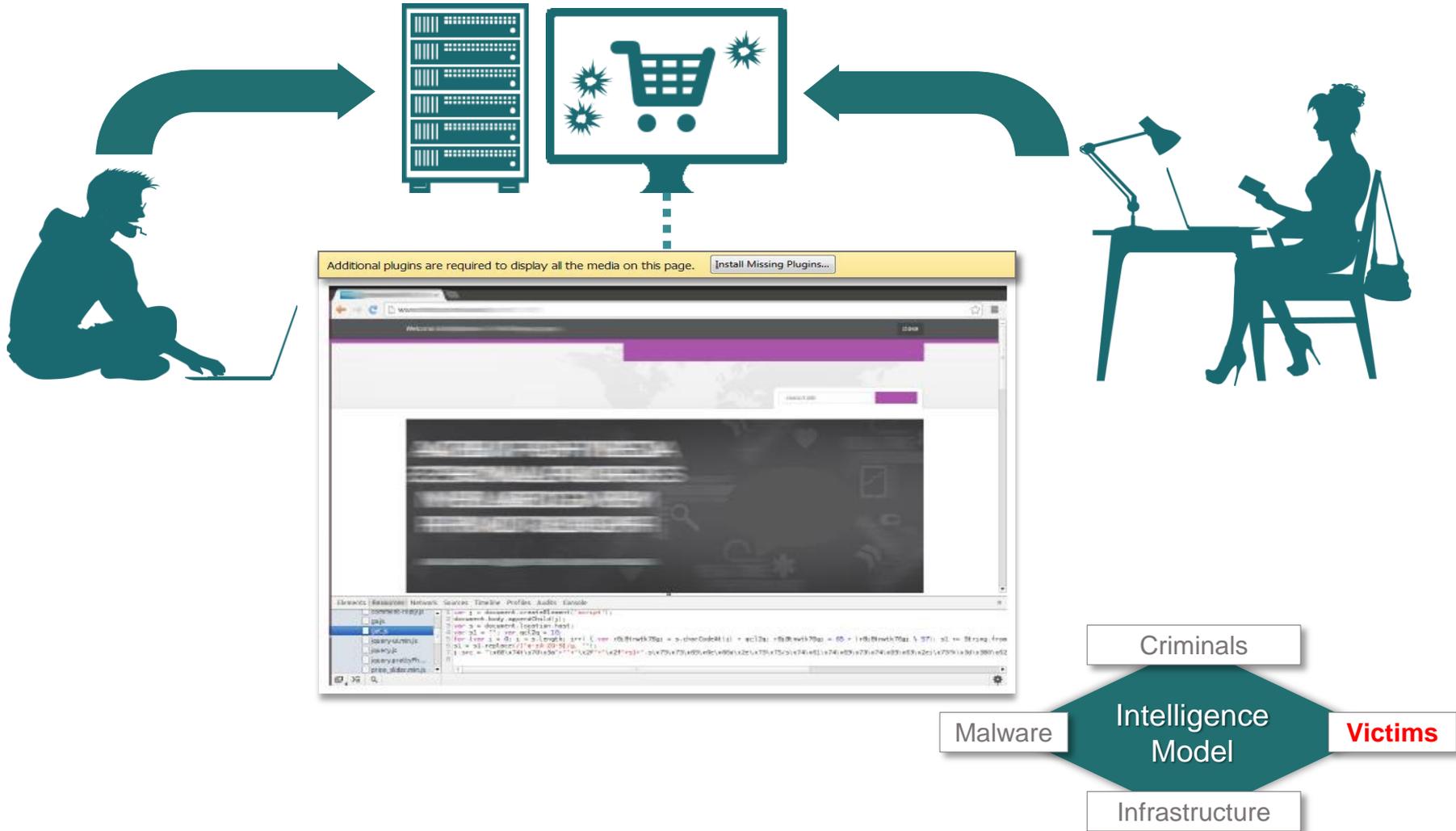
- **Estimated** at over 50K machines compromised
- **Global** victimisation, but with a **preference** for UK, US, and Italy



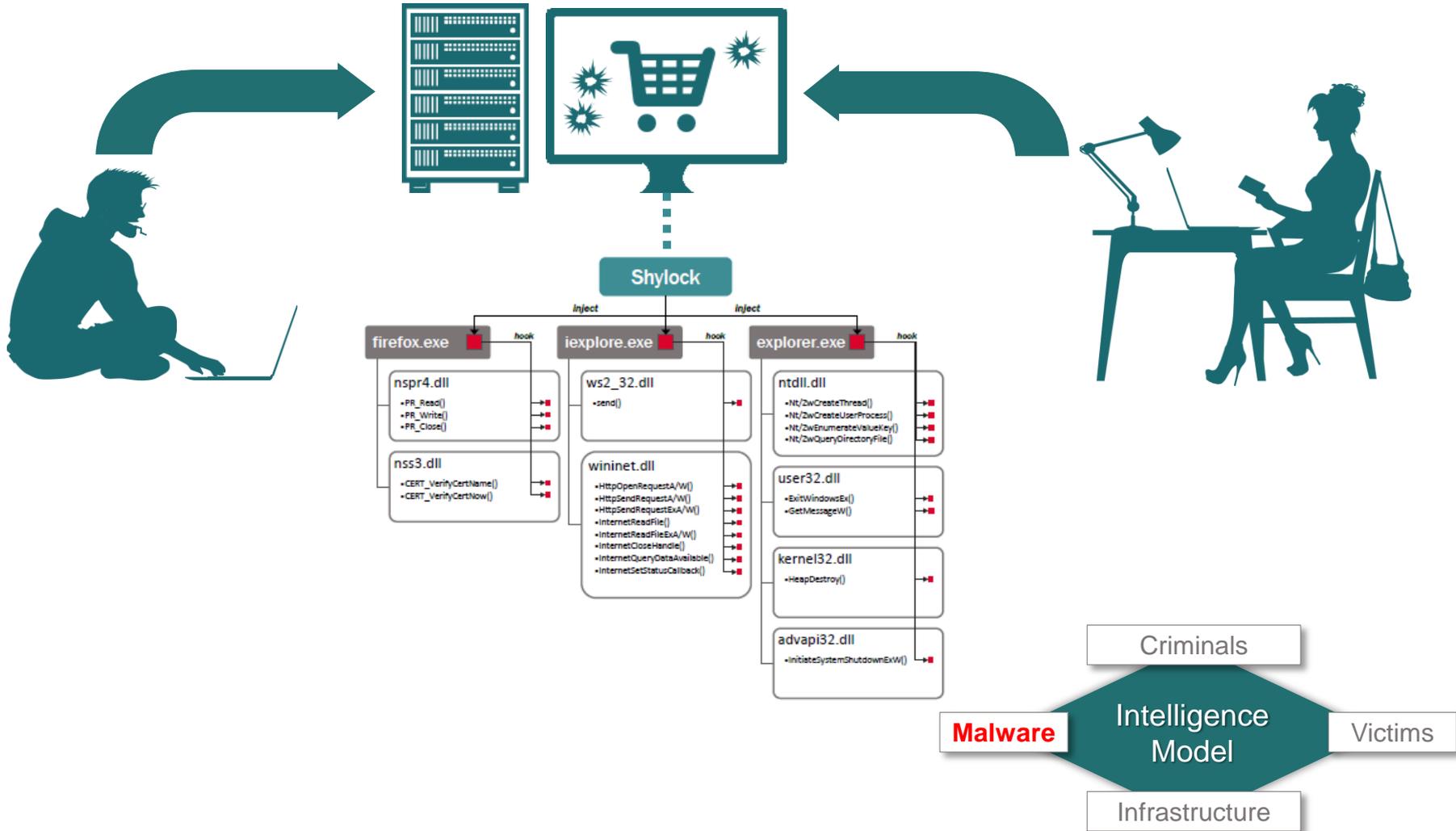
■ UK ■ US ■ IT ■ BR ■ TW ■ UA ■ DE ■ Other



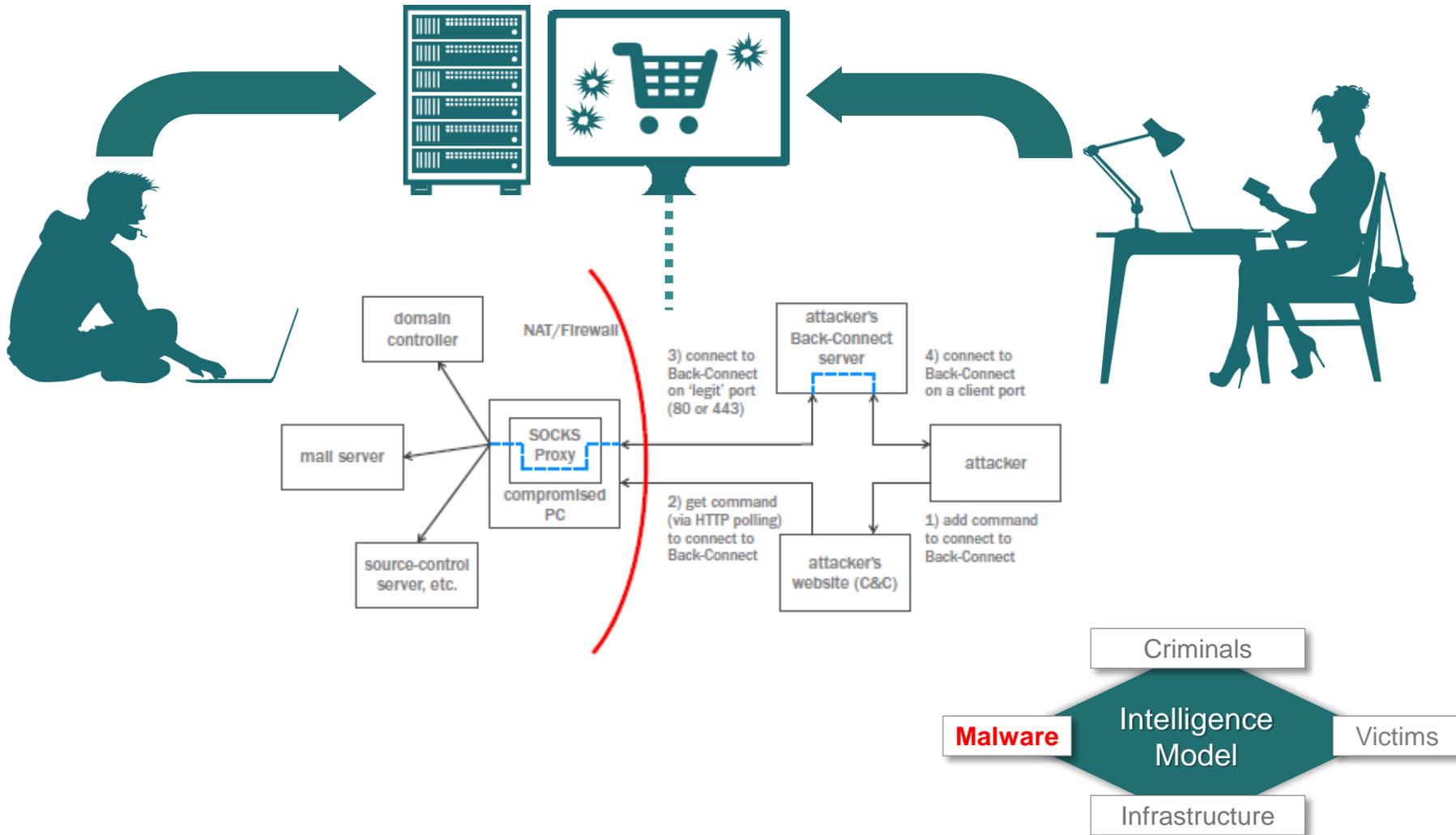
HOW IT WORKS – COMPROMISING THE VICTIM



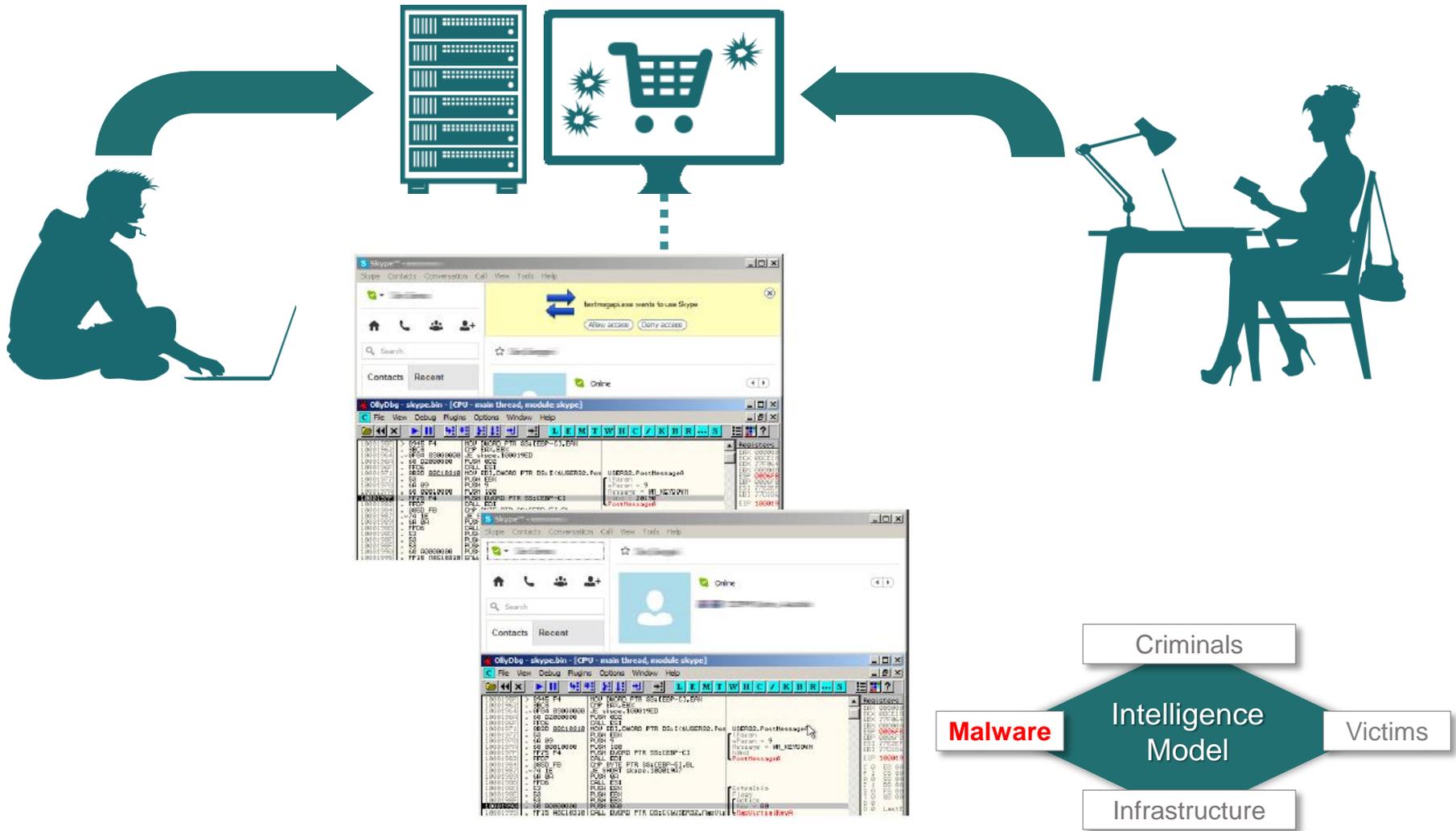
HOW IT WORKS – MALWARE AUTOMATION



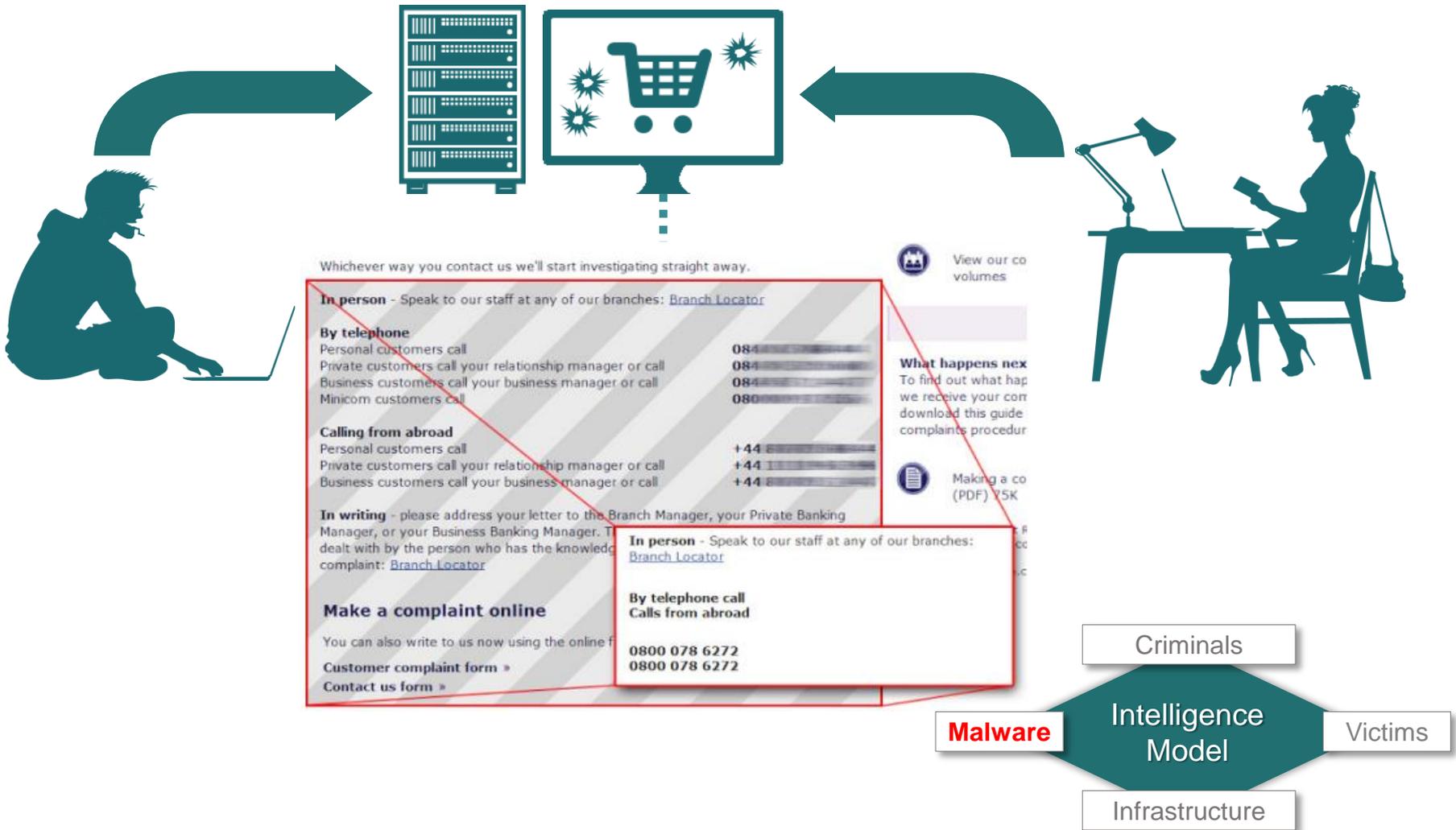
HOW IT WORKS – MALWARE AUTOMATION



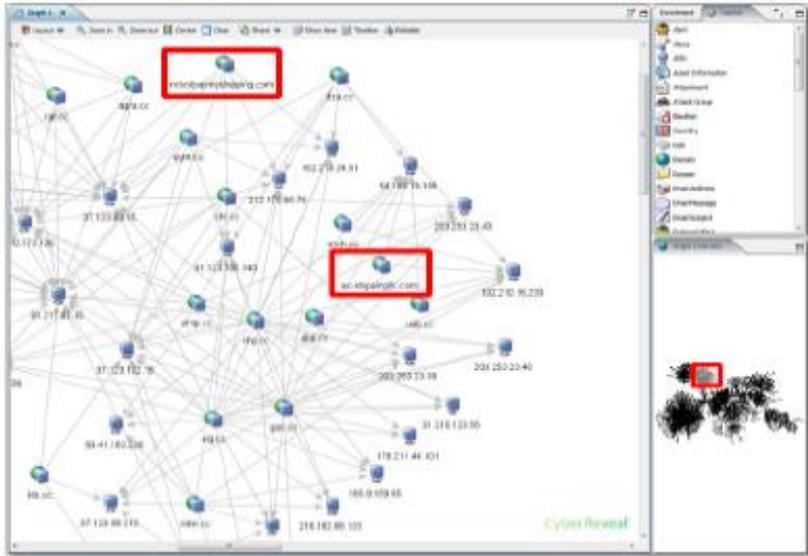
HOW IT WORKS – MALWARE AUTOMATION



HOW IT WORKS – BANKING WEBSITE MODIFICATION



LINKS TO MULE RECRUITMENT



AC Shipping LLC

Need something shipped from United States? We deliver to more than 220 Countries and territories worldwide.

Package Forwarding Worldwide - Review, choose, consolidate, repack and ship your packages in minutes. No hidden charges, easy to understand plans.

Main features ...

Main Features
Order your item from any U.S. based online store and have it delivered to your international address within 15 days!

3 Easy steps
1. Register with our service.
2. Choose your desired product.
3. Complete your payment.

Satisfaction Guaranteed
Over 100,000+ satisfied customers and over 50% repeat customers that prefer and trust our services over others.

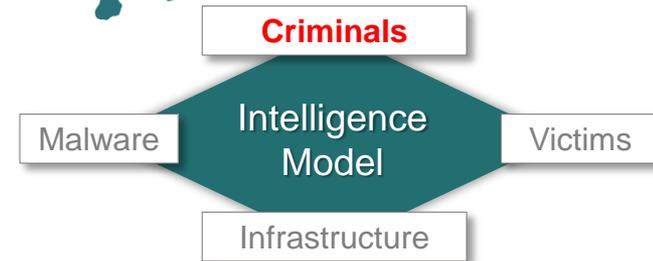
RICKOL EXPRESS SHIPPING

NEED SOMETHING SHIPPED FROM UNITED STATES? WE DELIVER TO MORE THAN 220 COUNTRIES AND TERRITORIES WORLDWIDE.

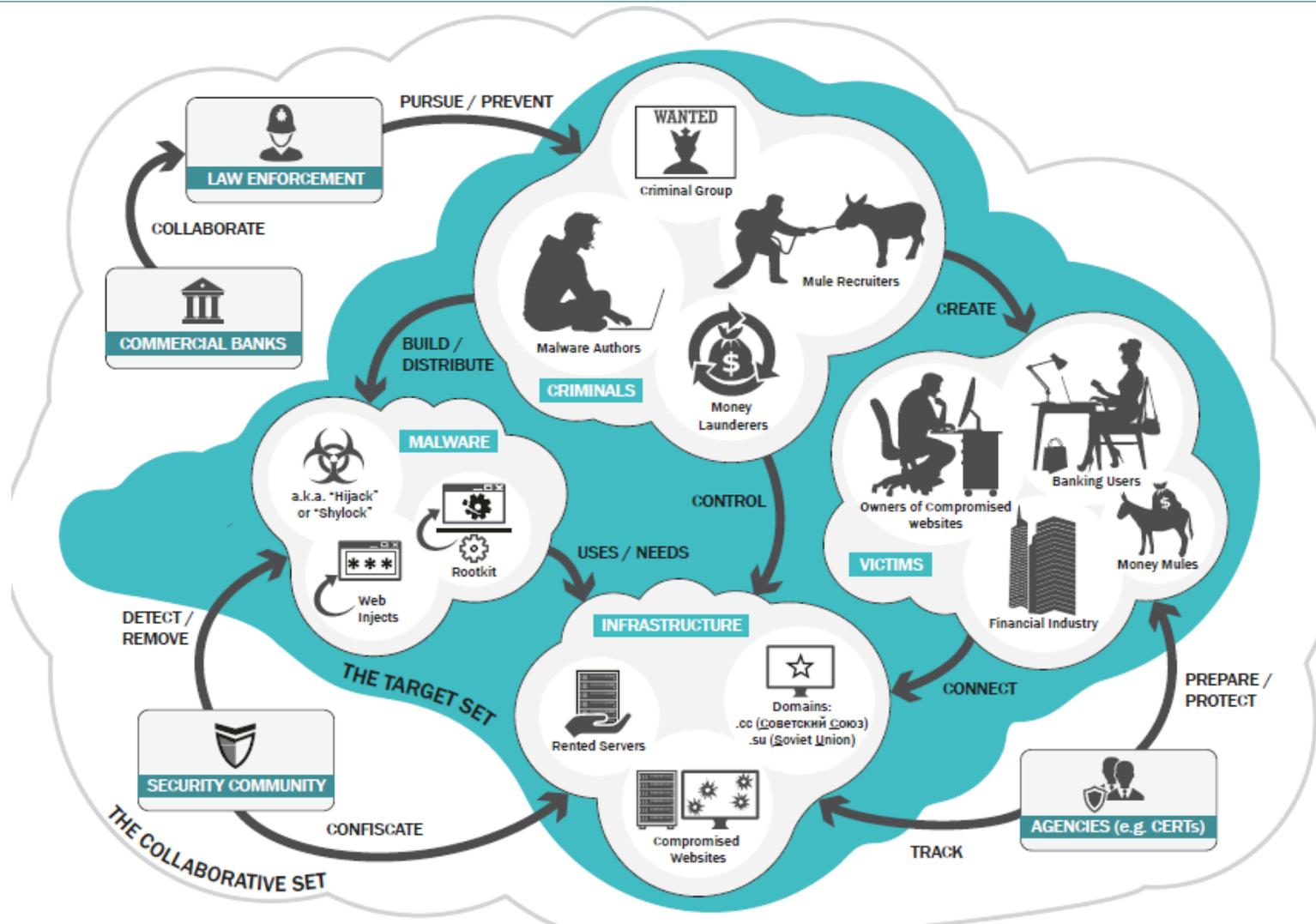
MAIN FEATURES
Order your item from any U.S. based online store and have it delivered to your international address within 15 days!

3 EASY STEPS
1. Register with our service.
2. Choose your desired product.
3. Complete your payment.

SATISFACTION GUARANTEED
Over 100,000+ satisfied customers and over 50% repeat customers that prefer and trust our services over others.



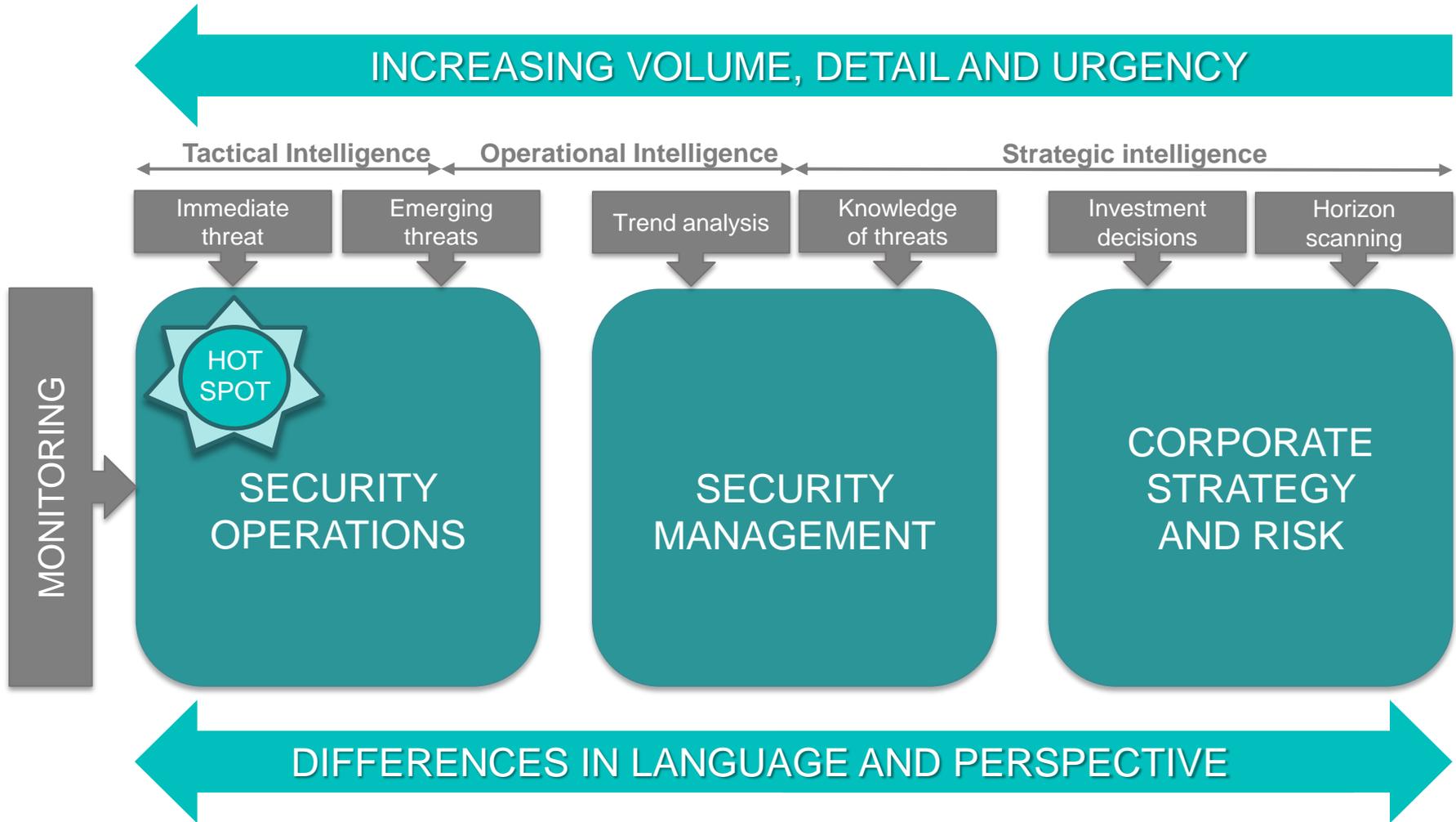
THE SHYLOCK TAKEDOWN – INTELLIGENCE INTO ACTION



Making threat intelligence work

Turning people, process and technology into action

FORMS OF THREAT INTELLIGENCE



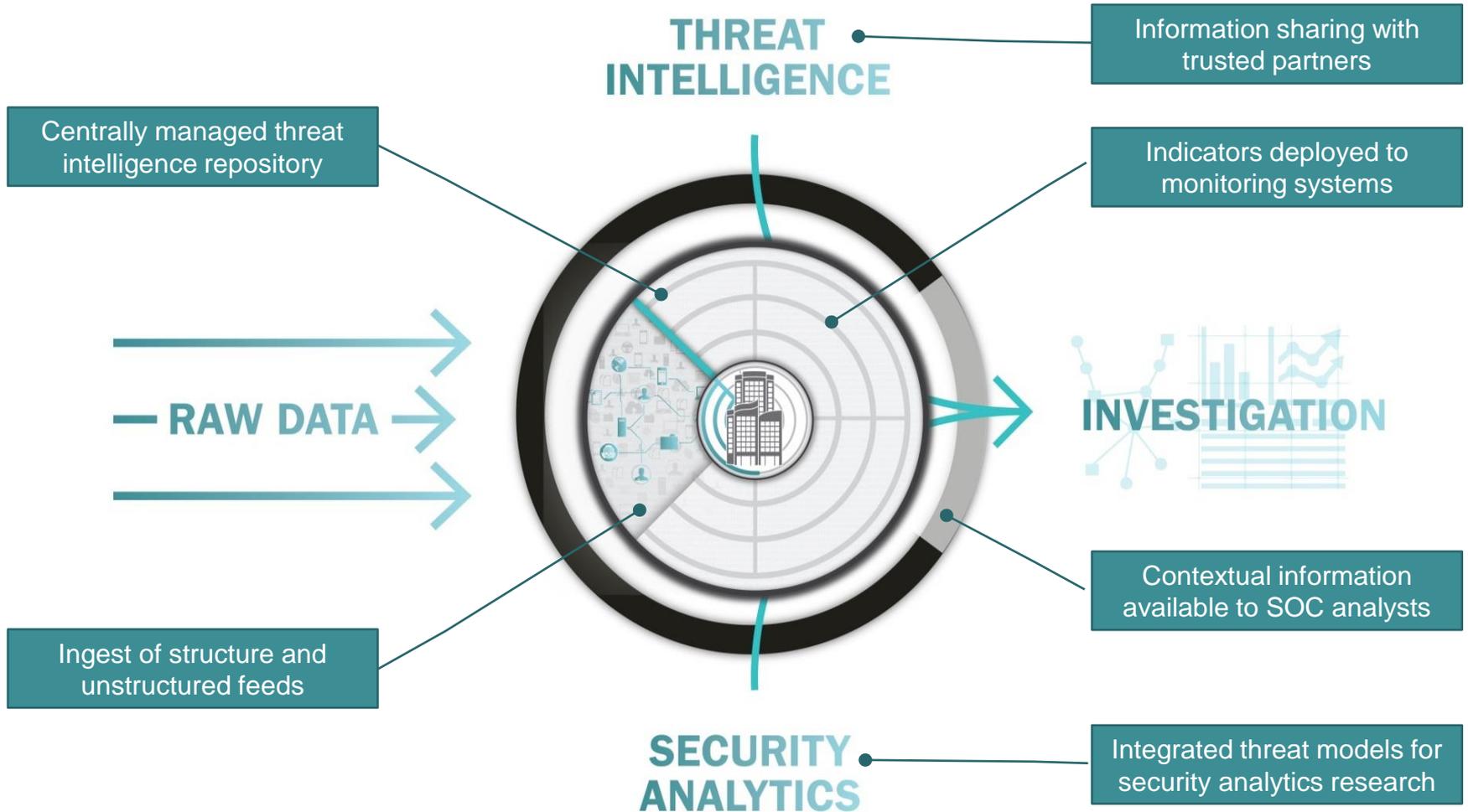
MAKING THREAT INTELLIGENCE WORK – PEOPLE



MAKING THREAT INTELLIGENCE WORK – ACTION



...IN A SECURITY OPERATIONS ENVIRONMENT



James Calder
Client Services Manager, Singapore

BAE Systems Applied Intelligence
Level 28, Menara Binjai
2 Jalan Binjai
Kuala Lumpur, 50450
Malaysia

T: +60 (3) 2191 3000
F: +60 (3)1483 816144



www.twitter.com/baesystems_ai



www.linkedin.com/company/baesystemsai

Copyright © BAE Systems 2014. All rights reserved. BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc. BAE Systems Detica and BAE Systems Applied Intelligence are trading names of Detica Limited registered in England (No.1337451) with its registered office at Surrey Research Park, Guildford, England, GU2 7RQ.