



27th ANNUAL
FIRST BERLIN
CONFERENCE

14-19 JUNE 2015

**UNIFIED SECURITY:
IMPROVING THE FUTURE**



The Daily Show Agenda

Chris Hall, Wapack Labs



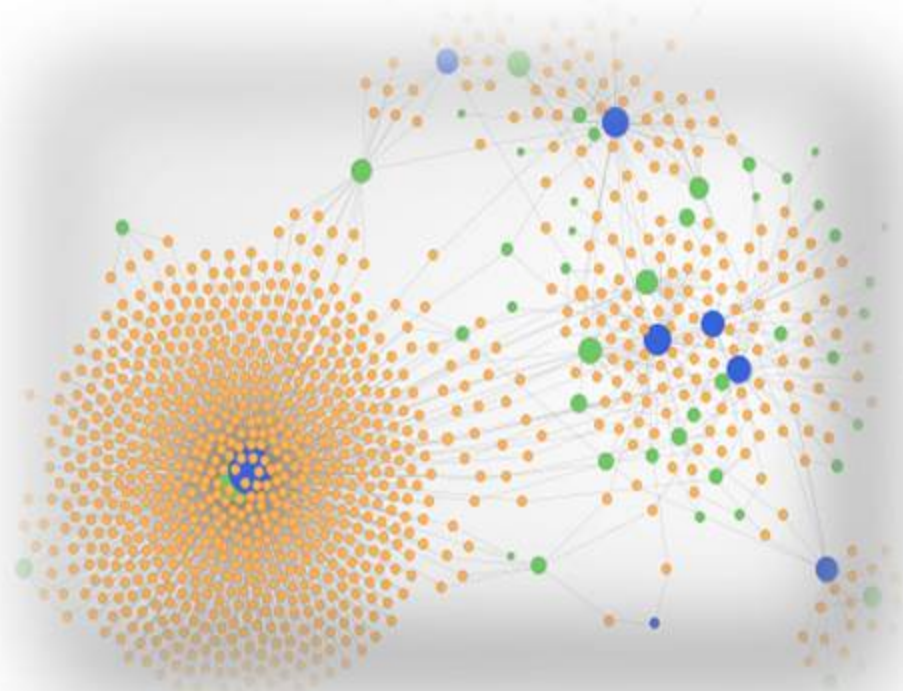
What is Daily Show?...

- A series of global cyber espionage campaigns - presumed related;
- Primarily targeting :
 - Maritime Transportation & Logistics
 - Oil, Gas & Petrochemical
 - most downstream sectors
 - Industrial Manufacturing



What is Daily Show?...

- Three distinct clusters of activity to date:
 - **“Daily Jon”**
 - Primarily Maritime Transportation targeting
 - **“Daily Mom”**
 - Primarily Oil, Gas, Petrochemical and manufacturing targeting
 - **“Daily Rom”**
 - Primarily Oil, Gas, Petrochemical and manufacturing targeting



It all started with a Google dork...



"Operating System Intel Recovery"

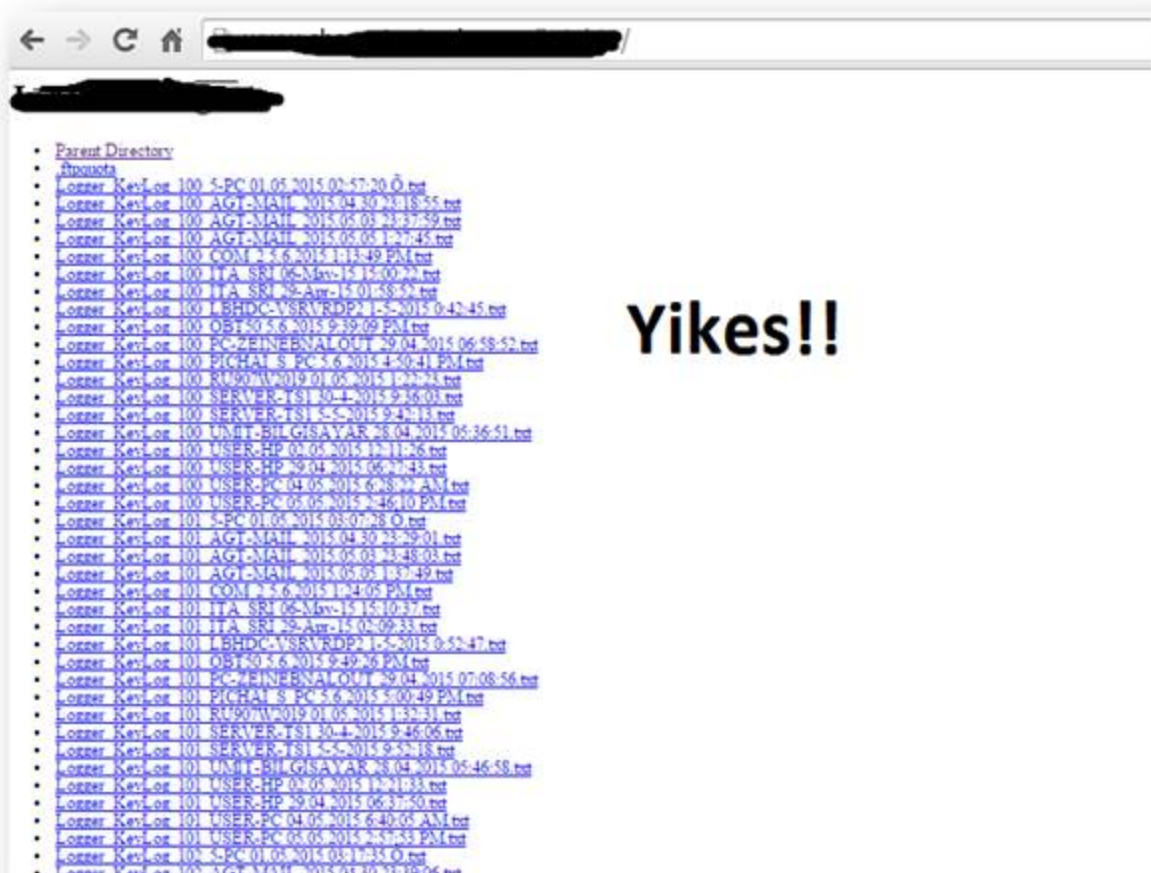
Ø6 ***** Operating ...
[REDACTED]/.../Logger_Recovery_Log_UTPAL-PC%2021.02.2015%... ▾
Feb 21, 2015 - Ø6 ***** Operating System Intel
Recovery ***** CPU Name: ...

[Operating System Intel Recovery ...](#)

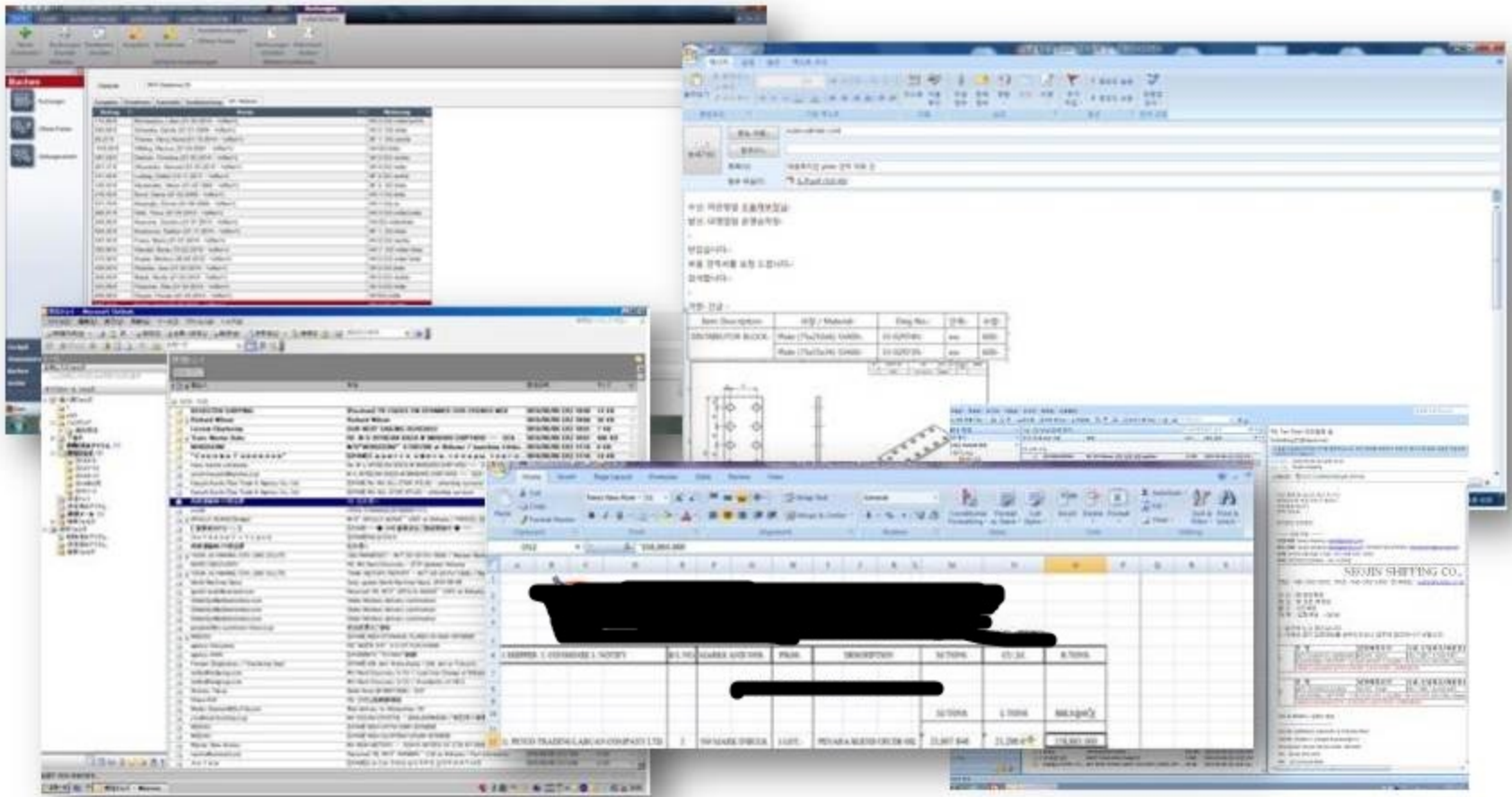
[REDACTED]_Logger_Recovery_Log_PATILANCI-PC%2031.10.2014%2... ▾
... Operating System Intel Recovery ***** CPU
Name: PATILANCI-PC Local Date and Time: 31.10.2014 г. 11:10:06 ч.



It all started with a Google dork...



It all started with Google dork...



It all started with Google dork...

Operating System Intel Recovery

CPU Name: WSW71715
Local Date and Time: 20.03.2015 17:05:57
Installed Language: ru-RU
Net Version: 2.0.50727.5420
Operating System Platform: Win32NT
Operating System Version: 6.1.7601.65536
Operating System: Microsoft Windows [redacted]
Installed Anti-Virus: System Center Endpoint Protection
Installed Firewall: [redacted]

WEB Browser Password Recovery

URL : [redacted]
Web Browser : Chrome
User Name : [redacted]
Password : [redacted]
Password Strength : Very Strong
User Name Field : [redacted]
Password Field : [redacted]

URL : [redacted]
Web Browser : Chrome
User Name : [redacted]
Password : [redacted]
Password Strength : Strong
User Name Field : [redacted]
Password Field : [redacted]

URL : [redacted]
Web Browser : Chrome
User Name : [redacted]
Password : [redacted]
Password Strength : Strong
User Name Field : [redacted]
Password Field : [redacted]

■ ■ ■

```
Follow TCP Stream
Stream Content
220 mx1.main-hosting.com ESMTP [Main-hosting.com Mail System]
EHLO [REDACTED]
250-mx1.main-hosting.com
250-PIPELINING
250-SIZE 5728640
250-ETRN
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
AUTH login [REDACTED]
[REDACTED]
235 2.7.0 Authentication successful
MAIL FROM: [REDACTED]
250 2.1.0 Ok
RCPT TO: [REDACTED]
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
mime-version: 1.0
from: [REDACTED]
to: [REDACTED]
date: 19 Apr 2015 18:16:08 -0400
subject: Logger - Server Ran - [REDACTED]
content-type: text/plain; charset=us-ascii
content-transfer-encoding: quoted-printable

This is an email notifying you that BUSTER1-3FE475D has ran your logger=
and emails should be sent to you shortly and at interval chosen.=00=0A=
=00=0ALogger Details: =00=0AServer Name: window.exe=00=0Akeylogger Enabled:=
True=00=0AClipboard-Logger Enabled: True=00=0ATime Logs will be delivered:=
Every 30 minutes=00=0A =00=0Astealers Enabled: True=00=0ATime Log will=
be delivered: Average 2 to 4 minutes=00=0A =00=0ALocal Date and Time: 4/19/2015=
6:16:06 PM=00=0AInstalled Language: en-US=00=0AOperating System: Microsoft=
Windows XP Professional=00=0AInternal IP Address: 192.168.35.128=00=0AExternal=
IP Address: [REDACTED]=00=0AInstalled Anti-virus: =00=0AInstalled Firewall:=
```



■ ■ ■

The screenshot displays a Windows desktop environment with three overlapping windows:

- Follow TCP Stream:** A small window titled "Follow TCP Stream" showing "Stream Content" with the following text:

```
220 mx1.main-hosting.com ESMTP [Main-hosting.com Mail System]
EHL[REDACTED]
250-mx1.main-hosting.com
250-PIPELINING
250-SIZE 5728640
```
- Outlook:** An Outlook inbox window showing a list of emails. The subject line for the selected email is "Logger - Key Recorder - [KSK-RAHAYU]". The "From" field is "admin@bl[REDACTED].com".
- File Explorer:** A File Explorer window titled "DL Sales Report" showing a file named "CS22925.tmp" with a size of 808 KB, modified on 4/15/2015 at 9:34 AM.



Filter

Search from date (dd.mm): 30.04 to date: 08.05

Bots: Botnets:

IP-addresses: Countries:

Search string:

Type of report: HTTP or HTTPS request

- Case sensitive
- Exclude robots
- Show only requests
- Show as text
- HTTP or HTTPS request
- HTTP request
- HTTPS request
- FTP login
- POP3 login
- VNC Connection Event
- All grabbed data
- Grabbed data [UI]
- Grabbed data [HTTP(S)]

Reset form Search Remove

Result:

Bots action: Full information

0.04.2015

Reports for this date not founded.

1.05.2015

View report [HTTP request, 608 bytes]

Get ID: [REDACTED]

Email: [REDACTED]

Source: [REDACTED]

OS version: [REDACTED]

OS Language: [REDACTED]

User-Agent: [REDACTED]

Request Size: [REDACTED]

Request Time: [REDACTED]

IP: [REDACTED]

Connected for bot: [REDACTED]

In the list of users: [REDACTED]

Private search: [REDACTED]

User of process: [REDACTED]

Source: [REDACTED]

http://129.124.116.26/browse/interface/getviewstat

Open: Input: w3gen+ Vegetables And/or Products @102.comgoogle.com.google.com.cw 499 Course Reels Farm Machinery & Equipment- Equipment Fresh Seafood- Grain Nuts/Seeds & Truffles

Request:

[REDACTED]

111.101.Safari/537.36

12440FD=1422064256



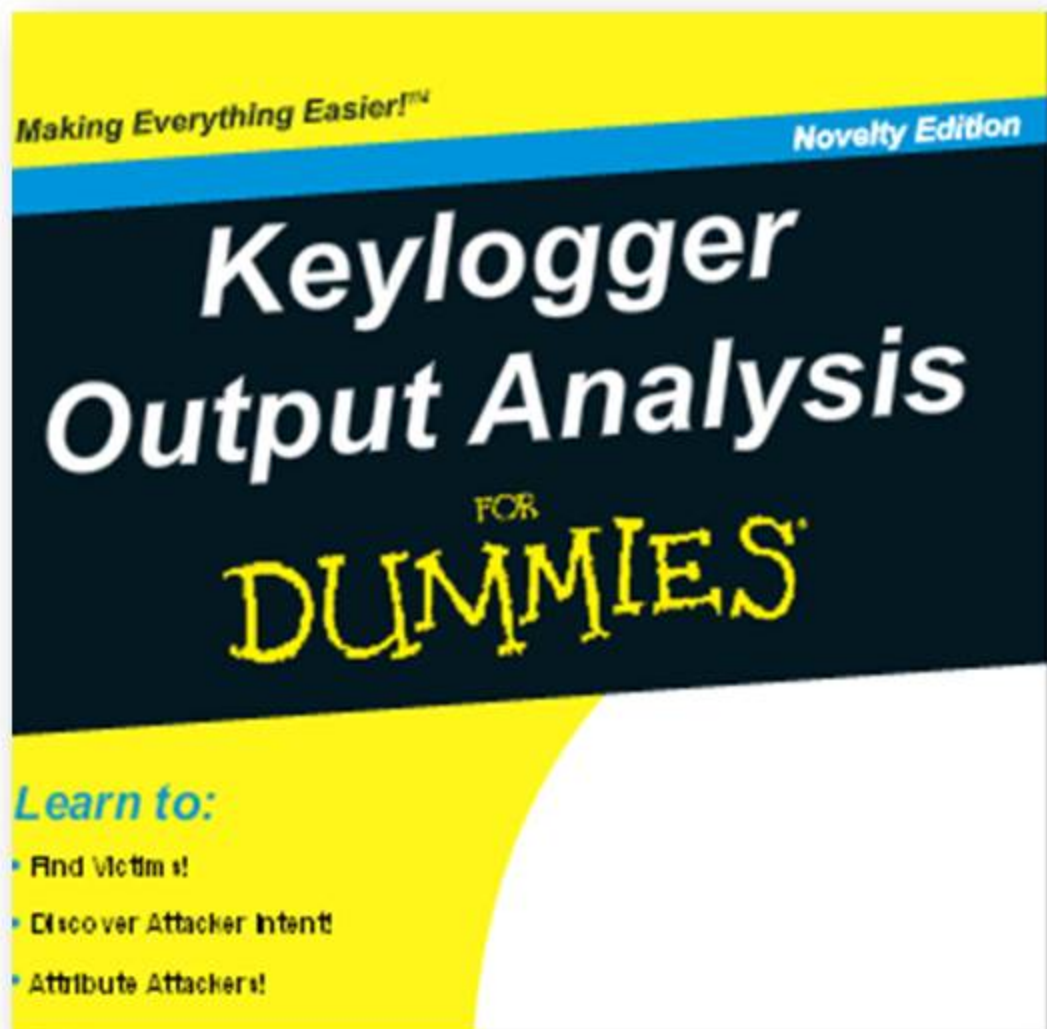
The (“big data”) problem..

What do you do when you stumble upon ...

- Thousands of key-logger output files (in multiple formats)
- Thousands of screenshots
- ***Perishable Intel***

?

The (“big data”) problem..



The (“big data”) problem..

Approach

- Scheduled tasks – Wget
- Parsing – Python
- Storage and Accessibility – MySQL
- Victimology / Data Mining –
 - ID compromised sites/emails
 - ID trends

The real problem..

Deconstructing Key-log Files:

- Concrete
 - science

Deconstructing intent:

- Abstract
 - art

Think like a criminal..

- What would you do with near perfect access and intelligence on:
 - ports
 - customs
 - shipping companies
 - finance
 - supply chain/procurement
 - **Oil and gas**
 - **manufacturing**



Objectives

- Create a plan to distribute goods and/or monitor and manipulate trade
- Identify a means to monitor and manipulate comings and goings of all activities in the ports.
- Identify a means of moving illegally gotten money without being caught.

How do we distribute our <stuff> internationally without being caught?



MarineTraffic [Live Map](#) [Vessels](#) [Ports](#) [Photos](#) [Participate](#) [Services](#)

CHAMPION TRADER

Chemical Tanker Fleet con


IMO: 9127667	Gross Tonnage: 21897
MMSI: 636014994	Deadweight: 40727 t
Call Sign: A8XY3	Length x Breadth: 188.73m x 29.5m
Flag: Liberia (LR)	Year Built: 1995
AIS Type: Tanker	Status: Active

Last Position Received Out of range


 Newer position available via Satellite 

Info Received: 2015-03-26 12:39
Area: Mediterranean
Latitude / Longitude: 31.1835° / 32.30517°
Status: Underway
Speed/Course: 9.3kn / 177°
AIS Source: 1416

Itineraries History
Latest Positions
Nearby Vessels



© JACK CLIFFORD
MarineTraffic.com



Know the routes.
Understand
movement, and
how/where cargo
gets tracked.

Imagine shipping UPS.
Use the tracking system
to send a test package,
and target the nodes.

It won't take long to
figure out where
packages get
transferred.

International shipping
works the same way.



Funktioner Rapporter System Hjælp

F	Navn	96t	NA	T	Skib	ETA da	ETA	Note
		2	0	NG		22-03	09:00	
		0	0	G		21-03	19:00	B
▶		69	0					
		73	1	NG		21-03	22:30	
		31	1	NG		22-03	19:00	
		45	0	G	S	22-03	01:00	
		69	0					
		26	1	G	S	22-03	00:25	



Then control them.. How?
Pick the right targets.

There's always a risk |reward | amount of work calculation necessary to access and hold access in systems that will allow continued, reliable monitoring or manipulation throughout the operation.

Target determination and prioritization:

1. Administrative – Enterprise Resource Planning System
2. Port operations – Command and control room

<i>Components of typical port operations*</i>	<i>Access required</i>	<i>Risk of of being caught during access</i>	<i>Work required by attacker (to gain access)</i>	<i>What would the attacker gain access to?</i>
<i>Cameras near cranes</i>	Physical	High	High	Limited
<i>License plate recognition connected to the dispatch systems</i>	Physical	High	High	Internal movement systems
<i>Wireless terminals used for field work</i>	Remote, but within wireless range	Low	Medium	Movement, inventory, dock work, coordination
<i>Command and control room</i>	Remote	Medium	Low	All internal operational systems
<i>Interfaces to external systems such as Enterprise Resource Planning systems, used to track employees, logistics, accounting, other.</i>	Remote	Low	Low	Full administrative access

* SOURCE: Magal S3 Corporation

ERP!

ERP can be used to satisfy both requirements—distribution and movement of money!

- VAT
- Customs
- Inventory tracking (fraud?)
- Money movement

ERP is a **SCHAAWEEEEET** target.... And these bad guys own it.

Voucher Display

Sales

No. : B437
Date : 11-Sep-2014
Reference :
Party Ledger A/c

Name of Item
[Redacted]

Total

Narration:

So, now that we know our desired target, How do we exploit the first victim?

Logistics are arranged by an 'agent' before a ship arrives in port.

This could include cargo transfer, or replenish food or fuel.

An email would normally include a large attachment with a list of requirements and payment information.

This attachment contained a special gift... a keylogger.

(OFFER)M/V AMERICAN SPIRIT AGENCY APPOINTMENT

Taylor Spencer [AS: [REDACTED]]

You replied on 3/30/2015 10:47 AM.

Sent: Mon 3/30/2015 4:27 AM

To: [REDACTED]

Message | shipment particulars.zip (2 MB) | _Certification_.txt (250 B)

From: AMERICAN STEAMSHIP COMPANY

On behalf of AMERICAN STEAMSHIP COMPANY a subsidiary of GATX Corporation, the owners and managers of The M/V American Spirit.

We would hereby like to officially nominate you as our agent for M/V American Spirit.

ATTACHED IS THE SI/ITENERARY AND VESSEL SHIPMENT PARTICULARS.

The vessel will call at your Port on the 4th of April 2015.

PLS ADVISE US OF THE FOLLOWING ITEMS ON URGENT BASIS.

1) ADVISE US OF FLWG ITEMS-

1. ESTIMATED VESSEL'S SCHEDULE
2. ESTIMATED PORT EXPENSES
3. OTHER INFORMATION IF ANY

Which dumps user credentials to every account used by that user. Over 15Gb recovered to date.

- Credentials
 - Computer login, email
 - All web accounts - including credentials for corporate resources
 - Application keys for all applications on the system
- Screen shots of shipping manifests
- Financial transactions between importing and exporting parties.

```
Éz
Operating System Intel Recovery
-----
CPU Name: WSW71715
Local Date and Time: 20.03.2015 17:05:57
Installed Language: ru-RU
Net Version: 2.0.50727.5420
Operating System Platform: Win32
Operating System Version: 6.1.7600.5512
Internal IP Address: [REDACTED]
External IP Address: [REDACTED]
Installed Anti-Virus: System Center
Installed Firewall: [REDACTED]
-----
URL : ftp://ftp.1
Web Browser : Chrome
User Name : [REDACTED]
Password : [REDACTED]
Password Strength : Very Strong
User Name Field :
Password Field :
-----
URL : ftp://konar
Web Browser : Chrome
User Name : [REDACTED]
Password : [REDACTED]
Password Strength : Strong
User Name Field :
Password Field :
-----
URL : http://217.
Web Browser : Chrome
User Name : [REDACTED]
Password : [REDACTED]
Password Strength : Strong
User Name Field :
Password Field :
-----
URL : http://file
Web Browser : Chrome
User Name : [REDACTED]
Password : [REDACTED]
Password Strength : Strong
-----
Name : [REDACTED]
Application : Thunderbird
Email : [REDACTED]
Server : [REDACTED]
Server Port :
Secured : No
Type : POP3
User : [REDACTED]
Password : [REDACTED]
Profile :
Password Strength : Very Strong
SMTP Server :
SMTP Server Port :
-----
Name : [REDACTED]
Application : Thunderbird
Email : [REDACTED]
Server : [REDACTED]
Server Port :
Secured : No
Type : IMAP
User : [REDACTED]
Password : [REDACTED]
Profile :
Password Strength : Very Weak
SMTP Server :
SMTP Server Port :
-----
Name : [REDACTED]
Application : Thunderbird
Email : [REDACTED]
Server : [REDACTED]
Server Port : 995
Secured : No
Type : POP3
User : [REDACTED]
Password : [REDACTED]
Profile : [REDACTED]
```

Once in, nothing is off limits.



- Customs
- Manifests
- Financials
- Movements/schedule
s
- More??

Is this real?

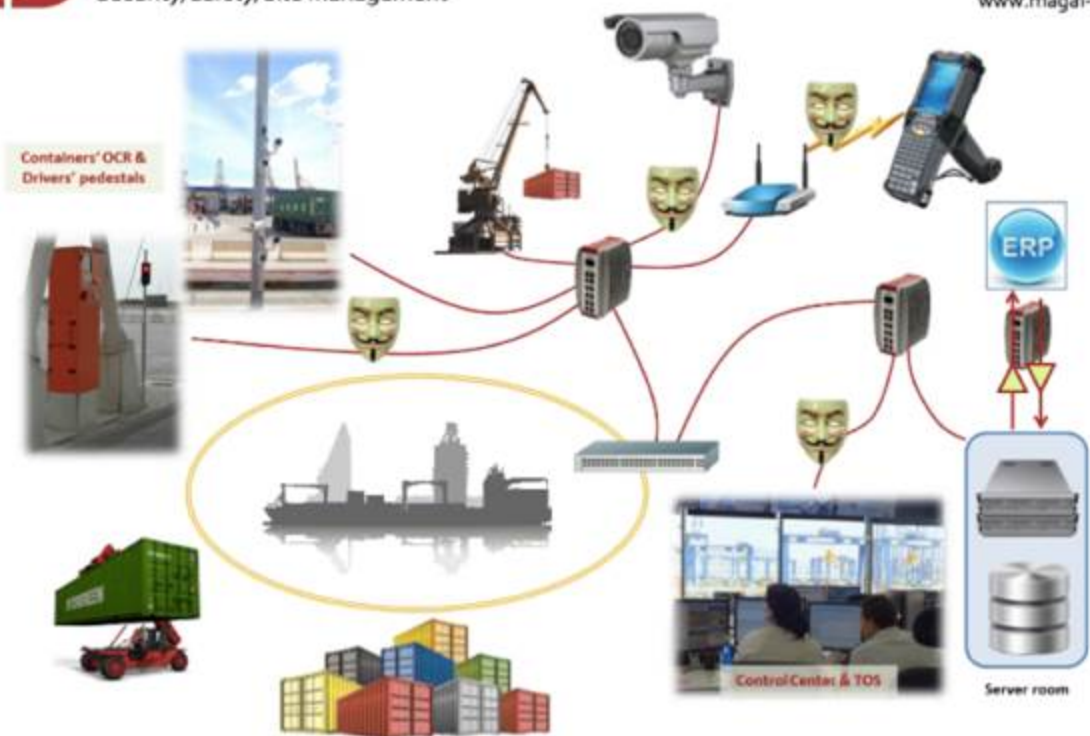
Absolutely.

Targeting ERP in a port allows hackers to freeze frames on video cameras, disable vessel tracking systems, create temporary delays in movements, falsify container counts/weights, and more.

...and it all started with one email.



17 Altalef Street
Yehud Industrial Zone, Israel 56100
T: 972-3-539-1444 F: 972-3-536-6245
www.magal-s3.com



An example... Antwerp

Police warning after drug traffickers' cyber-attack

By Tom Bateman
Reporter, Today programme

🕒 16 October 2013 | Europe

The head of Europe's crime fighting agency has warned of the growing risk of organised crime groups using cyber-attacks to allow them to traffic drugs.

The director of Europol, Rob Wainwright, says the internet is being used to facilitate the international drug trafficking business.

His comments follow a cyber-attack on the Belgian port of Antwerp.

Drug traffickers recruited hackers to breach IT systems that controlled the movement and location of containers.



Earlier this year drug traffickers hacked into the computer controlling shipping containers at the port of Antwerp

Money movement becomes much easier

- VAT Fraud – Missing Trader, Carousel Fraud
- Money Laundering
- Fake user accounts and payments...
- The world is now your illegal oyster.



Target Supply Chain

How?

- Exploit trust relationships
 - Manufacturers
 - Distributers
 - Suppliers
 - Logistics



Target Supply Chain

How?

- Identify Industries
- Identify “must-haves” for multiple industries
- Target the “must-haves” suppliers



Target Supply Chain

Must Haves:

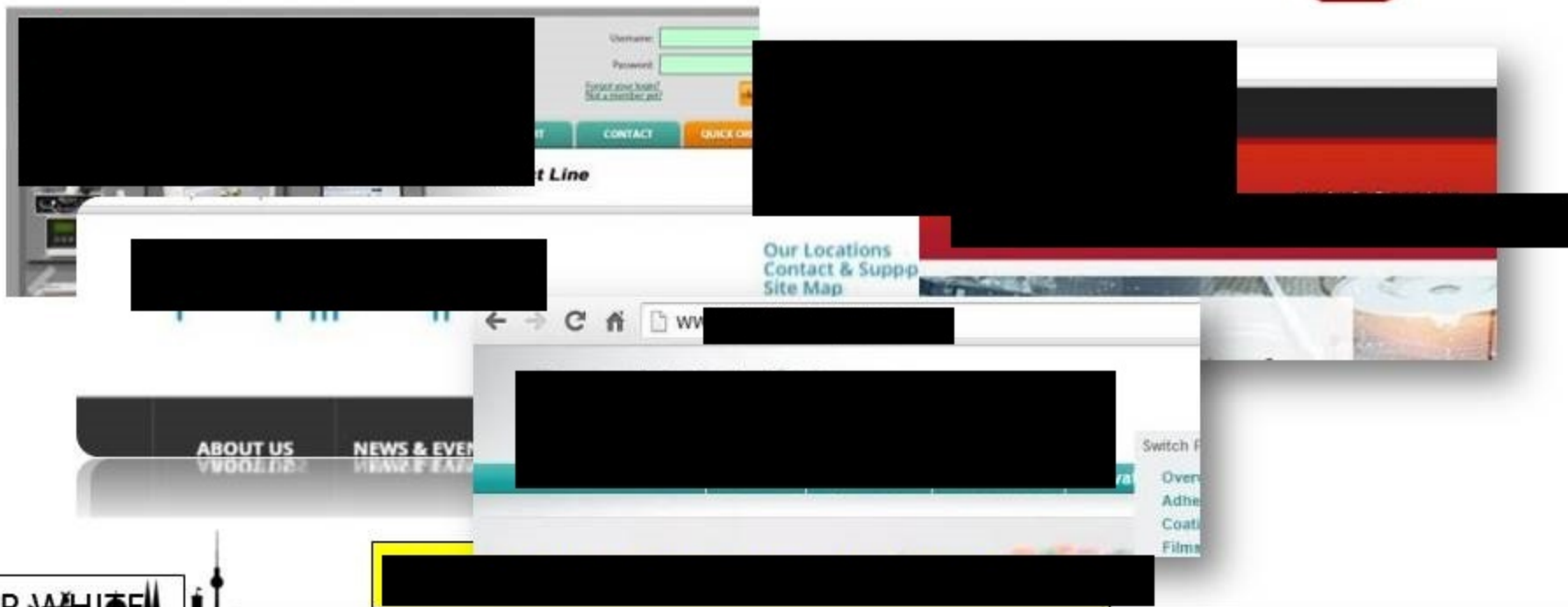
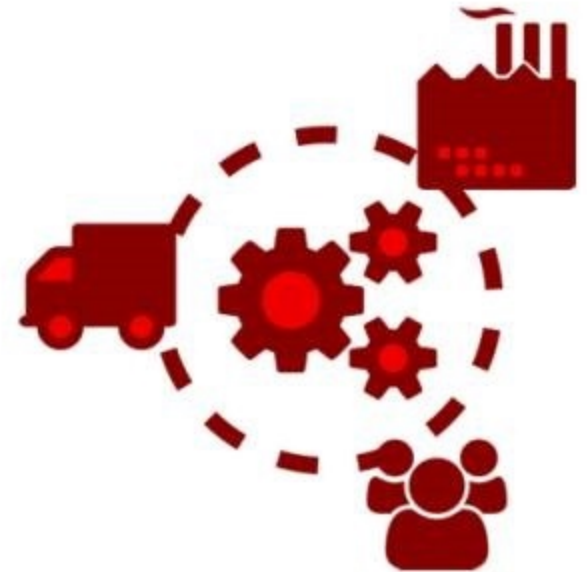
- Petrochemicals:
 - Lubricants
 - Plastics, polymers
- Parts
 - Bearings
 - Valves



Target Supply Chain

Go after the little guy
*Small Medical Respirator
Manufacturer*

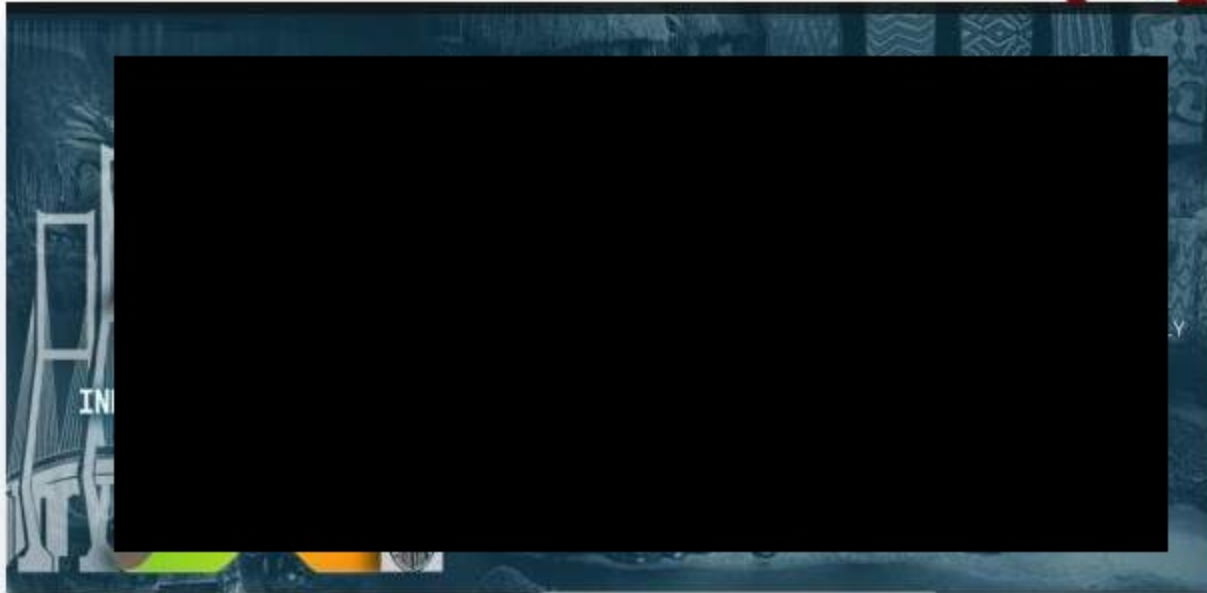
*Leads to intel on petrochemical
suppliers*



Target Supply Chain

Go after the conferences

Supply Chain Mgmt Summit



Target Supply Chain

Go after the conferences

Supply Chain Mgmt Summit

A screenshot of a web browser displaying a directory listing for the path /uploads. The browser's address bar is redacted with a black box. The page title is "Index of /uploads". The listing table has columns for Name, Last modified, Size, and Description. The Name column is mostly redacted with a large black box. The Last modified and Size columns contain data for several files. The footer of the page reads "Apache/2.4.10 (Ubuntu) Server at scmsummit.co.id Port 80".

Name	Last modified	Size	Description
[REDACTED]	2015-04-13 01:03	334K	-
[REDACTED]	2015-04-01 11:42	285K	-
[REDACTED]	2015-03-30 17:35	1.1M	-
[REDACTED]	2015-04-02 11:30	1.0M	-
[REDACTED]	2015-04-10 11:15	-	-
[REDACTED]	2015-04-16 10:36	-	-
[REDACTED]	2015-04-17 14:26	-	-
[REDACTED]	2015-04-06 16:25	-	-
[REDACTED]	2015-04-14 02:21	-	-
[REDACTED]	2015-04-20 20:37	-	-
[REDACTED]	2015-03-16 17:55	-	-
[REDACTED]	2015-04-13 12:44	-	-



Target Supply Chain

Go after the conferences

Supply Chain Mgmt Summit

A collage of various documents and forms, likely related to supply chain management. The documents include:

- A shipping label with fields for 'To', 'From', 'Weight', and 'Volume'. The 'To' field contains a redacted address.
- An email message with a redacted sender and recipient.
- A form with a logo and text, possibly a contract or invoice.
- A document with a large redacted area.
- A document with a table of data, possibly a shipping schedule or inventory list.



Target Supply Chain

Go after procurement



EPROCUREMENT SYSTEM

Main Menu

Print Eport E-Mail Upload Language

Lalgar Vouchers www.Tally60.com

Company Solutions

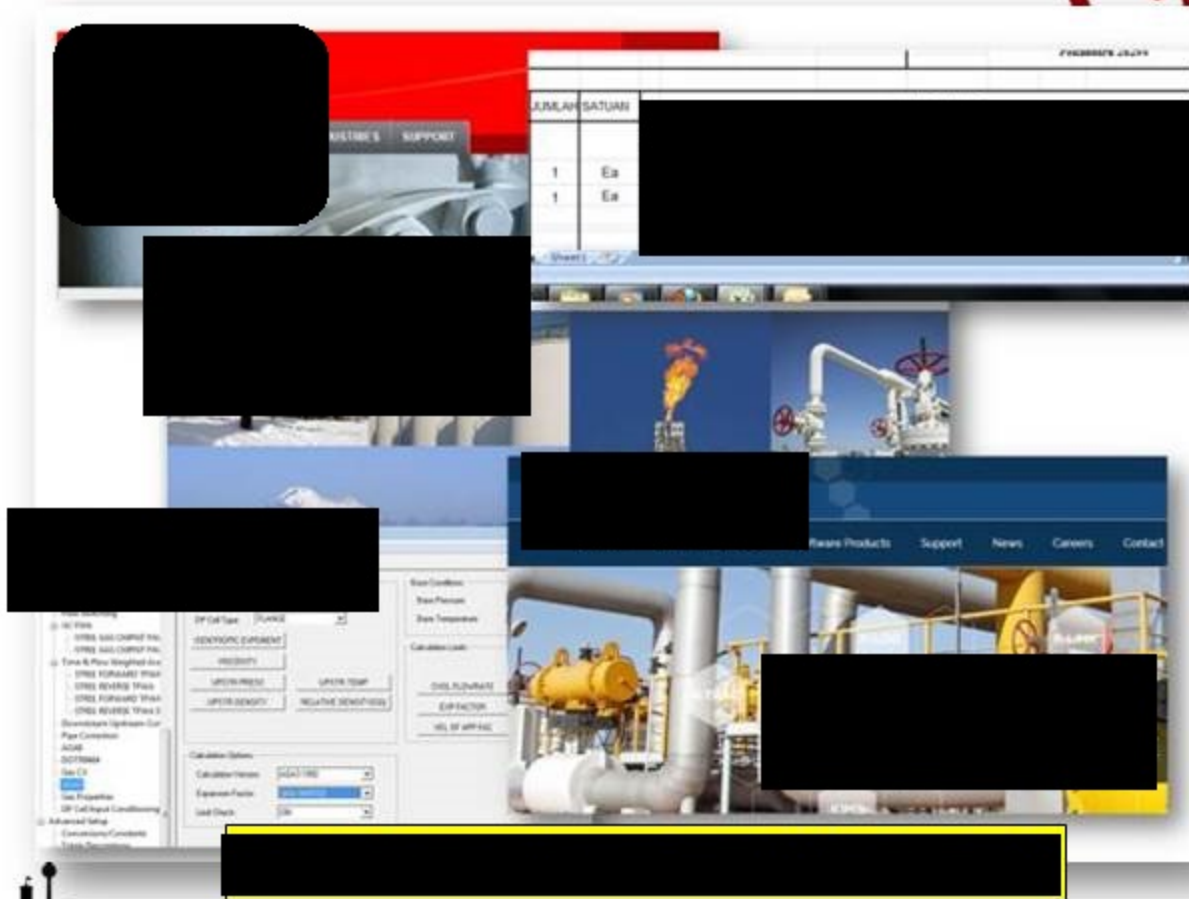
e-Procurement

Procurement



Target Supply Chain

*Go after the pipes:
Flow Metering*



Target Supply Chain

Go after parts manufacturers:



Target Supply Chain

Go after parts manufacturers:



Dear [REDACTED]

Thanks for your inquiry, This is [REDACTED] from [REDACTED] we have our own factory which have produced bearings for 16 years. Our products main include pillow block bearing, deep groove ball bearing and taper roller bearing.

Please tell me the models of bearing you need, the quantity and requirements of quality, so we can quote you best.

Best regards,

Alice

Alice



[General Mechanical Components](#) [REDACTED] [Bearing Manufacturer](#)

Hello

Target Supply Chain

Go after parts manufacturers:



Dear [REDACTED]

We would like to do business with you/our company. Please check attachment to view our specifications/document to see if you can provide the parts.

Thanks for your time and effort. We appreciate your response.

Please let us know if you have any questions.

Best regards,

Alice

David Perlmutter
Windows Corporation
VP Executive team
2200 Mission College Blvd.
Santa Clara, CA 95054-1543
USA

Copy#064046

16

 [General Mechanical Components](#) [REDACTED]

[REDACTED]

Hello

[REDACTED]

Why Bearings??



Why Bearings??



Why Bearings??

- Supply Chain!
 - Closely tied to downstream sectors
 - Multiple Industry coverage



Daily Show

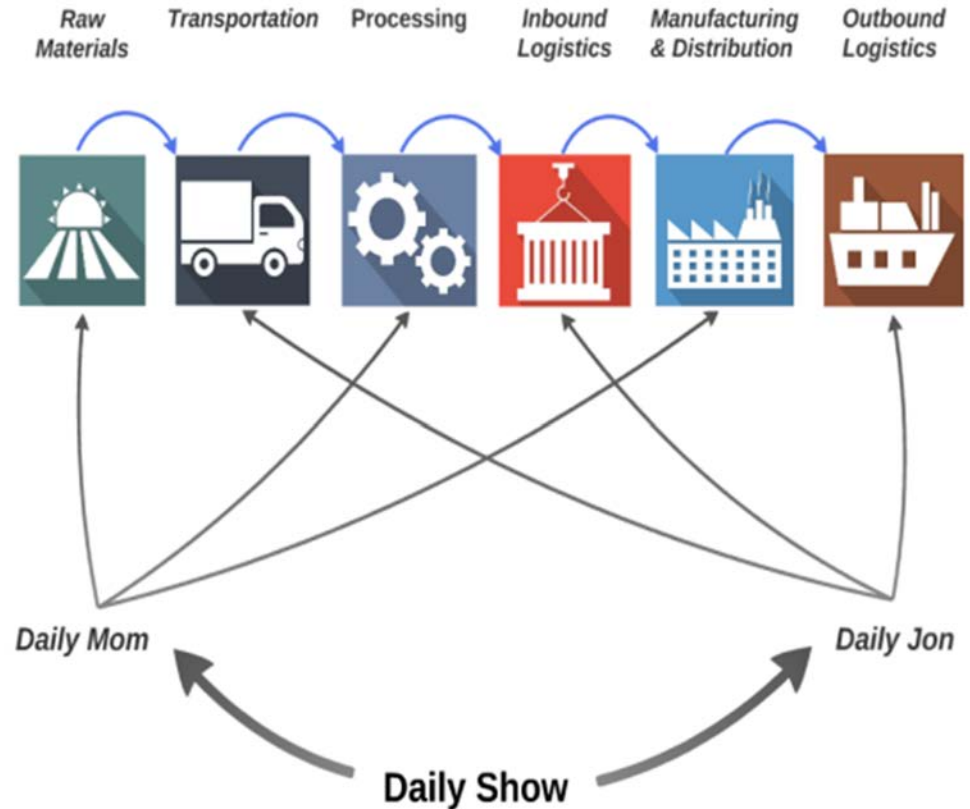


- Nearly every major port targeted... from LA to Singapore.
- Comprehensive supply chain targeting
 - Most downstream sectors
- 70+ domains and servers
- 1500+ victims and counting
- More than 15Gb of credentials, screenshots, and documents recovered to date.

Main targets?

– Supply Chain

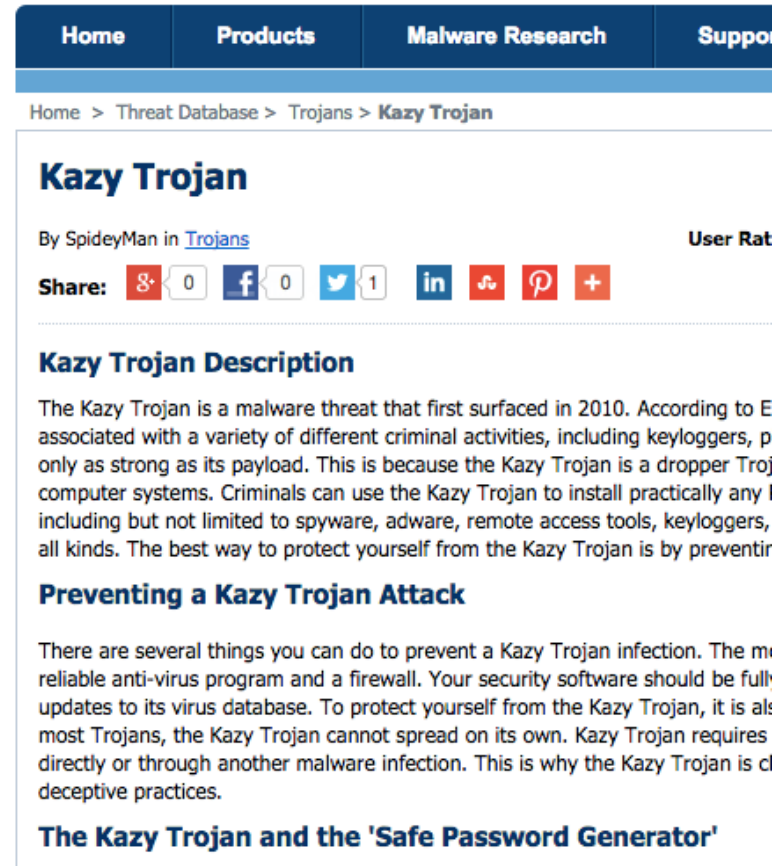
- **Logistics**
 - Maritime Transport
- **Manufacturing**
 - Materials
- **ERP / Procurement**
 - All of the above



That one email deployed Kazy keylogger

- Widely deployed
- Long used (2010)
- Many variants:
 - Hawkeye
 - Predator
 - Cyborg

Some with zero AV detection



The screenshot shows a webpage with a dark blue navigation bar containing links for Home, Products, Malware Research, and Support. Below the navigation bar is a breadcrumb trail: Home > Threat Database > Trojans > Kazy Trojan. The main content area features the title "Kazy Trojan" in a large, bold, blue font. Below the title, it says "By SpideyMan in Trojans" and "User Rating". There is a "Share:" section with icons for Google+, Facebook, Twitter, LinkedIn, Reddit, and Pinterest, along with a plus sign for more options. The counts for these shares are: Google+ (0), Facebook (0), Twitter (1), LinkedIn (0), Reddit (0), and Pinterest (0). Below the share section is a "Kazy Trojan Description" section with a paragraph of text. Underneath that is a "Preventing a Kazy Trojan Attack" section with another paragraph of text. At the bottom of the visible content is a link titled "The Kazy Trojan and the 'Safe Password Generator'".

Home > Threat Database > Trojans > **Kazy Trojan**

Kazy Trojan

By SpideyMan in [Trojans](#) User Rating

Share: 0 0 1 0 0 0

Kazy Trojan Description

The Kazy Trojan is a malware threat that first surfaced in 2010. According to E associated with a variety of different criminal activities, including keyloggers, p only as strong as its payload. This is because the Kazy Trojan is a dropper Troj computer systems. Criminals can use the Kazy Trojan to install practically any I including but not limited to spyware, adware, remote access tools, keyloggers, all kinds. The best way to protect yourself from the Kazy Trojan is by preventir

Preventing a Kazy Trojan Attack

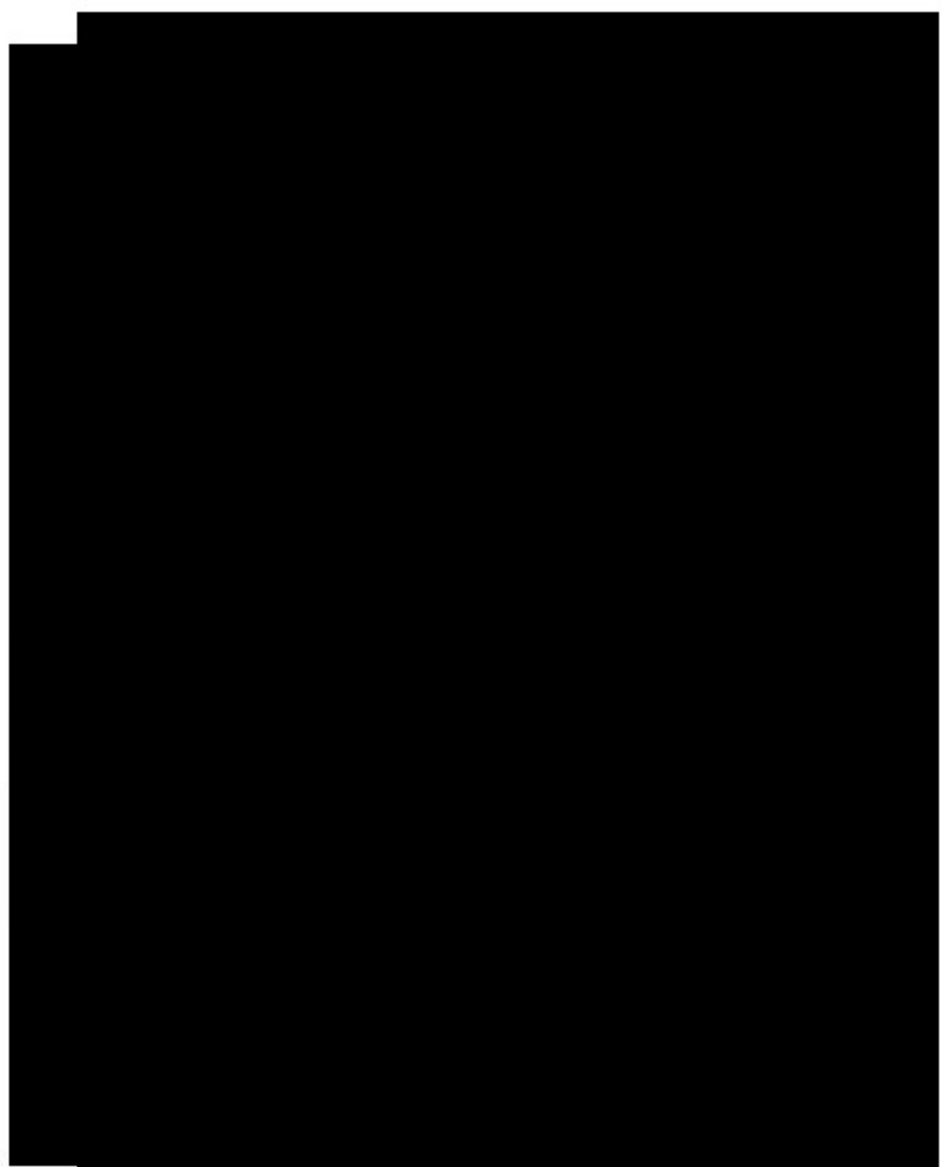
There are several things you can do to prevent a Kazy Trojan infection. The m reliable anti-virus program and a firewall. Your security software should be full updates to its virus database. To protect yourself from the Kazy Trojan, it is al most Trojans, the Kazy Trojan cannot spread on its own. Kazy Trojan requires directly or through another malware infection. This is why the Kazy Trojan is cl deceptive practices.

The Kazy Trojan and the 'Safe Password Generator'

Exploiting others

- Maritime Shipping Companies
- Logistics Companies
- Manufacturing – Oil and Gas
- Chemical and Pharma
- Energy
 - [REDACTED]
- Customs Offices
 - [REDACTED]
- Real Estate (Financing)

Financial systems also targeted:



What do we think it is??

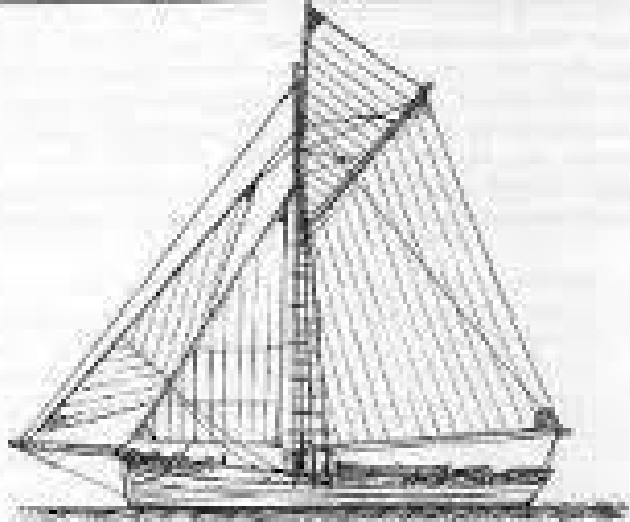
What do they want?

Intelligence

(High Confidence: 75%+)

This TTP offers a full view of all happenings in and around major world ports.

- **Military?** Unrest in the middle east requires to need to monitor comings and goings of troops, aid, logistics.
- **Pirating?** Pirate operations are becoming more high tech.
- **Commercial?** Many routes include Oil & Gas.
- **Drugs?**



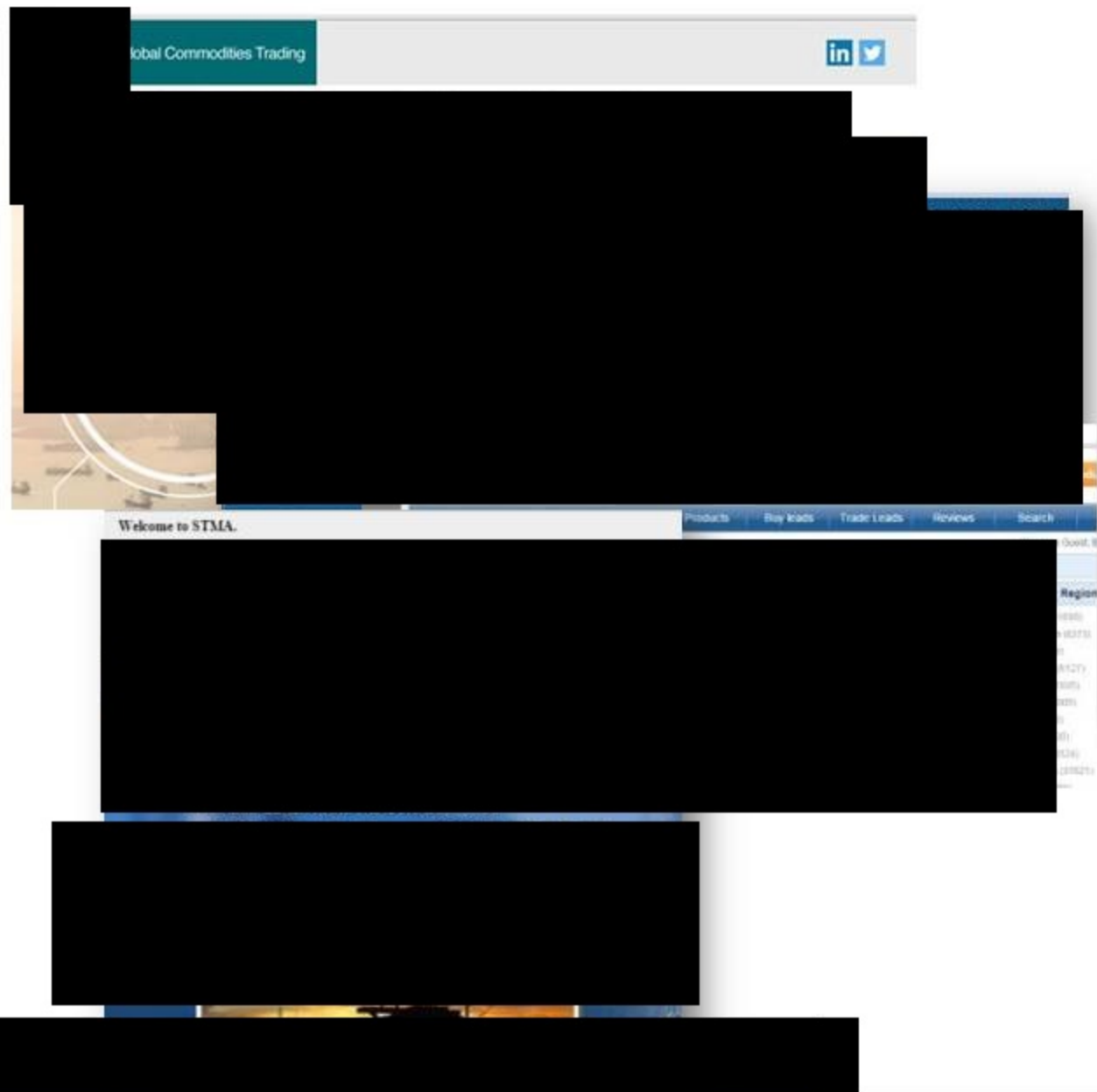
A SHIP HAS BEEN SIGHTED
in this quarter
ENGAGING IN THE UNLAWFUL ACT OF
SMUGGLING
whosoever can lay information
leading to the capture of this ship
or its crew
will receive a reward of
£500
From the Majesty's Government
This 29th day of October 1782

Commodities/ Front-running

(Medium Confidence:
50%+)

This TTP offers inside knowledge on large procurements of raw materials

- Targeting of procurement officers and purchasing platforms
- Targeting of traders and trading companies
- Manufacturers are large consumers of raw materials
- "Everything counts in large amounts"



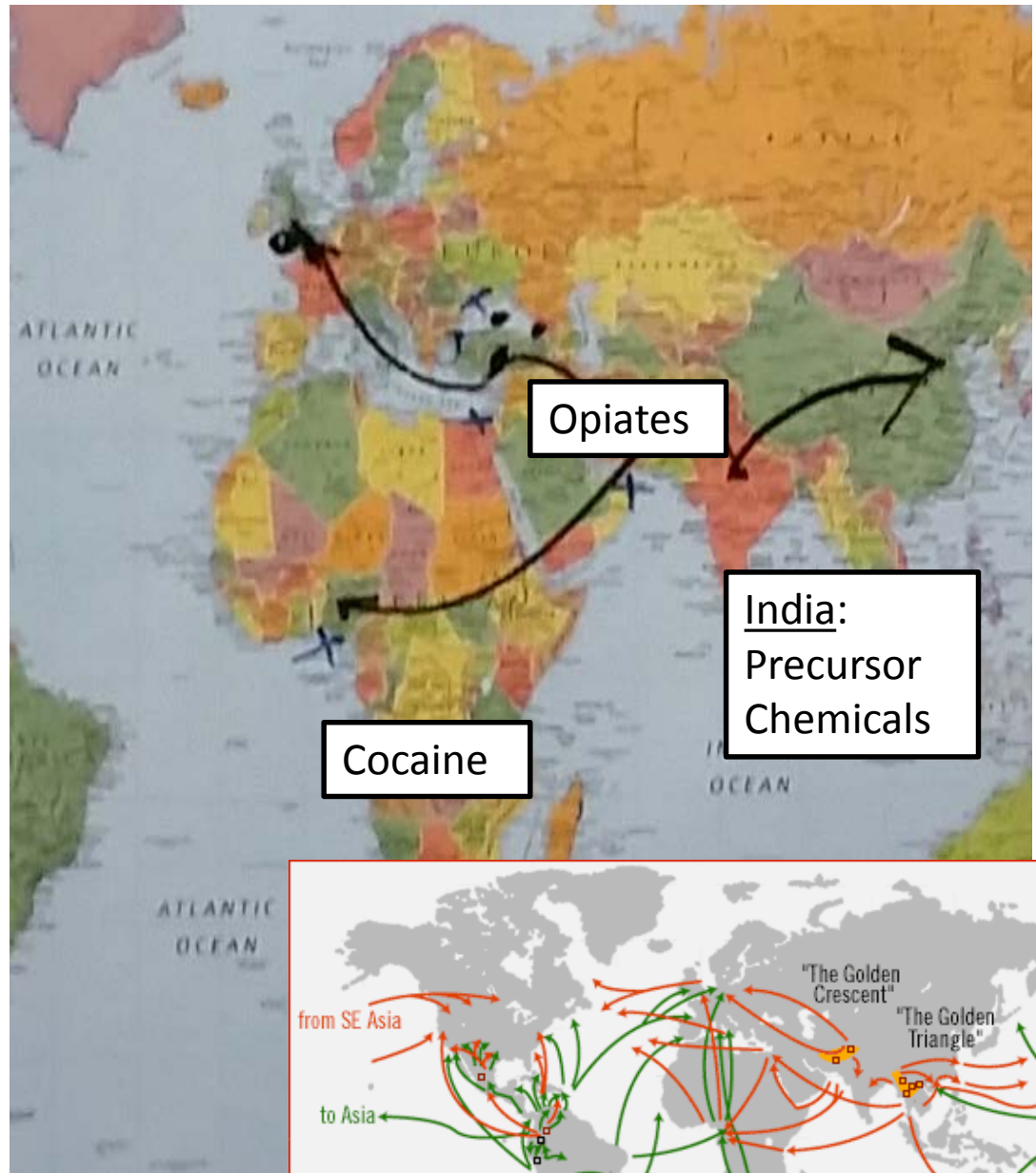
Drugs

(Medium – High

Confidence: 50-75%)

This TTP would allow full access/manipulation of documentation needed move drugs and transfer money.

- Antwerp attacks followed similar TTP
- One person has been identified using a similar TTP
- India and pharmaceutical nexus suggests the need to move drug precursor chemicals



Oil & Gas

(Low to Medium
Confidence: 25- 50%)

State sponsored or corporate espionage, monitoring shipping lanes, competitors.

From a geopolitical perspective, increased Oil & Gas distribution into the EU and Nordics is highly prized. Lower prices requires higher volume of sales to balance national budgets. Control of the Black Sea, Red Sea, Suez Canal become critical.

Other routes include LNG movement to S. Korea, Singapore.



We have also observed a Nigerian nexus but are unclear on involvement. Nigerian targeted victims include:



Real Estate, Investments, Construction, Loans

Low Confidence: This TTP may be used to smuggle low cost or sub-par building materials.

High Confidence: The Financial community is targeted in relation to Real Estate Holdings –holdings in the UAE and Iran.

While not believed to be the main operation, Nigerians are said to be one of the largest holders of the debt. Additionally, Nigerian scammers appear to be taking advantage of money movement.



More widespread? Air? Rail?

This TTP could easily have been spread to other shipping/logistics organizations.

While not witnessed directly, nearly all of the logistics companies and agents offer full service shipping, not just maritime. The possibility that this includes other modes of shipping/logistics is very real.

Access to customs, gac.com, one rail system (witnessed by Wapack Labs) could justify an assessment that this is more widespread than just maritime.



LESSONS LEARNED



Lessons learned

Strong passwords are meaningless without layered defenses.

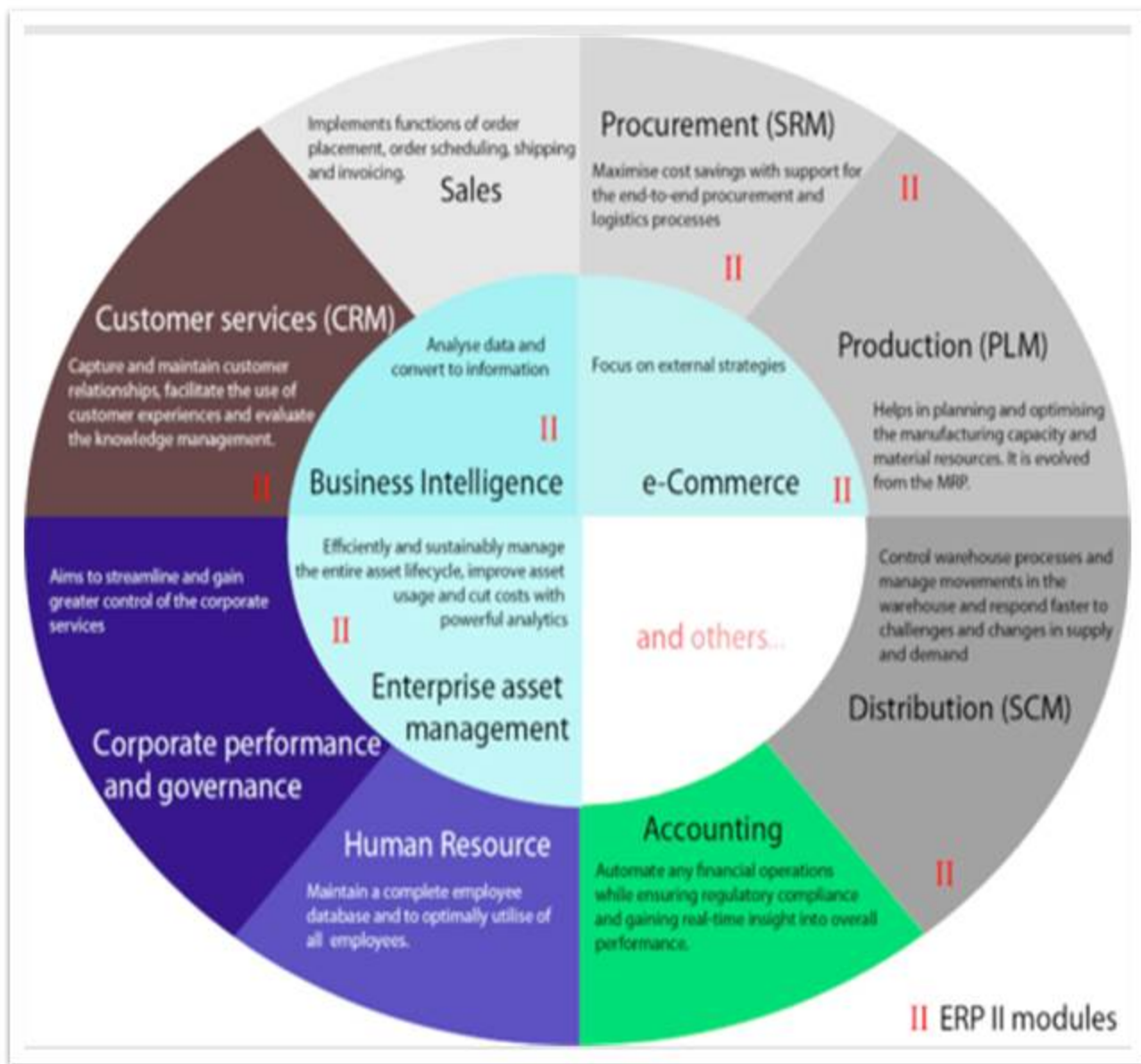
- Emails sent appeared legitimate
- Users clicked on what appeared to be a legitimate attachment
- Targets propagated exponentially once in, but only specific users were hit.
- Each of these targeted users had keyloggers installed

TYPE	PASSWORD
email	knj88445678
email	!qaz@wsx#edc\$rfrv
email	DxR28283Cf
email	leesk6266
email	sjdj2860
email	adam12345
email	2323@8Mj
email	vbnvbn
email	J6757ux5
email	J6757ux6
email	sukses50001
email	louis
email	2015ZEUS@#\$
email	9051945
email	Fktrctq165
email	Ray@neill1960
email	unilogops1
email	Kas@2014
email	Kk123456
email	kqEst@2014
email	1023RAZA1023RAZA

Lessons learned

ERP and other 'horizontal' systems are highly coveted targets

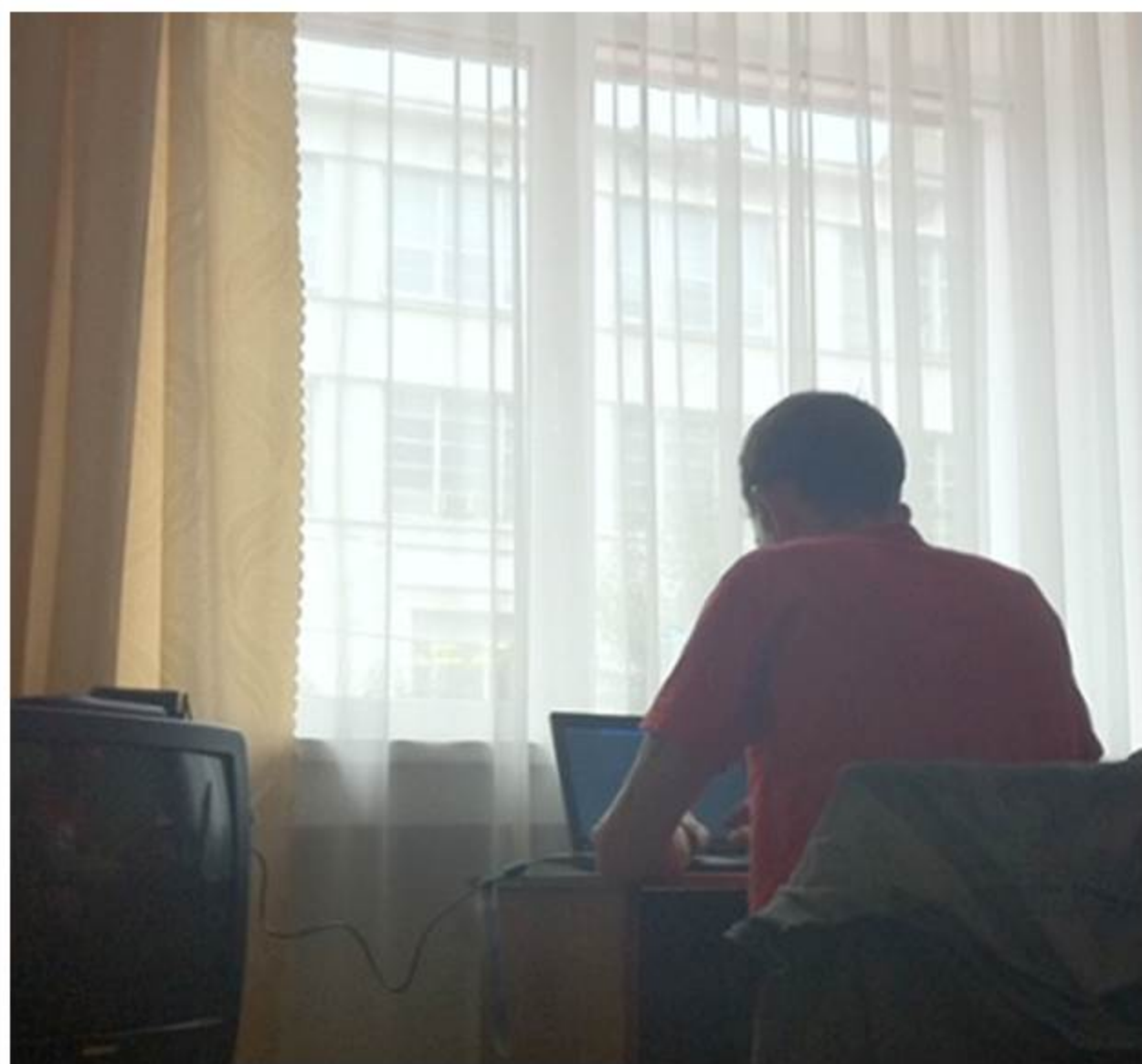
- Enterprise Resource Planning applications touch nearly everything
- One targeted computer offers access to many internal capabilities
- Because of its complexity, it is also the hardest system to protect.



Personnel (physical and information) Security matters.

Hotels are monitored for movement of ships personnel.

Many examples can be found online. As an example, in an unrelated event, hackers targeted senior executives travelling across Japan, China and Russia, using a keylogger to steal logins for Google, Facebook and Yahoo services. (SOURCE: theguardian.com, 10 Nov 2014)



Logistics and are easy (and highly prized) targets

Heavy cyber victim
count in Egypt suggests
full monitoring of all
activity in and out of the
Red Sea and Suez
Canal.

Others include routes
in/around the Black Sea,
Sea of Azov



The Easy Button..

Why “*hack the hard way*” ...

- Commercial malware works
 - Zero AV detection
 - CHEAP!
- Anonymous infrastructure providers
- Convincing social engineering
- “little fish” can easily catch big ones



Want more information

- Wapack Labs
 - Search “Daily Show” on cms.wapacklabs.com
- On Red Sky Alliance
 - Search Security Intelligence for “Daily Show”
 - Weekly Wolfpack - Introducing *Daily Show*
 - Wapack Labs 3.18.15 CTI&A The *Daily Show* Agenda.pdf



RED SKY®
ALLIANCE

