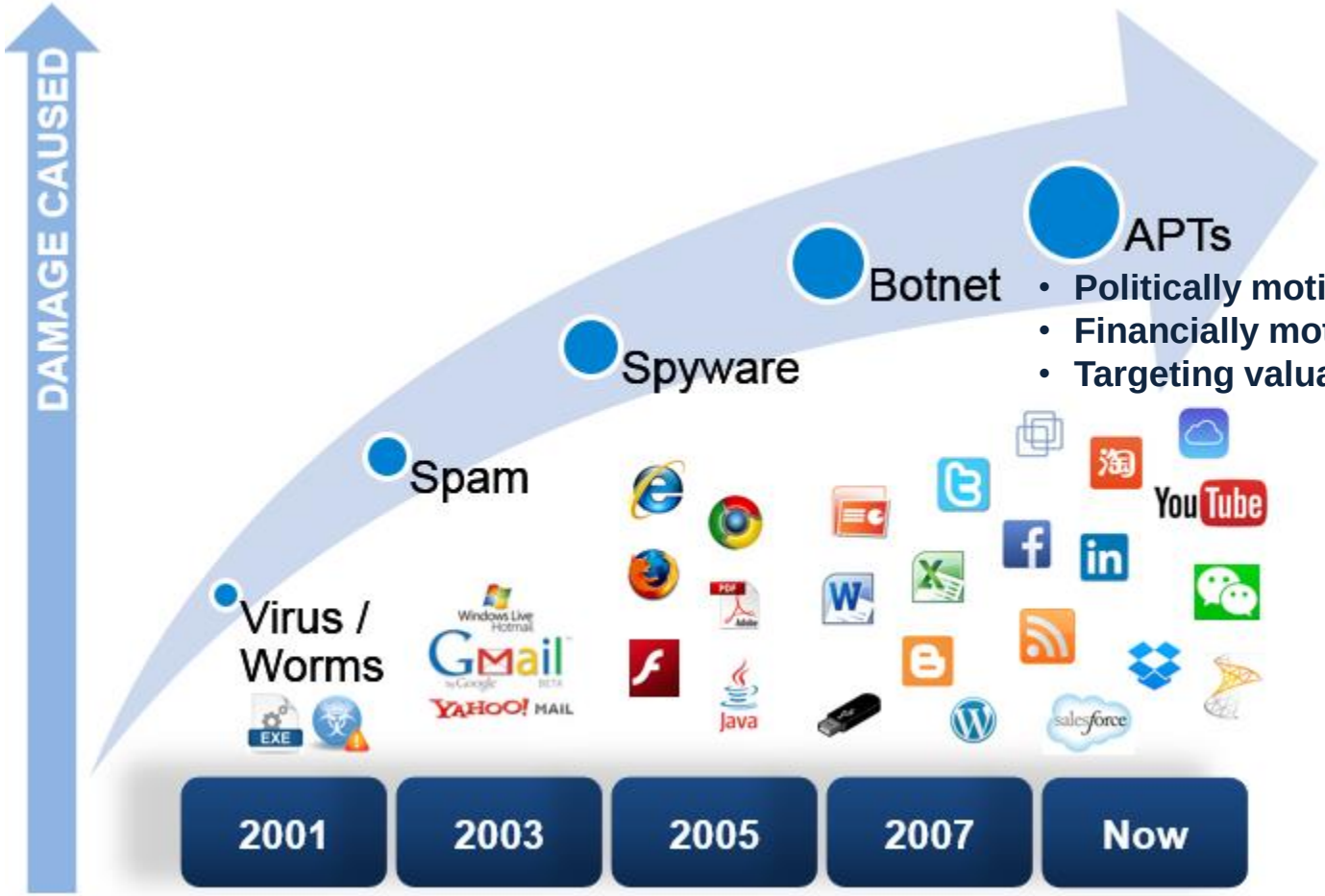

websense
EFFECTIVE ADVANCED THREAT PROTECTION STRATEGY
Michael Tam, Websense
TRITON STOPS MORE THREATS. WE CAN PROVE IT.
websense®
TRITON™

Threat Landscape



Top 10 Countries Hosting Phishing

1. China
2. United States
3. Germany
4. United Kingdom
5. Canada
6. Russia
7. France
8. Hong Kong
9. Netherlands
10. Brazil

Some interesting points about this list:

- China and Hong Kong made their debuts in 2013, having never before been included in our lists
- Chinese is now the 2nd most common spam language, overtaking Russian.
- The U.S. dropped out of the number one spot, for the first time in a long, long time

Visit: http://securitylabs.websense.com/

HSBC

Sir/Madam

Upon your request, attached please find payment e-Advice for your reference.

Yours faithfully

HSBC

****

We maintain strict security standards and procedures to prevent unauthorised access to information about you. HSBC will never contact you by e-mail or otherwise to ask you to validate personal information such as your user ID, password, or account numbers. If you receive such a request, please call our Direct Financial Services hotline.

Please do not reply to this e-mail. Should you wish to contact us, please send your e-mail to commercialbanking@hsbc.com.hk and we will respond to you.

Note: it is important that you do not provide your account or credit card numbers, or convey any confidential information or banking instructions, in your reply mail.

****

Payment_Advice.zip

- The email is send from the spoofed address payment.advice@hsbc.com.hk
- The attached ZIP file has the name Payment_Advice.zip and contains the 96 kB file Payment_Advice.exe.
- 3 of the 50 AV engines did detect the Trojan at Virus Total.

virustotal

SHA256:	b45f2dbfe77dd2fecef23a667d31e1fbf7a0857ba036527ea8285c7d4c989e40
File name:	Payment Advice.zip^Payment Advice.exe
Detection ratio:	3 / 50
Analysis date:	2014-01-30 10:13:22 UTC

New York Times

websense

Chinese Hackers Stole Every New York *Times* Employee's Password

By Adam Martin

On Wednesday night, after enduring four months of hacking, the New York *Times* finally reported that its computer network had been infiltrated and that it had ousted its attackers, who it linked to the Chinese military. In the meantime, hackers stole every *Times* employee's corporate password, and used them to get into 53 employees' personal computers. The attacks started as the paper wrapped up reporting on its bombshell investigative piece about the family wealth of Chinese Prime Minister Wen Jiabao, and ramped up after publication of the story that, it was warned, would "have consequences."

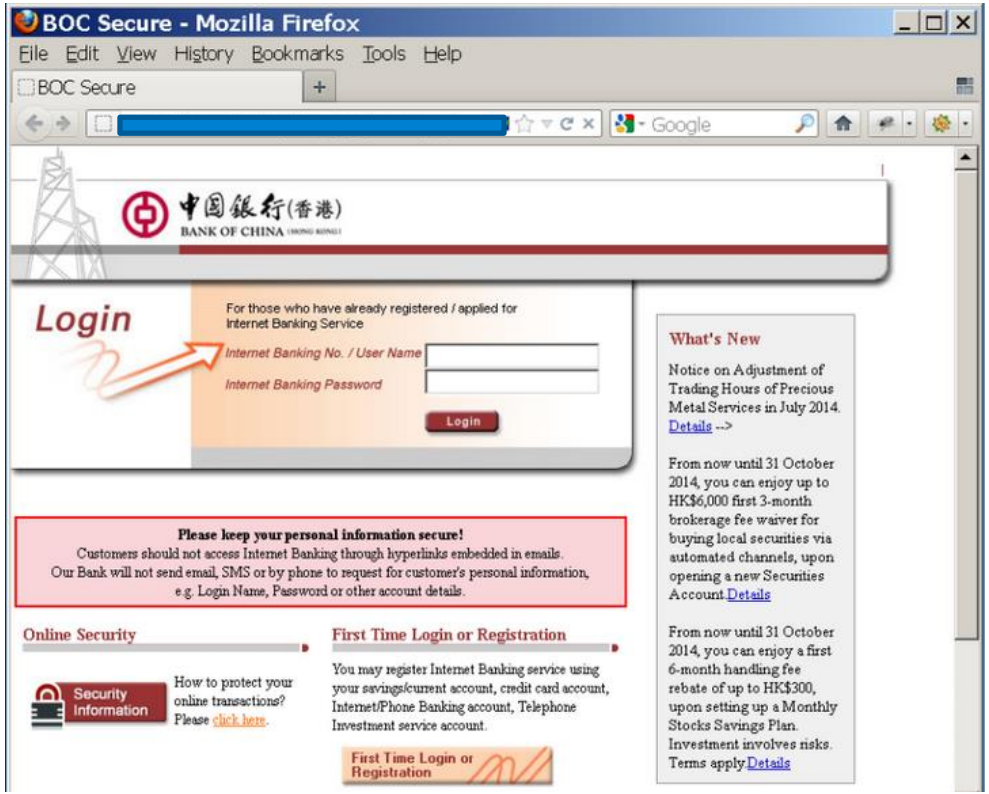
Among the evidence pointing to Chinese government hackers, in addition to increasingly familiar tactics and the targeting of the reporters on the Wen story, was the fact that the attacks tended to start at 8 a.m. Beijing time and generally lasted for a workday before easing off. There was also this:

"Symantec, maker of the NYTimes's anti-virus software, which **found just 1 of the 45** pieces of custom malware installed on the Times servers. Not a ringing endorsement"

The New York Times

2% ***Detection Rate***

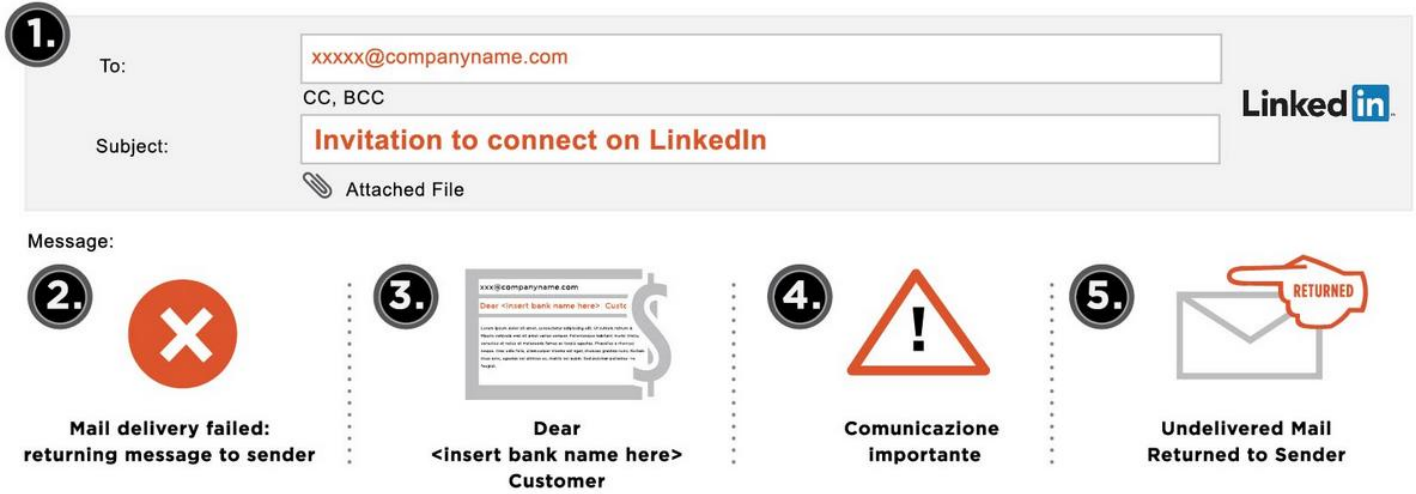
Bank of China (Hong Kong)



A fraudulent website with the domain name "http://ibc.bcdirecthk.com/Obs_lgn_Secure.php"and hosted in the British Virgin Islands. The website purports to be the official website of Bank of China (Hong Kong) Limited (BOCHK). BOCHK has clarified that it has no connection with the fraudulent website.

Five Most Dangerous Subject Lines

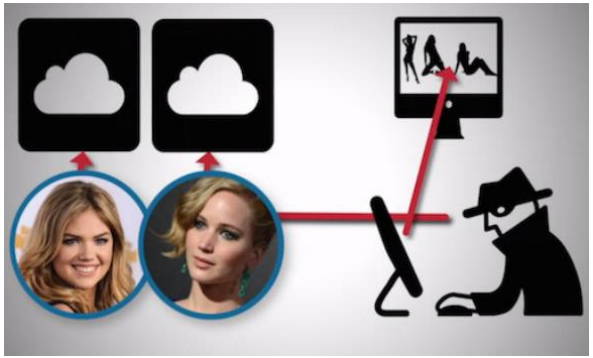
- 1. Invitation to connect on LinkedIn
- 2. Mail delivery failed: returning message to sender
- 3. Dear <insert bank name here> Customer
- 4. Comunicazione importante
- 5. Undelivered Mail Returned to Sender



Data Leakage

Target

The Home Depot



iCloud

Edward Snowden

Impact

- Target: Stolen information involved at least 70 million people
- The Home Depot: Affected 56 million payment cards
- iCloud: The accounts of some Hollywood actors and leaked their personal pictures online
- Edward Snowden: Only 10%of the NSA's collected data pertains to possible illegal activity

Security Effectiveness is Declining Rapidly

websense

" Signature based tools (anti-virus, firewalls, and intrusion prevention) are **only effective against 30-50% of current security threats**. Moreover, customers expect the effectiveness of signature-based security to continue to decline rapidly."

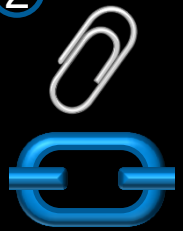
IDC Threat Intelligence Update, 14-Feb-2012

websense TRITON

Traditional Attack

1

2



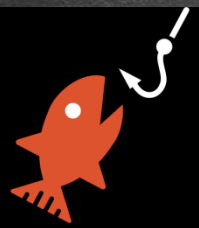
3

Advanced Threat

The Nature of Advanced Persistent Threats

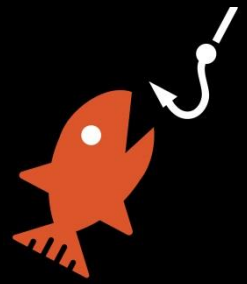
Can You See Threats Across the Kill Chain?

websense

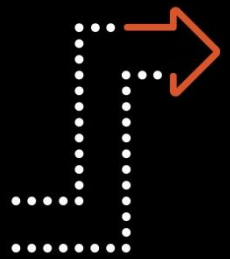
01	02	03	04	05	06	07
						
RECON	LURE	REDIRECT	EXPLOIT KIT	DROPPER FILE	CALL HOME	DATA THEFT

websense TRITON

RECON



LURE



REDIRECT

EXPLOIT KIT

DROPPER FILE

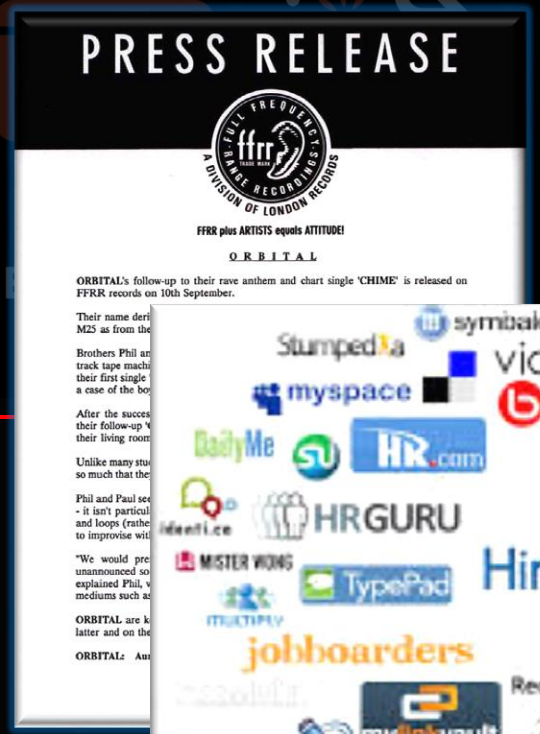
CALL HOME

DATA THEFT

websense TRITON

RECON LURE REDIRECT CALL DATA

- Social Media
- Press
- Agency web site
- Insider


PRESS RELEASE

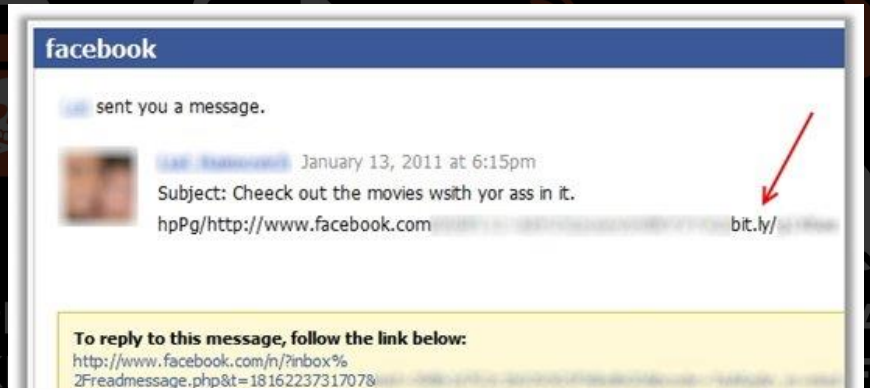
FFRR plus ARTISTS equals ATTITUDE!

ORBITAL

ORBITAL's follow-up to their rave anthem and chart single 'CHIME' is released on FFRR records on 10th September.

RECON **LURE** REDIRECT EXP

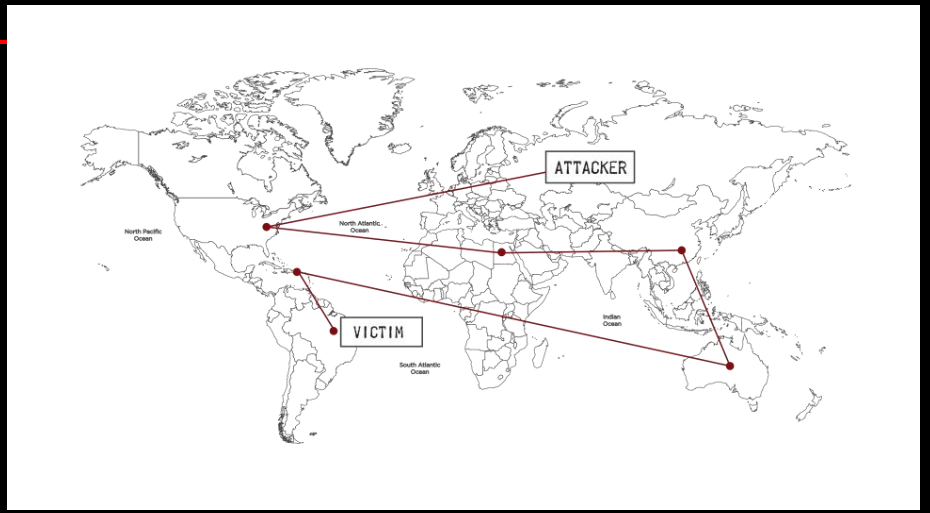
- Mass Spam
- Social Media
- Targeted Email
- SMS

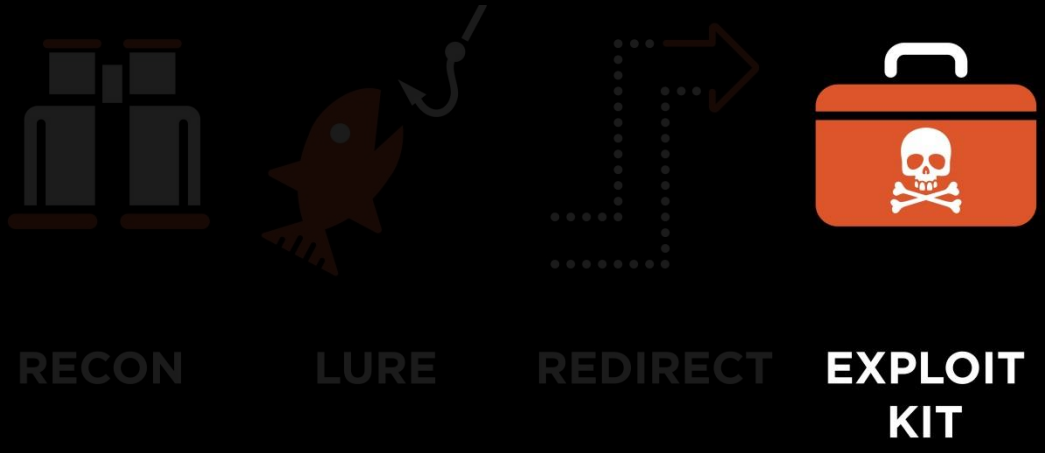


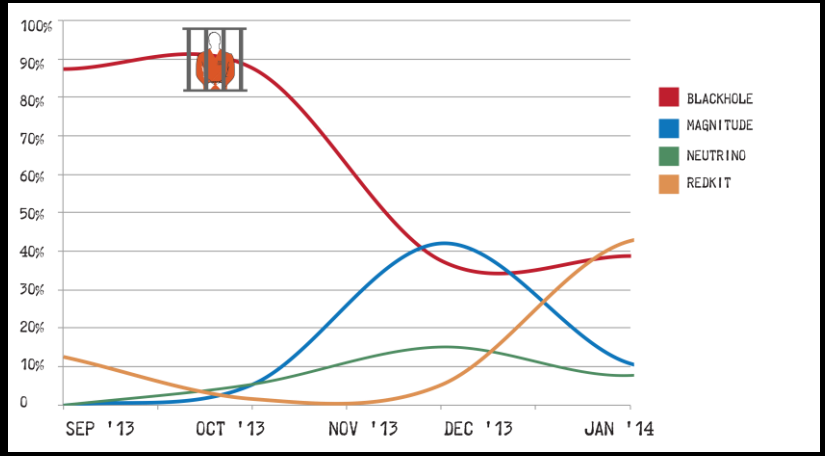
RECON LURE **REDIRECT** EXPLOIT KIT DROPPER FILE CALL HOME DATA THEFT

Evasion Techniques

- Bypass Filters
- Defies analysis





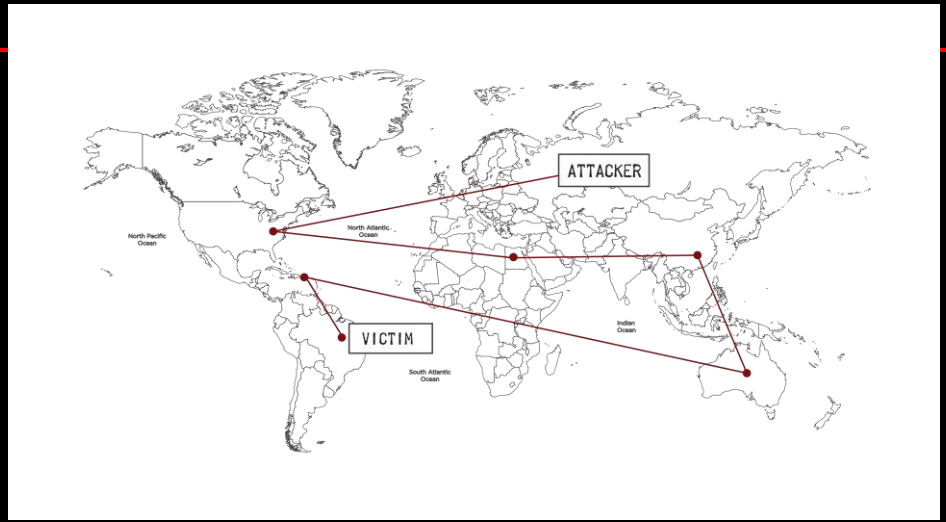


Penetrate Defenses

- OS Exploits
- Browser Exploits
- App Exploits

- File download
- Drive-by download
- Embedded code
- Nested objects

RECON LURE REDIRECT EXPLOIT KIT DROPPER FILE **CALL HOME** DATA THEFT



- Botnet Mgmt
  - Connect
  - Update
- Evasion, such as Dynamic DNS
- Web, Email, etc.

websense TRITON

RECON

DROPPER FILE

CALL HOME

DATA THEFT

Cryptorbit

YOUR PERSONAL FILES ARE ENCRYPTED

All files including videos, photos and documents, etc on your computer are encrypted.

Encryption was produced using a **unique** public key 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 time specified in this window**. After that, nobody and never will be able to restore files

In order to decrypt the files, open site **4sfxctgp53imlvzk.onion.to/index.php** and follow the instructions.

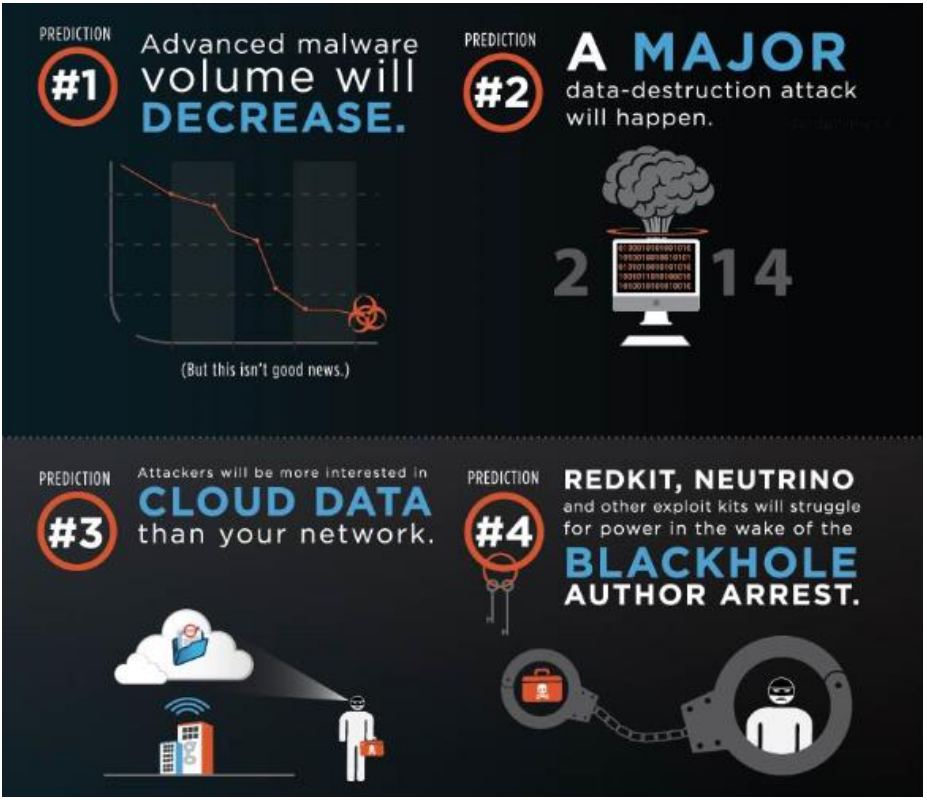
If **4sfxctgp53imlvzk.onion.to** is not opening, please follow the steps below:
1. You must download and install this browser:
http://www.torproject.org/projects/torbrowser.html.en
2. After installation, run the browser and enter the address:
4sfxctgp53imlvzk.onion/index.php
3. Follow the instructions on the web-site. We remind you that the sooner you do, the more chances are left to recover the files.

Realize Objective

- Theft
- Destruction
- Corruption

Websense 2014 Security Predictions

websense



2014 Predictions Accuracy

websense

1. Advanced malware volume will decrease: Yes
2. A major data-destruction attack will happen: Yes
3. Attackers will be more interested in cloud data than your network: Yes
4. Redkit, Neutrino and other exploit kits will struggle for power in the wake of the Blackhole author arrest: Yes
5. Java will remain highly exploitable and highly exploited — with expanded repercussions: Yes
6. Attackers will increasingly lure executives and compromise organizations via professional social networks: Yes
7. Cybercriminals will target the weakest links in the data-exchange chain: Yes
8. Mistakes will be made in “offensive” security due to misattribution of an attack’s source: Inconclusive

LIVE WEBCAST: Wednesday, Dec. 3, 2014
11 a.m. CST/HKT/SG

www.websense.com/2015PredictionsAPAC


websense
THANK YOU
TRITON STOPS MORE THREATS. WE CAN PROVE IT.
websense®
TRITON™