RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking

SESSION ID: CLE-F04

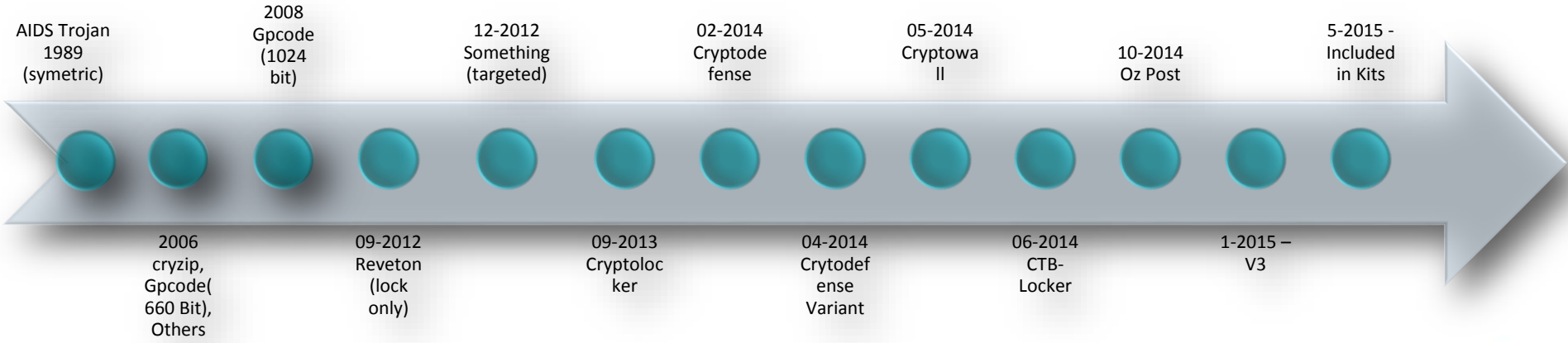
Ransomware

A good driver for backups

Mark Hofman

Chief Technology Officer
Shearwater / Phriendly Phishing
@markhofman

A little bit of history



Some earlier attempts

Some sad stories

Home > News

Cyber raiders [illegible] $3000

On Monday, The ABC had to suspend programming out of Sydney, Australia and move broadcasting to Melbourne after their network was targeted by Ransomware. The malware prevented normal operations, resulting in ABC News 24 going off air for just over 30 minutes.

In a statement, ABC said:

"There was an IT security issue this morning which affected some of the ABC's broadcasting systems and created technical difficulties for ABC News 24. As a result we broadcast stand-by programming from 9.30am before resuming live news broadcasts from Melbourne at 10am. We are now operating normally."

[illegible] their files, rather [illegible] day of Queensland's fraud

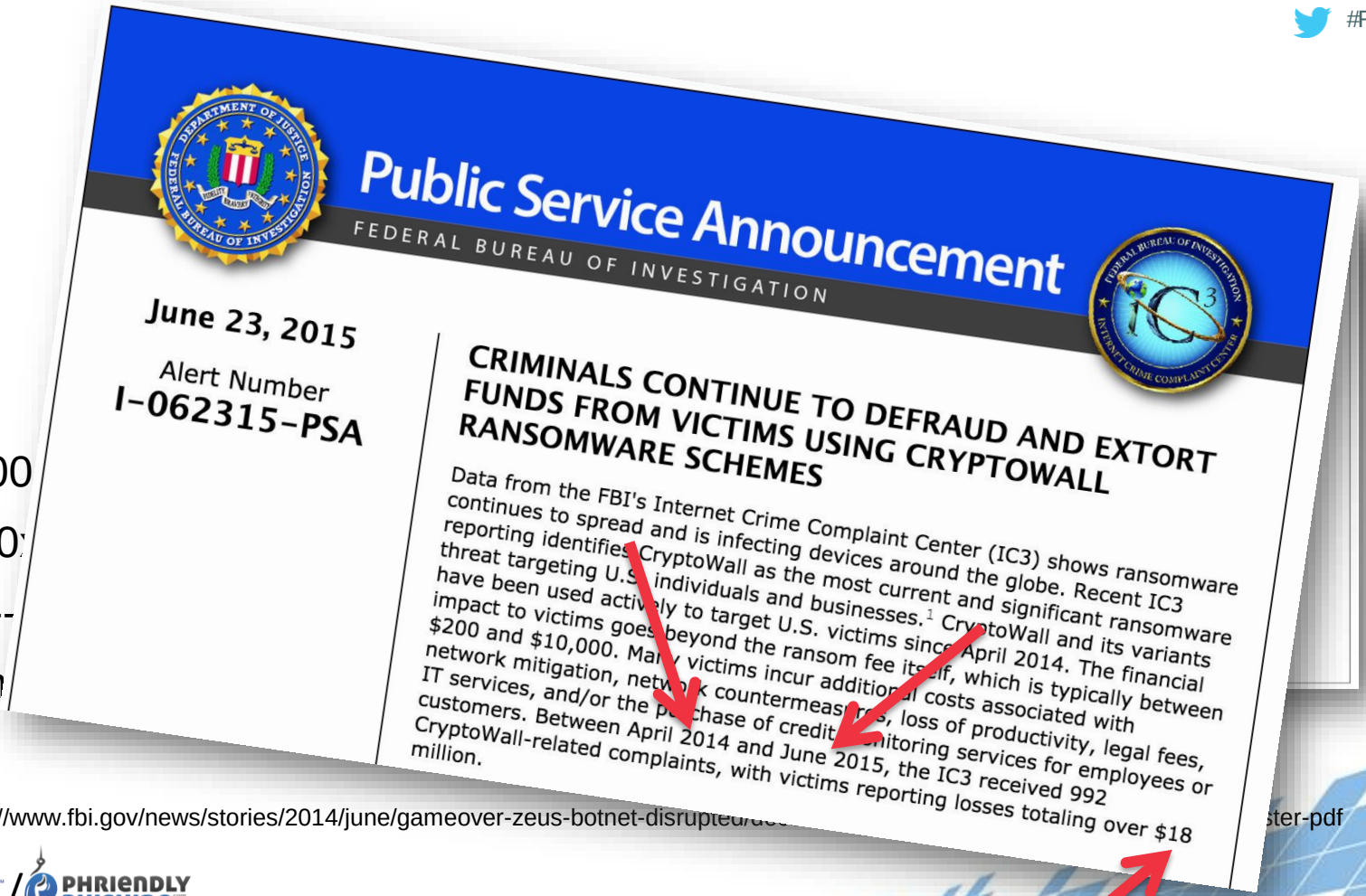
[illegible] etched and probably serious breach of law [illegible] to a local news report, this is exactly what the police [illegible] Massachusetts decided to do when "several images and word [illegible] were found to have been encrypted by the malware.

Value

~1,000,000

€500

A big num



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

June 23, 2015

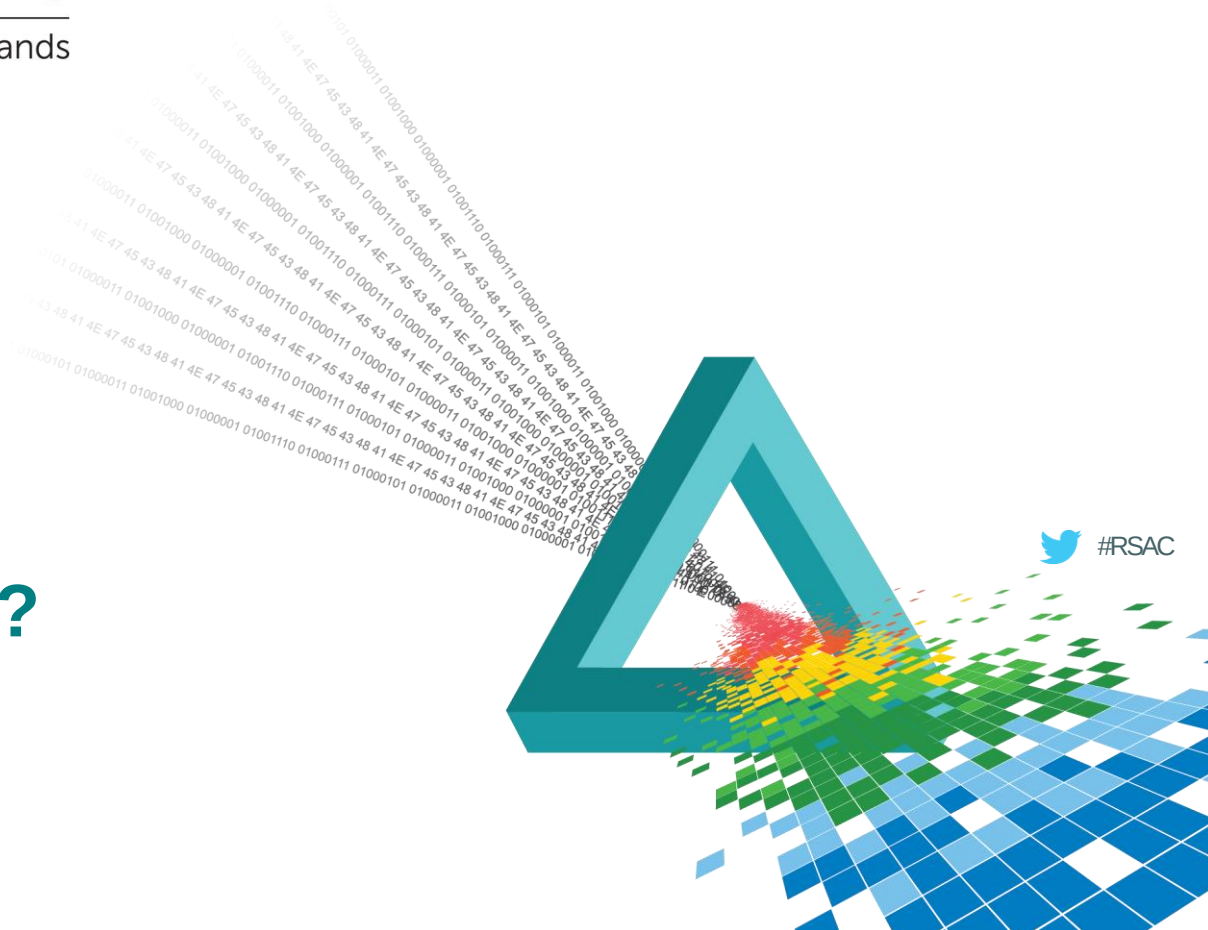
Alert Number
I-062315-PSA

CRIMINALS CONTINUE TO DEFRAUD AND EXTORT FUNDS FROM VICTIMS USING CRYPTOWALL RANSOMWARE SCHEMES

Data from the FBI's Internet Crime Complaint Center (IC3) shows ransomware continues to spread and is infecting devices around the globe. Recent IC3 reporting identifies CryptoWall as the most current and significant ransomware threat targeting U.S. individuals and businesses.[1] CryptoWall and its variants have been used actively to target U.S. victims since April 2014. The financial impact to victims goes beyond the ransom fee itself, which is typically between $200 and $10,000. Many victims incur additional costs associated with network mitigation, network countermeasures, loss of productivity, legal fees, IT services, and/or the purchase of credit monitoring services for employees or customers. Between April 2014 and June 2015, the IC3 received 992 CryptoWall-related complaints, with victims reporting losses totaling over $18 million.

http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted/...ster-pdf

How does it work?



Anatomy of an attack (Reminder)

- ~~Reconnaissance~~
- Delivery/Infiltration
- Code execution
- ~~Network Propagation~~
- ~~Data Exfiltration~~

Not everything needed

If you prefer APT Cyber Kill Chain®

- ~~Reconnaissance~~
- Weaponization
- Delivery
- Code execution
- ~~Installation~~
- Command & Control
- ~~Actions on Objectives~~

Needed infrastructure

- A computer (anyone's is fine)
- A server (anyone's is fine)
- Tor set up
- Account for deposits
  - Bitcoin, kashu

Using Tor to hide

All files including videos, photos and documents on your computer are encrypted by CryptoDefense Software.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet;
The server will destroy the key after a month. After that, nobody and never will be able to restore files.

In order to decrypt the files, open your personal page on the site **https://rj2bocejarqnpuhm.browsetor.com/346h** and follow the instructions.

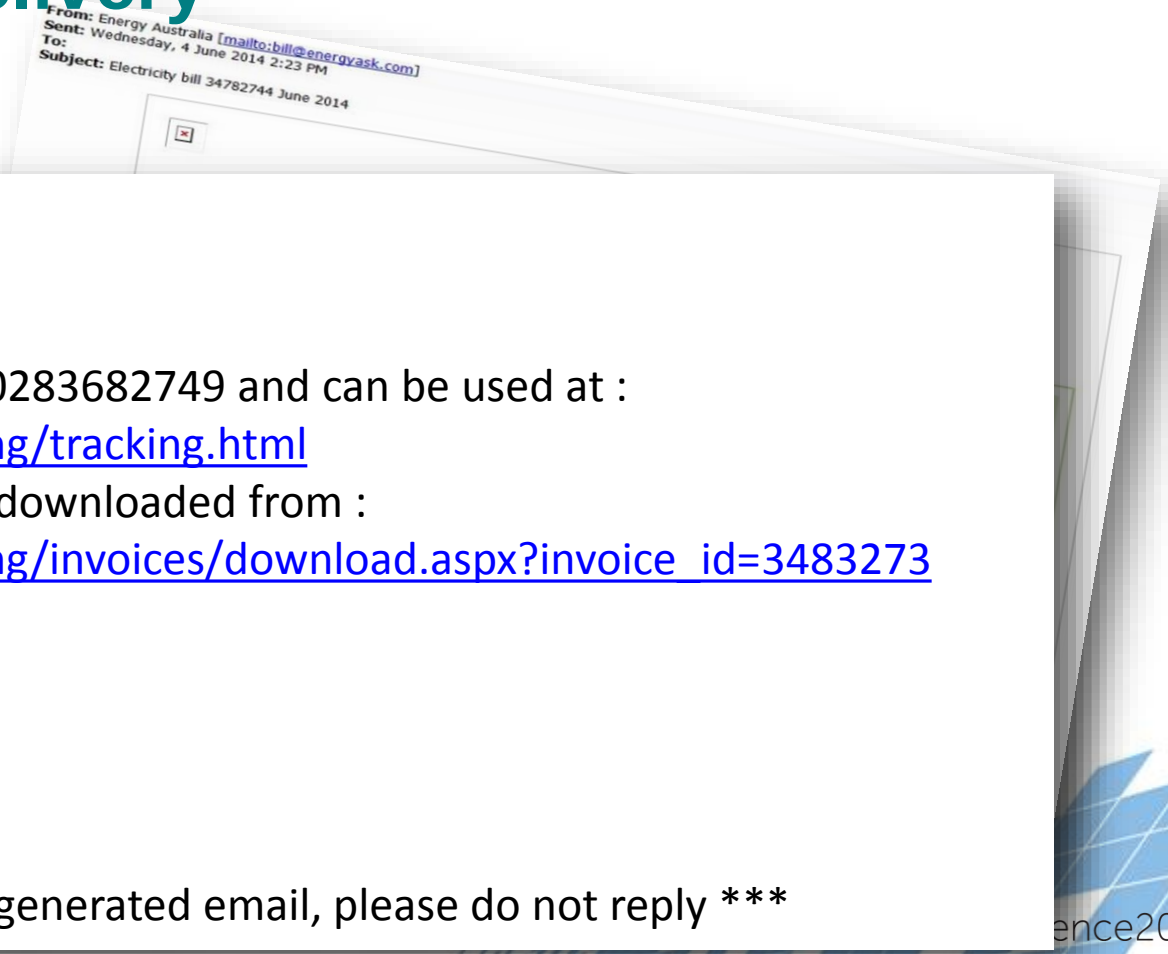
If https://rj2bocejarqnpuhm.browsetor.com/346h is not opening, please follow the steps below:

1. You must download and install this browser http://www.torproject.org/projects/torbrowser.html.en
2. After installation, run the browser and enter the address: **rj2bocejarqnpuhm.onion/346h**
3. Follow the instructions on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.

IMPORTANT INFORMATION:

Your Personal PAGE:
https://rj2bocejarqnpuhm.browsetor.com/346h
Your Personal PAGE(using TorBrowser):
rj2bocejarqnpuhm.onion/346h
Your Personal CODE(if you open site directly): **346h**

It starts here - Delivery



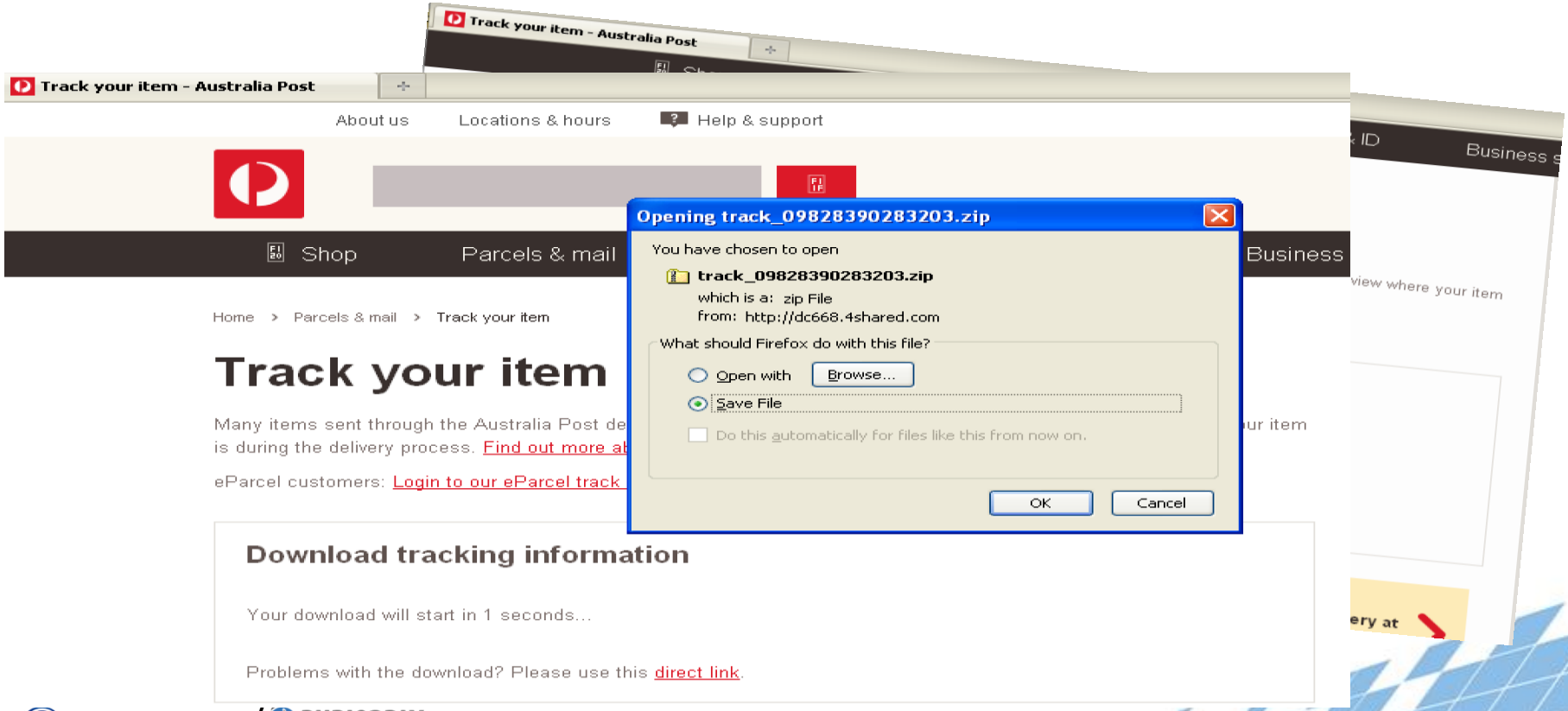
Dear client

Your package has arrived.
The tracking# is : 1Z45AR990283682749 and can be used at :
http://www.ups.com/tracking/tracking.html
The shipping invoice can be downloaded from :
http://www.ups.com/tracking/invoices/download.aspx?invoice_id=3483273

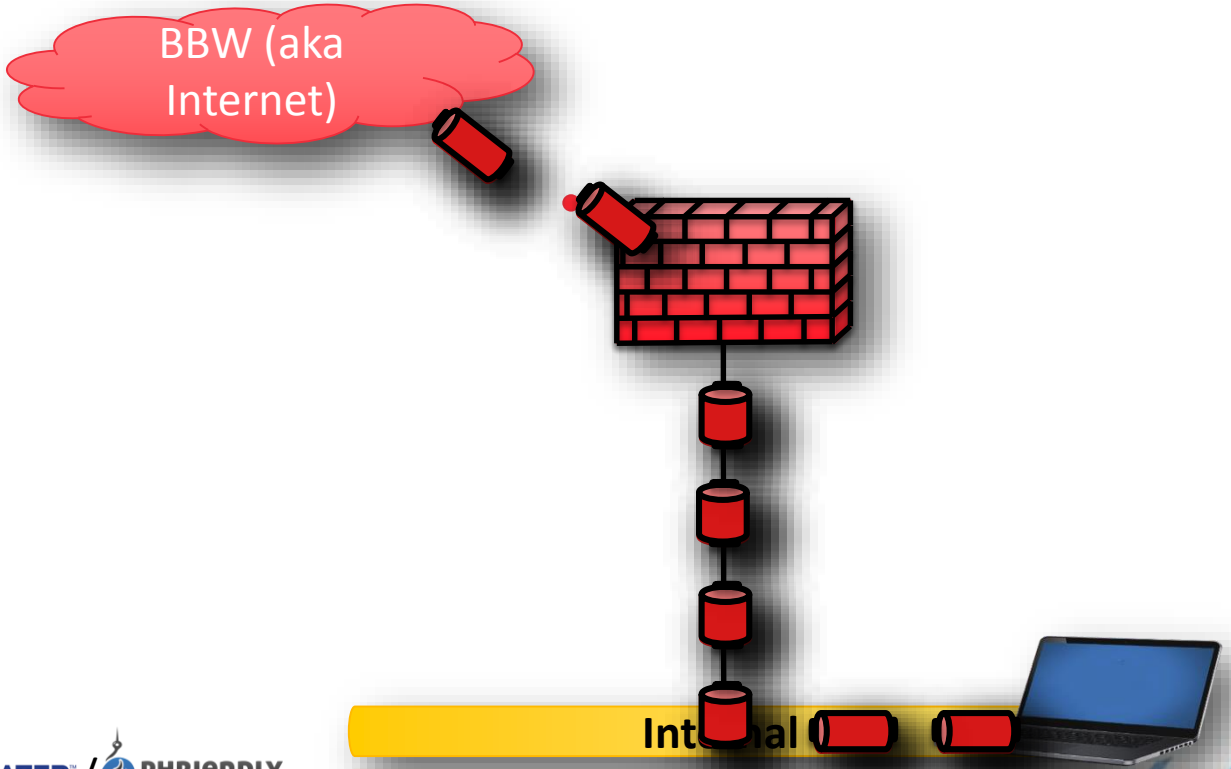
Thank you,
United Parcel Service

*** This is an automatically generated email, please do not reply ***

It starts here – Pickup for one



Fetch Malware (if needed)



and then – Code Execution (almost)

Wed Apr 23 2014 18:52:04,0,macb,r/rrwxrwxrwx,0,0,120976-128-1,"/Users/{VICTIMUSER}/AppData/Local/Temp/CVR8D02.tmp.cvr"

Wed Apr 23 2014 18:52:04,134,macb,r/rrwxrwxrwx,0,0,120981-128-1,"/Users/{VICTIMUSER}/AppData/Local/Temp/101634.od"

Wed Apr 23 2014 18:52:06,342960,.ac.,r/rrwxrwxrwx,0,0,121032-128-4,"/ProgramData/Adobe/ARM/Acrobat_10.1.8/17525/AcrobatUpdater.exe"

Wed Apr 23 2014 18:52:06,959904,.a..,r/rrwxrwxrwx,0,0,121065-128-3,"/ProgramData/Adobe/ARM/Acrobat_10.1.8/17525/AdobeARM.exe"

Wed Apr 23 2014 18:52:06,56,...b,d/drwxrwxrwx,0,0,86295-144-5,"/ProgramData/Adobe/ARM/Acrobat_10.1.8/17525"

Wed Apr 23 2014 18:52:07,53864,.a.b,-/rrwxrwxrwx,0,0,120795-128-4,"/Users/{VICTIMUSER}/AppData/Roaming/Skype/{VICTIMUSER}_{COMPANY}/keyval.db-journal (deleted)”

--snip--

Almost…

Wed Apr 23 2014 18:52:11,1080,.ac.,r/rrwxrwxrwx,0,0,2119-128-1,"/Windows/security/templates/policies/tmpgptfl.inf"

Wed Apr 23 2014 18:52:11,6144,.a.b,r/rrwxrwxrwx,0,0,24745-128-4,"/Users/{VICTIMUSER}/AppData/Roaming**/Dropbox/UPDATED_8yxbxq**"

Wed Apr 23 2014 18:52:11,6144,.a.b,r/rrwxrwxrwx,0,0,3436-128-4,"/Users/{VICTIMUSER}/AppData/Roaming/Dropbox/PENDING_ln1z4y"

Wed Apr 23 2014 18:52:11,1408,mac.,r/rrwxrwxrwx,0,0,4015-128-1,"/Windows/security/templates/policies/gpt00000.dom”

--snip—

Wed Apr 23 2014 18:53:11,37358015,...b,r/rrwxrwxrwx,0,0,122495-128-3,"/**Program Files/Trend Micro/OfficeScan Client/icrc$oth.743”**

--snip--

Ready…

Wed Apr 23 2014 18:57:52,643,m.c.,r/rrwxrwxrwx,0,0,25199-128-5,"/Users/{VICTIMUSER}/AppData/LocalLow/Sun/**Java/Deployment/deployment.properties"**

Wed Apr 23 2014 18:57:59,12861,.a.b,r/rrwxrwxrwx,0,0,92319-128-5,"/Users/{VICTIMUSER}/AppData/Local/Temp/jar_cache4093301292953746614.tmp"

Wed Apr 23 2014 18:58:00,12861,m...,r/rrwxrwxrwx,0,0,92319-128-5,"/Users/{VICTIMUSER}/AppData/Local/Temp/jar_cache4093301292953746614.tmp"

Wed Apr 23 2014 18:58:03,137529,macb,r/rrwxrwxrwx,0,0,122810-128-5,"/Users/{VICTIMUSER}/AppData/Local/Temp/**~tmf57849818705828531 66.tmp**"

Wed Apr 23 2014 18:58:07,144,...b,d/dr-xr-xr-x,0,0,122868-144-1,"/Users/{VICTIMUSER}**/AppData/Local/Temp/stjcrtu**"

Wed Apr 23 2014 18:58:07,0,macb,r/rrwxrwxrwx,0,0,122877-128-4,"/Users/{VICTIMUSER}/AppData/Local/Temp/~tmf59727845815307790.tmp"

Wed Apr 23 2014 18:58:09,16896,macb,r/rrwxrwxrwx,0,0,122855-128-3,"/Users/{VICTIMUSER}/**AppData/Local/sollenh.dll**"

Set…

Wed Apr 23 2014 18:58:09,48,macb,d/drwxrwxrwx,0,0,122879-144-1,"/Users/{VICTIMUSER}/AppData/Roaming/Microsoft/Crypto/Keys

Wed Apr 23 2014 18:58:10,2080,.a.b,r/rrwxrwxrwx,0,0,122927-128-4,"/Users/{VICTIMUSER}/AppData/Roaming/**Microsoft/Crypto/RSA**/S-1-5-21-254666440-1725212059-1820442801-6608/**28093c3a55c1788ef10f8a6ac25eff17_55be799d-cb75-4e81-9059-484e3bdbf27e**"

GO!

Wed Apr 23 **2014 18:58:29,144**,mac.,d/dr-xr-xr-x,0,0,122868-144-1,"/Users/{VICTIMUSER}/**AppData/Local/Temp/stjcrtu**”

Wed Apr 23 **2014 18:58:29,56,**...b,d/dr-xr-xr-x,0,0,122874-144-5,"/Users/{VICTIMUSER}/AppData/Local/Temp/**stjcrtu/sfpbkpv”**

Setting up some working directories

Wed Apr 23 2014 18:58:34,56,...b,d/drwxrwxrwx,0,0,123016-144-6,"/Users/{VICTIMUSER}/AppData/Local/Temp/cache"
Wed Apr 23 2014 18:58:34,56,...b,d/dr-xr-xr-x,0,0,123313-144-5,"/Users/{VICTIMUSER}/AppData/Local/Temp/cache/7484"
Wed Apr 23 2014 18:58:34,56,...b,d/dr-xr-xr-x,0,0,123444-144-5,"/Users/{VICTIMUSER}/AppData/Local/Temp/cache/7468"
Wed Apr 23 2014 18:58:34,488,...b,d/dr-xr-xr-x,0,0,123467-144-1,"/Users/{VICTIMUSER}/AppData/Local/Temp/cache/7444"
Wed Apr 23 2014 18:58:34,712,...b,d/dr-xr-xr-x,0,0,123469-144-1,"/Users/{VICTIMUSER}/AppData/Local/Temp/cache/7452"
Wed Apr 23 2014 18:58:34,56,...b,d/dr-xr-xr-x,0,0,123493-144-5,"/Users/{VICTIMUSER}/AppData/Local/Temp/cache/7476"
Wed Apr 23 2014 18:58:34,56,...b,d/dr-xr-xr-x,0,0,123495-144-5,"/Users/{VICTIMUSER}/AppData/Local/Temp/cache/7492"
Wed Apr 23 2014 18:58:34,56,...b,d/dr-xr-xr-x,0,0,123501-144-5,"/Users/{VICTIMUSER}/AppData/Local/Temp/cache/7460"
Wed Apr 23 2014 18:58:34,56,...b,d/dr-xr-xr-x,0,0,123503-144-5,"/Users/{VICTIMUSER}/AppData/Local/Temp/cache/7500"
Wed Apr 23 2014 18:58:34,56,...b,d/dr-xr-xr-x,0,0,123508-144-5,"/Users/{VICTIMUSER}/AppData/Local/Temp/cache/7548”

Going…

Wed Apr 23 **2014 18:58:29,144**,mac.,d/dr-xr-xr-x,0,0,122868-144-1,"/Users/{VICTIMUSER}/**AppData/Local/Temp/stjcrtu**”

Wed Apr 23 **2014 18:58:29,56,**...b,d/dr-xr-xr-x,0,0,122874-144-5,"/Users/{VICTIMUSER}/AppData/Local/Temp/**stjcrtu/sfpbkpv”**

Deleting and replacing

Wed Apr 23 2014 18:58:42,854,m.c.,r/rrwxrwxrwx,0,0,100378-128-4,"/**$Recycle.Bin/S-1-5-21-254666440-1725212059-1820442801-6608/$I0BSMNY.tif"**
Wed Apr 23 2014 18:58:42,854,m.c.,r/rrwxrwxrwx,0,0,101122-128-4,"**/$Recycle.Bin/S-1-5-21-254666440-1725212059-1820442801-6608/$I0UNIVL.PNG**"
Wed Apr 23 2014 18:58:42,854,m.c.,r/rrwxrwxrwx,0,0,103555-128-4,"/$Recycle.Bin/S-1-5-21-254666440-1725212059-1820442801-6608/$I10PECH.pdf"
Wed Apr 23 2014 18:58:42,854,m.c.,r/rrwxrwxrwx,0,0,103561-128-4,"/$Recycle.Bin/S-1-5-21-254666440-1725212059-1820442801-6608/$I03M4QT.jpg"
Wed Apr 23 2014 18:58:42,854,m.c.,r/rrwxrwxrwx,0,0,105290-128-4,"/$Recycle.Bin/S-1-5-21-254666440-1725212059-1820442801-6608/$I00U31E.pdf"
Wed Apr 23 2014 18:58:42,854,m.c.,r/rrwxrwxrwx,0,0,107665-128-4,"/$Recycle.Bin/S-1-5-21-254666440-1725212059-1820442801-6608/$I0YZL1S.pdf"
Wed Apr 23 2014 18:58:42,854,m.c.,r/rrwxrwxrwx,0,0,109246-128-5,"/$Recycle.Bin/S-1-5-21-254666440-1725212059-1820442801-6608/$I0U6IOY.docx"
Wed Apr 23 2014 18:58:42,854,m.c.,r/rrwxrwxrwx,0,0,110317-128-4,"/$Recycle.Bin/S-1-5-21-254666440-1725212059-1820442801-6608/$I17OQ7Z.pdf"
Wed Apr 23 2014 18:58:42,854,m.c.,r/rrwxrwxrwx,0,0,110577-128-4,"/$Recycle.Bin/S-1-5-21-254666440-1725212059-1820442801-6608/$I0SQE7R.JPG"
Wed Apr 23 2014 18:58:42,854,m.c.,r/rrwxrwxrwx,0,0,110581-128-4,"/$Recycle.Bin/S-1-5-21-254666440-1725212059-1820442801-6608/$I0J3VWG.JPG"
Wed Apr 23 2014 18:58:42,854,m.c.,r/rrwxrwxrwx,0,0,114186-128-4,"/$Recycle.Bin/S-1-5-21-254666440-1725212059-1820442801-6608/$I0K7G6U.pdf"
Wed Apr 23 2014 18:58:42,854,m.c.,r/rrwxrwxrwx,0,0,121162-128-4,"/$Recycle.Bin/S-1-5-21-254666440-1725212059-1820442801-6608/$I13206U.pdf

Going…

Wed Apr 23 **2014 18:58:29,144**,mac.,d/dr-xr-xr-x,0,0,122868-144-1,"/Users/{VICTIMUSER}/**AppData/Local/Temp/stjcrtu**”

Wed Apr 23 **2014 18:58:29,56,**...b,d/dr-xr-xr-x,0,0,122874-144-5,"/Users/{VICTIMUSER}/AppData/Local/Temp/**stjcrtu/sfpbkpv”**

Leaving Instructions

Wed Apr 23 2014 18:58:42,1267,macb,r/rrwxrwxrwx,0,0,123701-128-4,"/**ProgramData/Adobe/SLStore/HOW_DECRYPT.TXT"**
Wed Apr 23 2014 18:58:42,2785,macb,r/rrwxrwxrwx,0,0,123728-128-4,"/**ProgramData/Adobe/SLStore/HOW_DECRYPT.HTML"**
Wed Apr 23 2014 18:58:42,135,macb,r/rrwxrwxrwx,0,0,123733-128-1,"/**ProgramData/Adobe/SLStore/HOW_DECRYPT.URL"**
Wed Apr 23 2014 18:58:42,1267,macb,r/rrwxrwxrwx,0,0,123734-128-4,"/ProgramData/Adobe/HOW_DECRYPT.TXT"
Wed Apr 23 2014 18:58:42,2785,macb,r/rrwxrwxrwx,0,0,123742-128-4,"/ProgramData/Adobe/HOW_DECRYPT.HTML"
Wed Apr 23 2014 18:58:42,135,macb,r/rrwxrwxrwx,0,0,123801-128-1,"/ProgramData/Adobe/HOW_DECRYPT.URL"

Still going

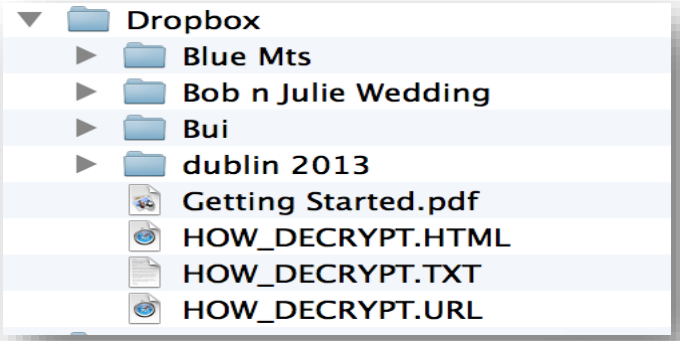
Wed Apr 23 2014 19:33:40,3946070,m.c.,r/rrwxrwxrwx,0,0,121842-128-1,"/Users/{VICTIMUSER}/Desktop/{VICTIMUSER}/HEN MADNESS/Beyoncé - Crazy In Love ft. JAY Z.mp3"

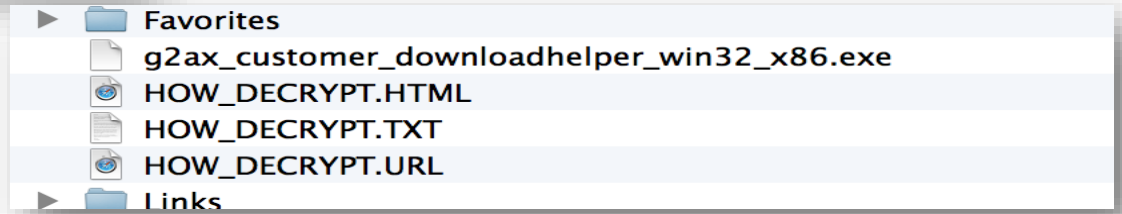
And …….Done

Wed Apr 23 2014 21:00:09,541526,..c.,r/rrwxrwxrwx,0,0,127646-128-4,"/Users/{VICTIMUSER}/Desktop/{COMPANY} Group Chart (External)(apr 2014).ppt"

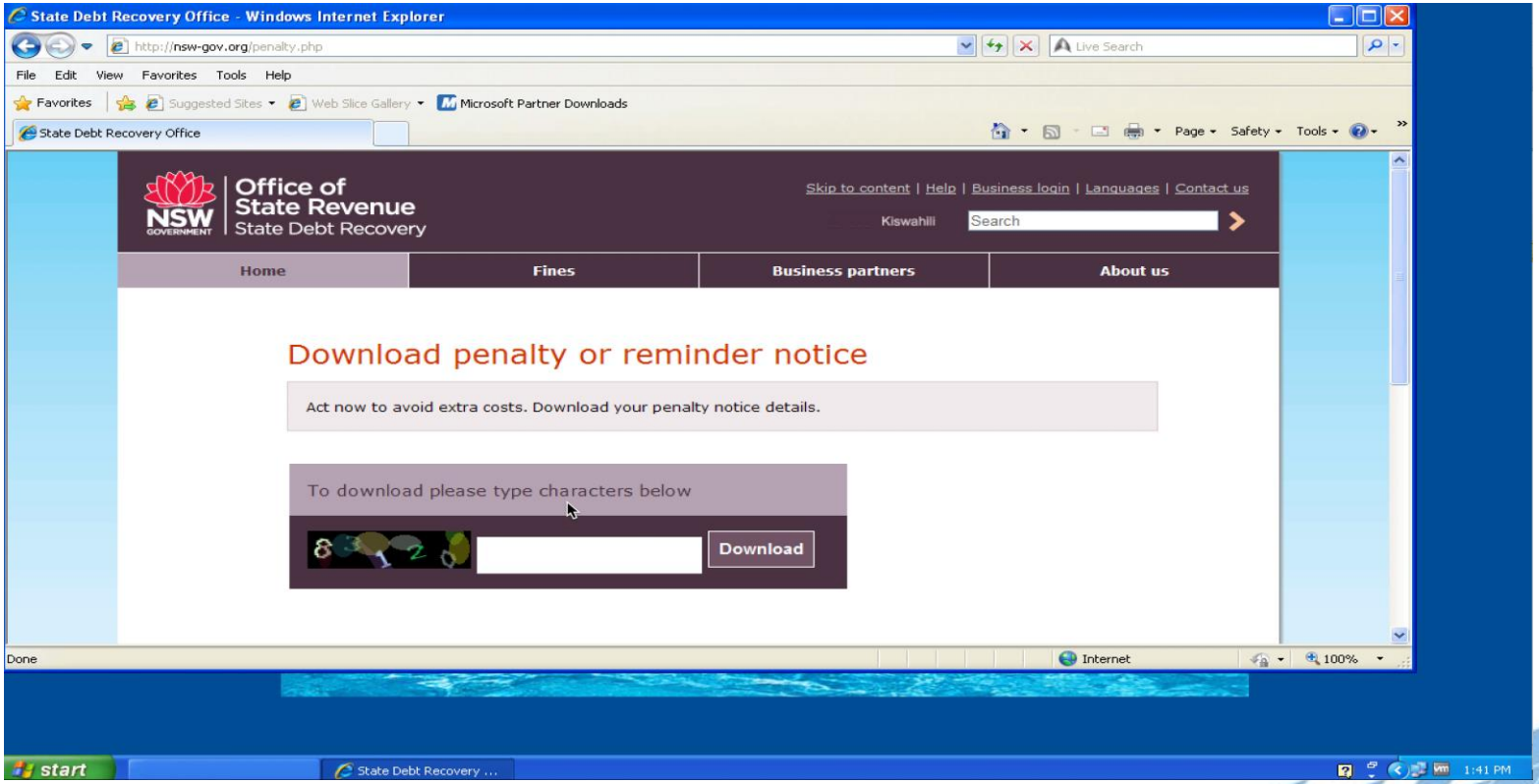
Wed Apr 23 2014 21:00:09,1267,..c.,r/rrwxrwxrwx,0,0,135836-128-4,"/Users/{VICTIMUSER}/Desktop/HOW_DECRYPT.TXT"

End Result

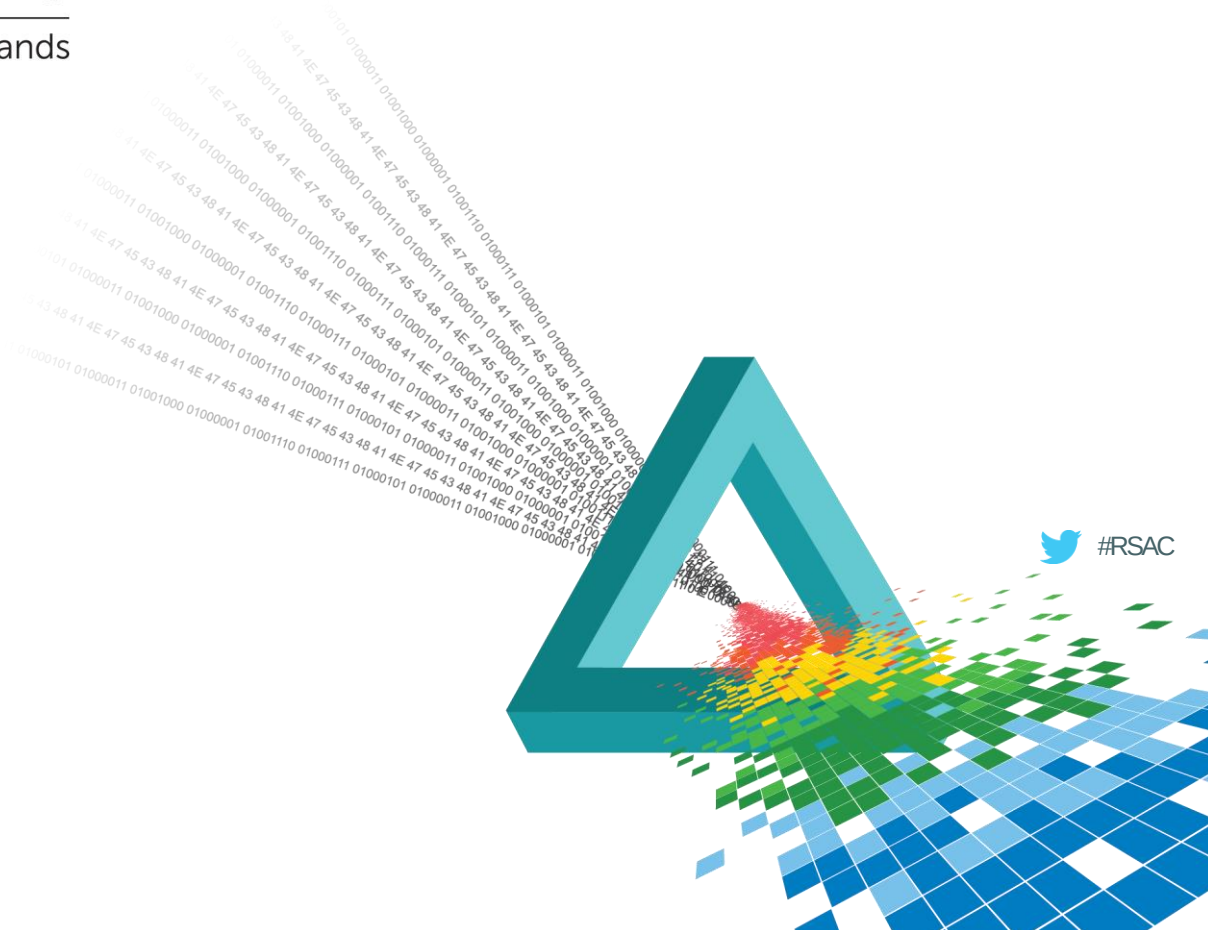

Dropbox
Blue Mts
Bob n Julie Wedding
Bui
dublin 2013
Getting Started.pdf
HOW_DECRYPT.HTML
HOW_DECRYPT.TXT
HOW_DECRYPT.URL


Favorites
g2ax_customer_downloadhelper_win32_x86.exe
HOW_DECRYPT.HTML
HOW_DECRYPT.TXT
HOW_DECRYPT.URL
Links

Ransomware at work



What now?



Recovery options

- Recycle bin? X Sometimes ✓
- Unallocated space? X Sometimes ✓
- Backups? ✓
- Prayer and/or Magic? X

Recovery options

- Pay? ✓

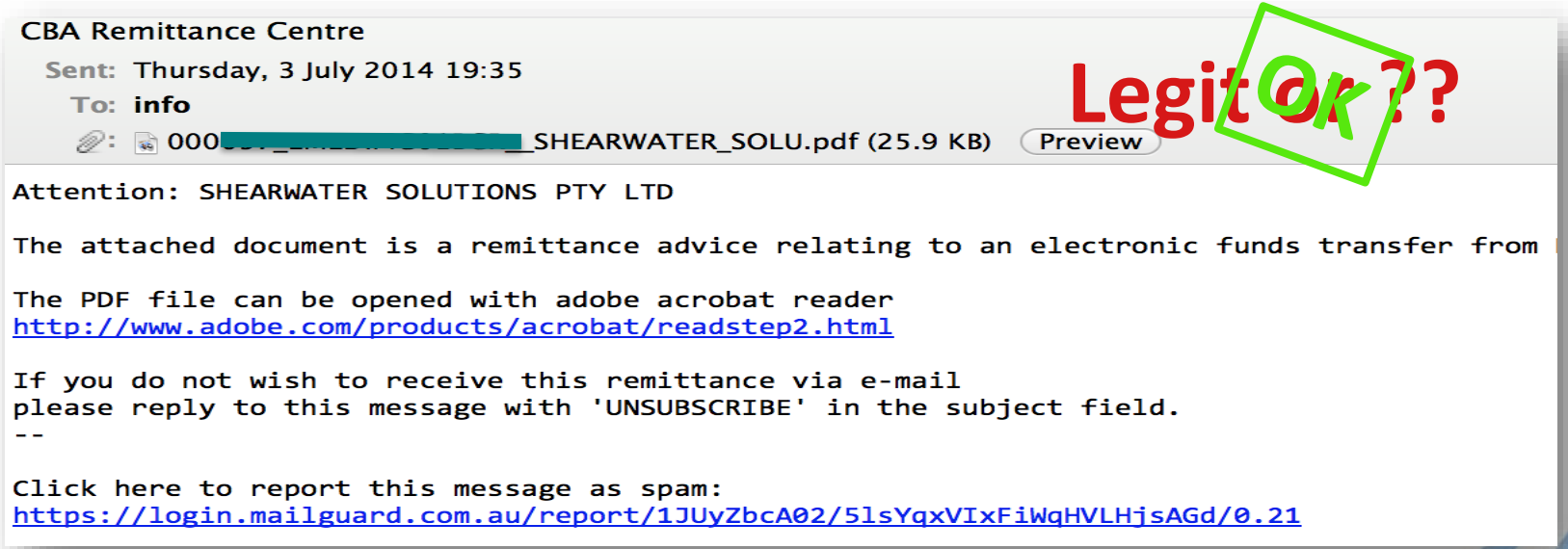
But depending on where you are you may be committing a crime

Recovery

- Backups
  - Backup all locations
    - Cloud, network, local, everything
  - Test recovery

Educate

- Teach users not to click



Next steps

- Next week
  - Check backup and recovery processes
    - Make sure you can recover
  - Check AV on email, web and desktop
    - Are they updating? Have you covered TLS?

- Next few months
  - Educate users (most are delivered through phishing)
    - Even if only 50% “get it” still better off
  - Improve monitoring on outbound connections (C2C)

Future 2015 SANS Events in India

Questions?

SANS

Secure India

4-16 May | Bangalore

SEC401: **Security Essentials Bootcamp Style** (GSEC)
4-9 May

SEC504: **Hacker Tools, Techniques, Exploits, and Incident Handling** (GCIH)
4-9 May

SEC503: **Intrusion Detection In-Depth** (GCIA)
11-16 May

Delhi

24 August - 5 September | Delhi

FOR526: **Memory Forensics In-Depth**

FOR610: **Reverse-Engineering Malware: Malware Analysis Tools and Techniques** (GREM)

Bangalore

28 September - 10 October | Bangalore

NEW! SEC511: **Security Essentials Bootcamp Style** 28 Sep - 3 Oct

SEC575: **Mobile Device Security and Ethical Hacking** (GMOB) 28 Sep - 3 Oct

SEC642: **Advanced Web App Penetration Testing and Ethical Hacking** 28 Sep - 3 Oct

SEC560: **Network Penetration Testing and Ethical Hacking** (GPEN) 5-10 Oct

Hyderabad

24 November - 5 December | Hyderabad

SEC542: **Web App Penetration Testing and Ethical Hacking** (GWAPT) 24-29 Nov

SEC660: **Advanced Penetration Testing, Exploit Writing, and Ethical Hacking** (GXPN) 30 Nov - 5 Dec

ICS410: **ICS/SCADA Security Essentials** (GICSP) 30 Nov - 4 Dec

COMPLETE DETAILS AT **sans.org/security-training/by-location/apac** | CONTACT **AsiaPacific@sans.org**