Using CTI to Profile and Defend Against the World’s Most Successful Email Scam

Matt Bromiley, Senior Managing Consultant
@mbromileyDFIR
The Life of a Speaker

- **August 13, 2016**

  Hey Matt! Stay tuned for lots more details in the next few weeks, but your talk has been accepted for the SANS CTI Summit 2017, January 31 & February 1 in Arlington,

- **November 9, 2016**

  Rick Holland
  @rickholland

  Super excited 2 have Cliff Stoll speak at CTI Summit. Cuckoo’s Egg was 1 of 1st books I read when starting in space
Using CTI to Profile and Defend Against the World’s Most Successful Email Scam

Matt Bromiley, Senior Consultant, Kroll

Reversing Threat Intelligence - Fun with Strings in Malware

Ronnie Tokazowski, Senior Malware Analyst, FlashPoint @iHeartMalware
Matt Bromiley

- Dallas, TX
- **Kroll** – Senior Managing Consultant, specialize in DFIR
- **SANS** – FOR508 Instructor, Secure the Human SME, Analyst
- **Hobbies**: Family, food, moar DFIR
Why does this matter?
Why does this matter?

January 2015
FBI alerts that thieves have stolen ~$215mil via email scamming

Victims: 2,126
Date Range: 2013-10-01 – 2014-12-01

$214mil
14 months
Why does this matter?

- **January 2015**
  - Date Range: 2013-10-01 – 2015-08-01
  - $585mil
  - 8 months

- **August 2015**
  - FBI alerts that thieves have stolen ~$800mil via email scamming
  - Victims: 8,179
  - Date Range: 2013-10-01 – 2015-08-01
Why does this matter?

January 2015

August 2015

$1.5bn
6 months

April 2016
FBI alerts that thieves have stolen ~$2.3bn via email scamming

Victims: 17,642
Date Range: 2013-10-01 – 2016-02-01

Why does this matter?

January 2015

August 2015

$1.5bn
6 months

April 2016
FBI alerts that thieves have stolen ~$2.3bn via email scamming

Victims: 17,642
Date Range: 2013-10-01 – 2016-02-01
Why does this matter?

January 2015

August 2015

April 2016

June 2016
FBI alerts that thieves have stolen ~$3.1bn via email scamming

Victims: 22,143
Date Range: 2013-10-01 – 2016-06-01

$800mil
2 months
Why does this matter?

January 2015  August 2015  April 2016  June 2016

Total (as of June 2016): $3.1bn
Daily Average: $3,168,634.59
Most Successful Month: $400mil
Business email scams
Business email scams

- Key ingredients:
  - “Smaller” business ($millions); although big business has fallen victim too
  - Incorrect domain
  - CEO name
  - CFO name
  - Some random person in accounting who doesn’t want to piss the boss off
Business email scams

- Transposed/incorrect domain
  MICROSOFT.COM
  M1CROSOFT.COM
  - M1CROSOFT.COM
  - MICROSOFT.COM

- This makes sense to the trained eye (aka this conference)
  *Letters for numbers; extra letters, transposed letters*
  *whiskey vs vvhiskey*
  *.info, .biz, .co, etc.*

- These are not trained eyes
Business email scams

- Where can one acquire these domains?
  - Small business-focused domain purchasing sites
  - Vistaprint, GoDaddy, etc.
  - In 90%+ of cases, Vistaprint is the purveyor

- VistaPrint will allow us to setup an account with *ONLY* a valid credit card
  - No charges; not even on a $0.01 card
  - 1 month free trial
  - Account setup INCLUDES Vistaprint webmail access
Business email scams

I just want to go home

acmeacb =/= acmeabc

now we're talking

not an actual forward
Defining the campaign
Defining the campaign

- Our “indicators”
  - We have a domain; any use?
  - We have a PDF; any use?
    - Title
    - MD5
    - Machine Information
    - Timestamps
    - Author
    - Bank info
Defining the campaign

- Let’s start with our PDF metadata

- Hrm..I wonder if ‘Bosslod’ has written any other documents
  - site:malwr.com “Bosslod”
  - 17 results!
### Defining the campaign

<table>
<thead>
<tr>
<th>File Details</th>
<th>File Details</th>
<th>File Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FILE NAME</strong></td>
<td>R&amp;R ENGRAVING WIRING INS.PDF</td>
<td>ORIENTAL WIRING INSTRUCTIONS.pdf</td>
</tr>
<tr>
<td><strong>FILE SIZE</strong></td>
<td>115052 bytes</td>
<td>167583 bytes</td>
</tr>
<tr>
<td><strong>FILE TYPE</strong></td>
<td>PDF document, version 1.5</td>
<td>PDF document, version 1.5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>File Details</th>
<th>File Details</th>
<th>File Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FILE NAME</strong></td>
<td>WITZKE WIRING INSTRUCTIONS_3_.pdf</td>
<td>RICHER WIRING INSTRUCTIONS.pdf</td>
</tr>
<tr>
<td><strong>FILE SIZE</strong></td>
<td>110366 bytes</td>
<td>111539 bytes</td>
</tr>
<tr>
<td><strong>FILE TYPE</strong></td>
<td>PDF document, version 1.5</td>
<td>PDF document, version 1.5</td>
</tr>
</tbody>
</table>
Defining the campaign

- Can we assume “Bosslod” works alone?
  - How about “WIRING INSTRUCTIONS”?

- site:malwr.com “WIRING INSTRUCTIONS”

- 55 results!

This can get distracting; remember to keep your focus.
Defining the campaign

- What did we find in 3 minutes of searching?

16 authors
29 documents
9 banks
Defining the campaign

- What did we find?
  - Additional authors:
    - Compaq
    - Houdini
    - Ray
    - Killz
    - Colvis Amue
    - Rizwan Khalid
Defining the campaign

- **What did we find?**
  - Banks they like to use:
    - HSBC
    - Bank of America
    - TD Canada Trust
    - Hang Seng Bank Limited
    - China Construction Bank
    - Texas Bank
    - Citizens Bank
Defining the campaign

- **What did we find?**
  - Some banks may only be used once
How do we get better?
How do we get better?

Phases of the Intrusion Kill Chain

One, two, skip a few

How do we get better?

- **The evidence:**
  - A text email with a benign PDF attached

- **What security device will prevent against this type of attack?**
  - Firewall?
  - IDS?
  - Anti-virus?
  - HIDS/HIPS?
  - NIDS/NIPS?
  - Email prevention
How Do We Get Better?
How Do We Get Better?

- Employee gets an email with transfer details
- Employee initiates transfer
- Money out the door
Using CTI to Profile and Defend Against the World’s Most Successful Email Scam

Matt Bromiley (@mbromleyDFIR)

How Do We Get Better?

Employee gets an email with transfer details

Employee initiates transfer

Money out the door

Choke Point
- Is this how we normally receive transfer requests?
- Is this who I normally receive requests from?

Choke Point
- Do we normally work with these banks?
- DO NOT XFER LIST
How do we get better?

Realize where your **front lines** are

Arm them with everything they need to be **successful**
How do we get better?

For the business:

- Do we normally work with this bank?
- Does this information match expected financial details?
- Does this vendor information look familiar?
How do we get better?

- **Sharing is caring**
  - Something as prolific as $400mil a month should not be “news”
  - Krebs should NOT be your IDS

- Admitting to being phished is not embarrassing; we are all being targeted
  - OK to admit increases/decreases and/or new campaigns
  - OK to share indicators
    - Indicators of value
How do we get better?

Everyone in this room already has a free threat intelligence source

- Your own environment!
- If you are protecting an organization, and not keeping notes on previous adversaries/incidents/malware/suspicions, something is wrong.
- We get better by learning cumulatively, not resetting the clock each day.
How do we get better?

**Tracking** your own threat intel can be really easy to start

- Notepad
- Notepad++
- Diary/Journal/ Pen + Paper

Include enough information that if you read this again in the future, you would remember the event fully

“Oh, I’ll remember this” works 0% of the time
How do we get better?

Level up your threat tracking expertise with... spreadsheets!

- Allows you to maintain relational data
- Naked eye can find patterns/inconsistencies
  - Wow, look at how many times \( x \) shows up in this data

<table>
<thead>
<tr>
<th>File Name</th>
<th>MD5</th>
<th>Bank</th>
<th>Bank Address</th>
<th>Bank Account #</th>
<th>Company</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORIENTAL WIRING INSTRUCTIONS.pdf</td>
<td>39f38a0b09e8edc1ed57911a7b97b75f</td>
<td>HSBC Bank</td>
<td>1 Queens Road, Hong Kong</td>
<td>$27021212588</td>
<td>Oriental Strong Limited</td>
<td>Bassloz</td>
</tr>
<tr>
<td>YOUPONG WIRING INSTRUCTIONS.pdf</td>
<td>3783499372f5c95a7a5b7e8d5f532588</td>
<td>Hang Seng Bank Limited</td>
<td>85 Des Voeux Road, Central Hong Kong</td>
<td>384-2390918-882</td>
<td>Youpong Electronic Technology Co. Limited</td>
<td>Kiltz</td>
</tr>
<tr>
<td>JNIGHTLIGHT LIMITED WIRING INSTRUCTIONS.pdf</td>
<td>3c7e6f5fe59e1443f13de985c233bba</td>
<td>HSBC Bank</td>
<td>1 Queens Road, Hong Kong</td>
<td>819-577974-836 Jnighlight Limited</td>
<td>Ray</td>
<td></td>
</tr>
<tr>
<td>JNIGHTOUT LIMITED WIRING INSTRUCTIONS.pdf</td>
<td>577e5569e9b063c6ac3817d7e82568a</td>
<td>HSBC Bank</td>
<td>1 Queens Road, Hong Kong</td>
<td>819-577974-836 Jnighlight Limited</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>HONG KONG WEALTH INC LIMITED WIRING INSTRUCTIONS.pdf</td>
<td>db57e5113d4fe6cc8c43b79505ab35d</td>
<td>HSBC (HK) Limited</td>
<td>1 Queens Road, Hong Kong</td>
<td>023-52001-836 Hong Kong Wealth Inc Limited</td>
<td>Rizwan Khalid</td>
<td></td>
</tr>
<tr>
<td>FAR EAST WIRING INSTRUCTIONS.pdf</td>
<td>ddf2f27b3d04c9ed65ac984b289f19d12</td>
<td>HSBC Bank</td>
<td>1 Queens Road, Hong Kong</td>
<td>652-397936-836 Far East Nation Limited</td>
<td>Kiltz</td>
<td></td>
</tr>
<tr>
<td>WITZKE WIRING INSTRUCTIONS_u.pdf</td>
<td>29dc5524e3c407215da938e2e1c461</td>
<td>TD Canada Trust</td>
<td>7000 E Hwy 89, Prescott Valley, Arizona, 85814</td>
<td>8279148106</td>
<td>RC Contracting Specialists LLC</td>
<td>Houdini</td>
</tr>
<tr>
<td>RT CONTRACTING SPECIALISTS LLC WIRING INSTRUCTIONS.pdf</td>
<td>5543527f3f67d537145b7c578a5d7c5d</td>
<td>JP Morgan Chase Bank</td>
<td>7000 E Hwy 89, Prescott Valley, Arizona, 85814</td>
<td>8279148106</td>
<td>RT Contracting Specialists LLC</td>
<td>Houdini</td>
</tr>
<tr>
<td>CPL WIRING INSTRUCTIONS.pdf</td>
<td>fb8e7c5d59301589e2e190629e2e9980b</td>
<td>HSBC Bank</td>
<td>1 Queens Road, Hong Kong</td>
<td>642-036881-836 China Plus Logistics Ltd</td>
<td>Bassloz</td>
<td></td>
</tr>
<tr>
<td>WIRING INSTRUCTIONS.pdf</td>
<td>23a64d3d40e22ae79a84404901de1e3</td>
<td>ING Bank</td>
<td>LA, Norwalk 01229, Warsaw, Poland</td>
<td>642-036881-836 China Plus Logistics Ltd</td>
<td>Metropolia Boutique</td>
<td></td>
</tr>
</tbody>
</table>
How do we get better?

**Level up** again and look at *free* threat tracking tools/frameworks
It Does Get Better
It Does Get Better

- Let’s dig into one attacker: Colvis Amue

**File Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>FILE NAME</td>
<td>SYLONDIA ROWLAND WIRE INSTRUCTIONS 2.pdf</td>
</tr>
<tr>
<td>FILE SIZE</td>
<td>19169 bytes</td>
</tr>
<tr>
<td>FILE TYPE</td>
<td>PDF document, version 1.3</td>
</tr>
<tr>
<td>MD5</td>
<td>f7dc0a29c71e7e13884504b60c42d10b</td>
</tr>
</tbody>
</table>

Colvis Amue

@amuecolvis

coming soon

Joined November 2011
It Does Get Better

DALLAS

September 24, 2015

Federal Grand Jury Indicts Nigerian Man for Role in Business E-Mail Compromise Scheme That Caused Attempted $1.3 Million Loss to U.S. Companies

DALLAS—A Nigerian citizen in the U.S. on a student visa has been charged in a conspiracy to commit wire fraud stemming from his role in what has become known as the Nigerian 4-1-9 scam. The charging instrument was announced today by John Parker, the U.S. Attorney for the Northern District of Texas.

Amechi Colvis Amuegbunam, 28, of Lagos, Nigeria, was arrested late last month in the Northern District of Texas, when he entered the U.S. in Baltimore, Maryland. He appeared in federal court in the District of Maryland on August 25, 2015, and was detained. It is expected he will be transferred to the Northern District of Texas later this week.
References
References

- Ronnie Tokazowski’s research on using VistaPrint for phishing abuse: [http://phishme.com/vistaprint-abuse-free-phish-for-all/](http://phishme.com/vistaprint-abuse-free-phish-for-all/)

- FBI Alerts on BEC
  - August 2015 - [https://www.ic3.gov/media/2015/150827-1.aspx](https://www.ic3.gov/media/2015/150827-1.aspx)


THANK YOU!