RootCon

09/21-22/17 Philippines

I haz legal disclaimer
How to secure Banks & Enterprises (From someone who robs banks & enterprises)
Who am I?

Twitter: @JaysonStreet

INFO: http://JaysonEStreet.com

Email: jstreet@sphereny.com
We are terrible at risk management!

<table>
<thead>
<tr>
<th>Case Type</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagnosed in the U.S.</td>
<td>4</td>
</tr>
<tr>
<td>Evacuated to U.S. from other countries</td>
<td>7</td>
</tr>
<tr>
<td>U.S. Deaths</td>
<td>2</td>
</tr>
</tbody>
</table>

11 U.S. Cases

[Image of world map with Ebola outbreak locations and CNN news segment]
We are terrible at risk management!

Number of deaths for leading causes of death:

- Heart disease: 614,348
- Cancer: 591,699
- Chronic lower respiratory diseases: 147,101
- Accidents (unintentional injuries): 136,053
- Stroke (cerebrovascular diseases): 133,103
- Alzheimer’s disease: 93,541
- Diabetes: 76,488
- Influenza and Pneumonia: 55,227
- Nephritis, nephrotic syndrome and nephrosis: 48,146
- Intentional self-harm (suicide): 42,773

Source: Health, United States, 2015, Table 12 (Data are for 2014)
We are terrible at risk management!
We are terrible at risk management!
We are terrible at risk management!
Who do you think poses the most danger to businesses?
Who do you think poses the most danger to businesses?
Who do you think poses the most danger to businesses?
Being a TARGET of cyber-crime can be catastrophic!

Following Target's data breach in December 2013, the fallout for the company continues to grow.

**$236 million**
Target's total breach expenses

$236mm total expenses - $90mm insurance receivable = $146mm net expenses

- **40 million** credit and debit cards compromised
- **70 million** customer details compromised

**140+ lawsuits**
were filed against Target as a result of the breach

110 consumer + 30 banking/credit union + shareholder cases
Your greatest asset is your greatest weakness

Majority of workers blindly open email attachments

The vast majority (82 percent) of users open email attachments if they appear to be from a known contact, despite the prevalence of well-known sophisticated social engineering attacks, according to Glasswall. Of these respondents, 44 percent open these email attachments consistently every time they receive one, leaving organizations vulnerable to data breaches sourced to malicious attachments.

- Only 30% of office-workers believe their employer has been subjected to cyber attack
- 75% receive suspicious emails
- 62% don’t check email attachments from unknown sources
Eenie meenie miney mo
Demo of an attack!
Demo of an attack!
Demo of an attack!
Demo of an attack!
Demo of an attack!
Demo of an attack!
Demo of an attack!
Demo of an attack!
Demo of an attack!
Demo of an attack!
Demo of an attack!
Demo of an attack!
Demo of an attack!
Demo of an attack!
Demo of an attack!
Demo of an attack!
Demo of an attack!
Demo of an attack!
Demo of an attack!

Want to directly email someone at Banco de Oro but don’t know their address? Maybe you just had an interview and didn’t get a business card for a follow-up? Or you’ve got a name and nothing more from LinkedIn? Don’t sweat it, we’ve got you covered.
Demo of an attack!

<table>
<thead>
<tr>
<th>Email</th>
<th>Score</th>
<th>Date Found</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:sotto.aster@bdo.com.ph">sotto.aster@bdo.com.ph</a></td>
<td>0</td>
<td>Oct 2013</td>
</tr>
<tr>
<td><a href="mailto:lsr@bdo.com.ph">lsr@bdo.com.ph</a></td>
<td>0</td>
<td>May 2014</td>
</tr>
<tr>
<td><a href="mailto:wong.gigi@bdo.com.ph">wong.gigi@bdo.com.ph</a></td>
<td>0</td>
<td>Jun 2015</td>
</tr>
<tr>
<td><a href="mailto:sarahan.abigail@bdo.com.ph">sarahan.abigail@bdo.com.ph</a></td>
<td>0</td>
<td>Jun 2015</td>
</tr>
<tr>
<td><a href="mailto:santos.rachael@bdo.com.ph">santos.rachael@bdo.com.ph</a></td>
<td>0</td>
<td>Nov 2013</td>
</tr>
<tr>
<td>corp.americanexpress.com/gcs/intl/philippines/corpora</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:pjj@bdo.com.ph">pjj@bdo.com.ph</a></td>
<td>0</td>
<td>Oct 2013</td>
</tr>
<tr>
<td><a href="mailto:calixtro.elgenemark@bdo.com.ph">calixtro.elgenemark@bdo.com.ph</a></td>
<td>0</td>
<td>Oct 2013</td>
</tr>
<tr>
<td><a href="mailto:jmn@bdo.com.ph">jmn@bdo.com.ph</a></td>
<td>0</td>
<td>May 2014</td>
</tr>
<tr>
<td><a href="mailto:madduma.jovy@bdo.com.ph">madduma.jovy@bdo.com.ph</a></td>
<td>0</td>
<td>Jun 2015</td>
</tr>
<tr>
<td><a href="mailto:gamboa.georgiana@bdo.com.ph">gamboa.georgiana@bdo.com.ph</a></td>
<td>0</td>
<td>Jun 2015</td>
</tr>
</tbody>
</table>
| basquena.cherry@bdo.com.ph | 0     | Aug 2013    | bakersforum.123guestbook.com }
Remember the kittens!!
Demo of an attack!

Little seeds of terror: children exploited as warriors in Philippines
Asia Times - Sep 14, 2017
Little seeds of terror: children exploited as warriors in Philippines ... a mother cries not only in Marawi City in the Philippines but in the entire ...

US Deploys New Surveillance Drone to Philippines for Terror Fight
The Diplomat - Sep 12, 2017
This week, the United States announced that it had begun deploying a more capable unmanned aircraft system in the Philippines to help its ...
5 terrorists killed in Marawi clash
International - Inquirer.net - Sep 12, 2017
The Eagle will fly
International - Philippine Star - Sep 11, 2017

Australia lists Islamic State East Asia as official terrorist organisation ...
NEWS.com.au - Sep 7, 2017
Australia bans Philippine terror group
International - SBS - Sep 7, 2017

Terror Fight, Rebuilding Marawi to Cost Philippines $1.1 Billion
Bloomberg - Sep 6, 2017
Rebuilding the besieged Philippine city of Marawi could cost about 56 billion pesos ($1.1 billion), according to Defense Secretary Delfin ...

Drug war, Maute terrorists 'rising' risks for Philippines — Moody's
Rappler - Sep 16, 2017
MANILA, Philippines — President Rodrigo Duterte's deadly drug war and the armed Maute rebellion pose 'rising' risks to the Philippine ...
Marawi terrorist starting to target bank branches including ours!!

hello Enna,

I hope you are doing well. I read the news story [http://badlink.com](http://badlink.com) about the horrible terrorist declaring that they would start attacking bank branches including ours! I'm afraid that they may also target our job fair on the 23rd. It has me very frightened and I wanted to make sure you were aware since your branch may be targeted!!

Take Care,
Anne Sanchez

(Sent from a mobile device)

&lt;Lets all imagine that this is written in Filipino&gt;
Uptick in social media-based attacks

By Admine Moyo, ITWeb's senior news journalist.
Johannesburg, 31 Oct 2016

Cyber criminals are taking advantage of social media networks to spread malware and steal money from unsuspecting users.

This is one of the biggest findings in the Easy Solutions 2016 Fraud Boat report released on Friday. The report identifies the most recent and sophisticated cyber attacks impacting companies, financial institutions and consumers across the globe.

The digital revolution, led by users who are always connected to the Internet through their smartphones, offers boundless financial opportunities for banks and businesses, says Easy Solutions. However, the security solutions vendor notes the digital revolution is also attracting the attention of cyber criminals for the same reasons.

There are over 80 million fake profiles on Facebook, Twitter and Instagram alone, and a large portion are used to launch social media attacks, the vendor notes.

Facebook announced it had surpassed a billion-and-a-half users at the end of last year; the report notes. Its user base would be the largest nation in the world if it were a country, even bigger than China.

Facebook estimates 2% of its 1.6 billion users are fake, which translates into more than 30 million counterfeit accounts. Twitter estimates about 5% of its profiles are fake, while Instagram approximated this number at around 8%.
So what can we do?

Be One With The Attacker
OSINT Framework

Notes:
OSINT framework is focused on gathering information from free tools or resources. The intention is to help people find OSINT resources that return free information. Some of the sites included may require registration or offer more data for $36, but you should be able to get ahead a portion of the available information for no cost.
Attacker
Recon
Search results for: bdo bank

About 46 results (0.47 seconds)

<?xml version="1.0" encoding="utf-8"?> <soap:Envelope xmlns="..." https://pastebin.com/b33DBsia5d

Mar 7, 2016 ... <remarks>Use your BDO Retail Internet Banking (RIB) account to make a ... <url> https://gw.dragonpay.ph/Bank/OfflineGateway.aspx?... procid="..."

Cis Banks SLAMCI 01929518CF01 afsabad25 Sqvtrqapapis0925 + ... https://pastebin.com/Ssbjch4s


Kantor Polski Terminals iPay.by TBT account Micropayment Berliner ... https://pastebin.com/2mWZUQ2t


Hi. Sorry for my delayed reply. Lot of VIP slots were filled up and ... pastebin.com/6tgDJIpqm

Nov 29, 2016 ... the country location is Philippines. and then admin own several bank accounts from the following bank: --- BDO (Banco de Oro Universal Bank).

BDO tips - Pastebin.com https://pastebin.com/VVT888eY

May 24, 2017 ... When using contribution in cities to number worker race or bank race not all language are combinations have an equal return on
Demo of an attack!

45. 4183580119151100 (BANCO DE ORO VISA CLASSIC)
46. Expiration: 04/2018 Cvv: 214
47. Pamela Bianca O. Nollora
48. Phase 2, Block 12, Canyon Ranch, Brgy. Lantic
49. Carmona, Cavite City 4116
50. Philippines
51. https://www.facebook.com/pamelamae.nollora
Attacker
Recon
Attacker Recon
Attacker
Recon
Attack Recon

Country: Philippines
Organization: R8gcDZ13052460924fontana Resort And Country Club
ISP: Philippine Long Distance Telephone
Last Update: 2017-09-15T21:07:18.304640
ASN: AS9299
C
Schenker Philippines, Inc.
Cisco 881-K9 Series router
Deployed at PH0120-Clark
10.213.226.128/27

User Access Verification
Password:
The Road Map of an Attack

Cisco IOS http config

HTTP/1.1 401 Unauthorized
Date: Sat, 02 Sep 2017 15:50:55 GMT
Server: cisco-IOS
Connection: close
Accept-Ranges: none
WWW-Authenticate: Basic realm="level_15 or view_access"
Demo of an attack!
Demo of an attack!

Equifax had 'admin' as login and password in Argentina

13 September 2017 | Technology
Attacker

Recon
current status: 1.17 million host scanned 33,468 found infected.
Blue Team in a box
If All Else Fails!
1. Security is a cost center until the lack of it cost you everything!

2. Show your employees that you take security seriously and then they will!

3. Patch – Passwords – Public WIFI – Paranoia (a healthy amount) ;-)
WPAD
Make a null route (to 127.0.0.1 IPV4 ::1 IPV6) DNS entry for WPAD
Make a null route (to ::1 IPV6) DNS entry for WPAD
Make a null route (to ::1 IPV6) DNS entry for WPAD

Disable NetBios resolution domain wide.
Evil Canary
1. Create user called “DomainAdmin_TMP”
2. Put password in the description.
3. Add to Domain Admins Group!
4. Under Logon Hours set to ZERO!
5. Set an alert ANY time that account tries to logon!
Evil Canary
Make a public share called “Password Audit 2015” inside create a EXLS file about 4 MB but “Everyone: Deny” permission.
Rob Fuller

Twitter @mubix

Full video located here....
https://www.youtube.com/watch?v=VqcDjPUXPIw
Create A Submarine Not A Wall

.....NOT THIS!

THIS......
Create A Submarine
Not A Wall

THE PERCENTAGE OF UNSEGMENTED CORPORATE NETWORKS...

IS TOO DARN HIGH!!
1. PATCH! PATCH!! PATCH!!! PATCH!!!! PATCH!!!!! PATCH!!!!!!

A Few Last Tricks & Traps

ALSO PATCH!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
A Few Last Tricks & Traps

1. PATCH! PATCH!! PATCH!!! PATCH!!!! PATCH!!!!! PATCH!!!!!

ALSO PATCH!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
A Few Last Tricks & Traps

1. PATCH! PATCH!! PATCH!!! PATCH!!!! PATCH!!!!! PATCH!!!!!!

Also PATCH!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
A Few
Last
Tricks &
Traps

2. 1X1 pixel gif going to a link that alerts you.

It’s there I promise!!!
3. User agent strings should also alert you.

Alexibot Aqua_Products b2w/0.1 BackDoorBot/1.0 Black Hole BlowFish/1.0 Bookmark search tool BotALot BuiltBotTough Bullseye/1.0 BunnySlippers Cegbeieh CheeseBot CherryPicker CherryPickerElite/1.0 CherryPickerSE/1.0 CopernicCopyRightCheck cosmos Crescent Crescent Internet ToolPak HTTP OLE Control v.1.0 DittoSpyder dumbot EmailCollector EmailSiphon EmailWolf Enterprise_Search Enterprise_Search/1.0 EroCrawler es ExtractorPro FairAd Client Flaming AttackBot Foobot Gaisbot GetRight/4.2 grub grub-client Harvest/1.5 Hatena Antenna hloader httplib humanlinks ia_archiver ia_archiver/1.6 InfoNaviRobot Iron33/1.0.2 JennyBot Kenjin Spider Keyword Density/0.9 larbin LexiBot libWeb/clsHTTP libWeb/clsHTTPUser-agent: asterias LinextractorPro LinkScan/8.1a Unix LinkScan/8.1a Unix User-agent: Kenjin Spider LinkWalker LNSpiderguy lwp-trivial lwp-trivial/1.34 Mata Hari Microsoft URL Control Microsoft URL Control - 5.01.4511 Microsoft URL Control - 6.00.8169 MIIxpc MIIxpc/4.2 Mister PiX moget moget/2.1 Morfeus Mozilla/4.0 (compatible; BullsEye; Windows 95) Mozilla/4.0 (compatible; MSIE 4.0; Windows 9 Mozilla/4.0 (compatible; MSIE 4.0; Windows 95)
A Few Last Tricks & Traps

4. Control the countries that can see you if you can. http://ipinfo.io/countries
5. Own as many domains similar to yours as possible (Because someone will!)

A Few Last Tricks & Traps
6. You have to click links at some point or download attachments just be cautious!
7. Web Developers should be building good code!!!
(Which then makes it more secure)
LAST but NOT Least!!!!

Create teachable moments for your employees before a real attacker does!!!
A Few Last Tricks & Traps
A Few Last Tricks & Traps
A Few Last Tricks & Traps

ROOTCON 11 will be held in Taal Vista Hotel in Tagaytay on September 21-22, 2017.
A Few Last Tricks & Traps

ROOTCON 11 will be held in Taal Vista Hotel in Tagaytay on September 21-22, 2017.

REGISTRATION
CLOSING

CALL FOR SPONSORS
CLOSING

CALL FOR TRAININGS
CLOSING

CALL FOR PAPERS
CLOSING

BLACK CARD
CLOSING
A Few Last Tricks & Traps

http://rootcon.org.cgi-bin.email/confirmation/

OMG!! YOU CLICKED THE LINK DIDN'T YOU!?!?!?!!?
Remember your employees are an asset not a liability!!
Now let’s learn from others

Discussion and Questions????

Or several minutes of uncomfortable silence it’s your choice.

This concludes my presentation Thank You!!!
My own lil page!
http://JaysonEStreet.com

Interested in me being your teachable moment.
jstreet@sphereny.com

Twitter @jaysonstreet
WeChat jaysonstreet
Also on LinkedIn too! ;-)

Thanks to John of SHODAN, Mubix, IT-Defense Roundtable 2016, April Wright, Adriel of Netragard and all my ‘victims’ for not suing! ;-)