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"

Feb 21, 2015 - Ø6

Operating System Intel Recovery

CPU Name: ...

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...
220 mxi.main-hosting.com ESMTP [Main-hosting.com Mail System]
EHLO mxi.main-hosting.com
250-PIPELINING
250-SIZE 5728640
250-ETRN
250-AUTH PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-RIGHTS
250-DSN
250-AUTH login
235 2.7.0 Authentication successful
MAIL FROM:
250 2.1.0 OK
RCPT TO:
250 2.1.5 OK
DATA
354 End data with <CR><LF>,<CR><LF>
From: [REDACTED]
Date: [REDACTED]
Subject: Logger - Server Ran
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: quoted-printable
This is an email notifying you that BUSTER1-3FE4750D has run your Logger= and emails should be sent to you shortly and at interval choosen. 00=0D=0A
=0D=0ATime Logs will be delivered: True=0D=0AStealers Enabled: True=0D=0ATime Log will be delivered: Average 2 to 4 minutes=0D=0ATime Log will be delivered: Every 30 minutes=0D=0A=0D=0AInstalled Language: en-US=0D=0AInstalled Operating System: Microsoft- windows XP Professional=0D=0AInternal IP Address: 192.168.35.128=0D=0AExternal- IP Address: =0D=0AInstalled Anti-virus: =0D=0AInstalled Firewall: =
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?
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.
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.

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

* 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 SCHAAWEEEEEET target.... And these bad guys own it.
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:********]

You replied on 3/30/2015 10:47 AM.
Sent: Mon 3/30/2015 4:27 AM
To: [redacted]

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.

PLES 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.
Once in, nothing is off limits.

- Customs
- Manifests
- Financials
- Movements/schedules
- 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.
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.
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
Target Supply Chain

Go after the conferences

Supply Chain Mgmt Summit
Target Supply Chain

Go after procurement
Target Supply Chain

Go after the pipes:
Flow Metering
Target Supply Chain

Go after parts manufacturers:

General inquiry about your Bearing, Bearing Manufacturer
Target Supply Chain

Go after parts manufacturers:

Dear [Name],

Thanks for your inquiry. This is [Company Name], and 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

[Email Address]

[Logo] General Mechanical Components Bearing Manufacturer
Target Supply Chain

Go after parts manufacturers:
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
Exploiting others

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

Financial systems also targeted:
What do we think it is??

What do they want?
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**?
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 to 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

- Cocaine

- Opiates

India: 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

<table>
<thead>
<tr>
<th>TYPE</th>
<th>PASSWORD</th>
</tr>
</thead>
<tbody>
<tr>
<td>email</td>
<td>knj88445678</td>
</tr>
<tr>
<td>email</td>
<td>!qaz@wsx#edc$rfv</td>
</tr>
<tr>
<td>email</td>
<td>DxrR28283Cf</td>
</tr>
<tr>
<td>email</td>
<td>leesk6266</td>
</tr>
<tr>
<td>email</td>
<td>sjdj2860</td>
</tr>
<tr>
<td>email</td>
<td>adam12345</td>
</tr>
<tr>
<td>email</td>
<td>2323@8Mj</td>
</tr>
<tr>
<td>email</td>
<td>vbnvbn</td>
</tr>
<tr>
<td>email</td>
<td>J6757ux5</td>
</tr>
<tr>
<td>email</td>
<td>J6757ux6</td>
</tr>
<tr>
<td>email</td>
<td>sukses50001</td>
</tr>
<tr>
<td>email</td>
<td>louis</td>
</tr>
<tr>
<td>email</td>
<td>2015ZEUS@#$</td>
</tr>
<tr>
<td>email</td>
<td>9051945</td>
</tr>
<tr>
<td>email</td>
<td>Fktrctq165</td>
</tr>
<tr>
<td>email</td>
<td>Ray@neill1960</td>
</tr>
<tr>
<td>email</td>
<td>unilogops1</td>
</tr>
<tr>
<td>email</td>
<td>Kas@2014</td>
</tr>
<tr>
<td>email</td>
<td>Kk123456</td>
</tr>
<tr>
<td>email</td>
<td>kqEst@2014</td>
</tr>
<tr>
<td>email</td>
<td>1023RAZAM023RAZA</td>
</tr>
</tbody>
</table>
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