

بسم الله الرحمن الرحيم



الإختراق الاخلاقي والأمن الإلكتروني

Ethical Hacking and Cyber Security



@alosefer

ياسر العصيفير

Yaser.contact@gmail.com



المحاور



- تعريف
- هل الحماية مهمة؟
- أمان واختراق الأنظمة
- ransomware
- فيروس #WannaCry
- الهندسة الإجتماعية
- حماية البيانات داخل المنظمات
- أسئلة واستفسارات



المتحدث

ياسر العصيفير



- متخصص في الحاسب الآلي
- دكتوراه في أمن الإنترنت من جامعة كاردف، بريطانيا 2012
- مستثمر ومدير للعديد من الشركات التقنية الناشئة في الشرق الأوسط و سيلكون فالي



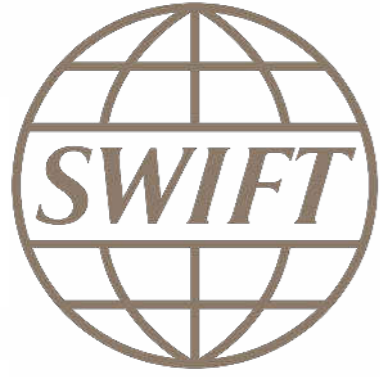
@alosefer



{أفضل الصدقة أن يتعلم المسلم علما ثم يعلمه أخاه المسلم}



هل الحماية مهمة؟



شبكة SWIFT المصرفية!



عدة اختراقات على شبكة

SWIFT في بانكوك و الفلبين

و غيرها بإجمالي سرقة =

٣٣٠ مليون ريال!



هل الحماية مهمة؟



وكالة الأمن القومي الأمريكية

Equation Group

Equation group victims map

- Finance
- Diplomatic / Embassies
- Energy / Infrastructure
- Military
- Telecommunications
- Islamic Scholars
- Other / Unknown
- Government
- Research institution
- University
- Aerospace
- Medical
- Media

High infection rate

- Iran
- Russian Federation
- Pakistan
- Afghanistan
- India
- China
- Syria
- Mali

Low infection rate

- Turkey
- Somalia
- Myanmar
- Germany
- South Africa
- Nigeria
- United States
- Venezuela
- Sudan
- Palestinian
- Morocco
- Malaysia
- Kazakhstan
- Iraq
- Brazil
- Uganda
- Switzerland
- Singapore
- Philippines
- Peru
- France
- Equador
- Belgium
- Bahrain

Medium-level infection rate

- Lebanon
- Yemen
- United Arab Emirates
- Algeria
- Kenya
- United Kingdom
- Libya
- Mexico
- Qatar
- Egypt



هل الحماية مهمة؟



اختراق وكالة الأمن القومي الأمريكية!!

The Shadow Brokers

Name	Size
▶ BANANAGLEE	6 items
▶ BARGLEE	1 item
▶ BLATSTING	7 items
▶ BUZZDIRECTION	2 items
▶ EXPLOITS	8 items
▶ OPS	6 items
▶ SCRIPTS	33 items
▶ TOOLS	15 items
▶ TURBO	2 items

NSA HACKED!
Private Hacking Tools & Exploits Leaked



هل الحماية مهمة؟



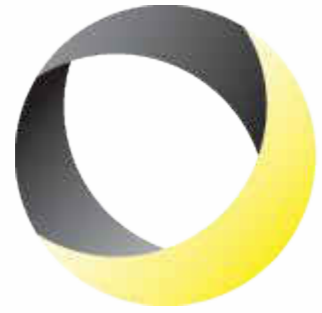
ياهو YAHOO

تسريب معلومات 500 مليون مستخدم،

والتنصت على الكل من NSA

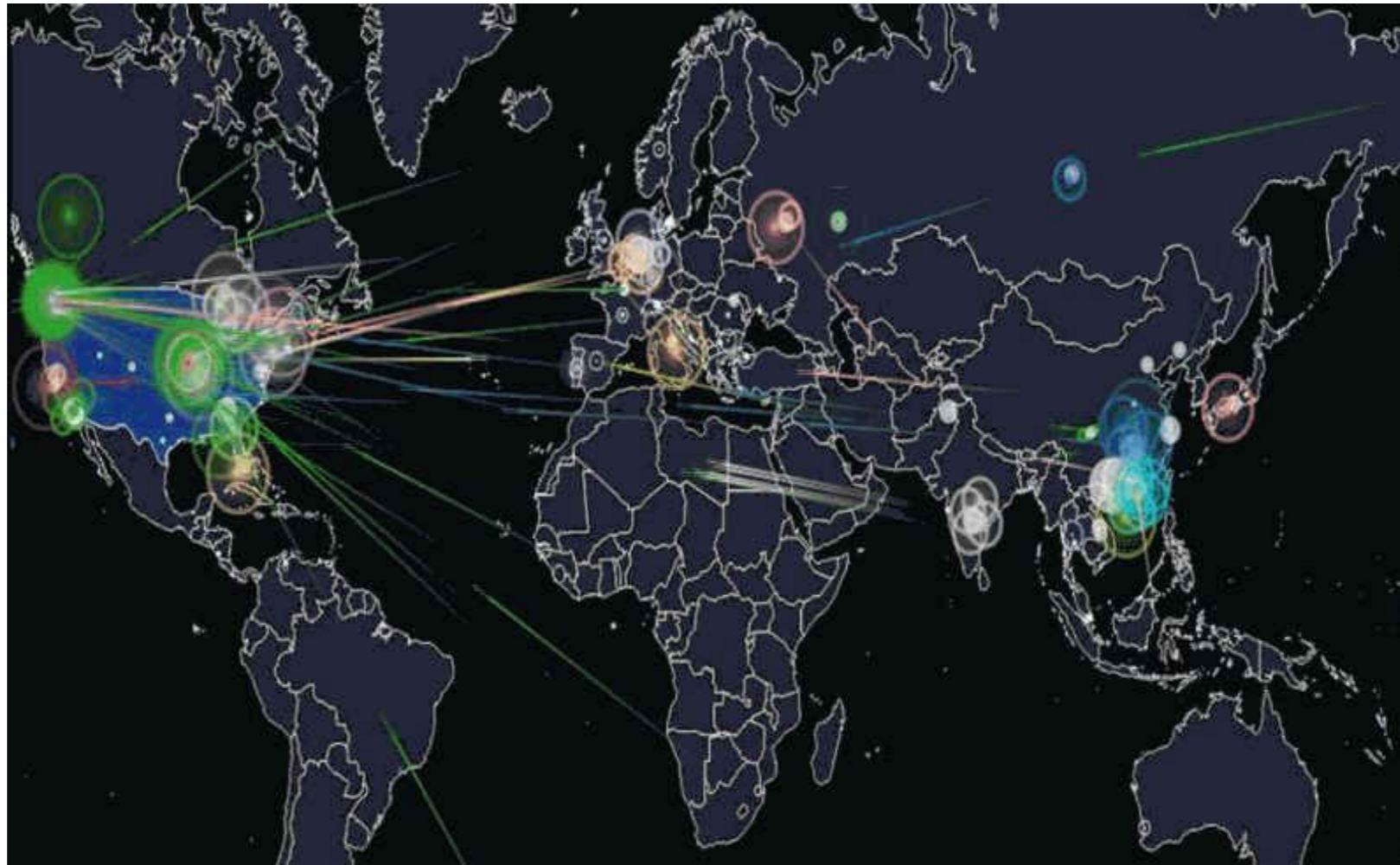


هل الحماية مهمة؟



DynSM | DNS
EMAIL
LABS

The DYN DNS



هل الحماية مهمة؟

خسارة تقدر بـ **\$1.3 billion**

SONY



1. You can download a part of Sony Pictures internal data the volume of which is tens of Terabytes on the following addresses.
2. These include many pieces of confidential data.
- 3.
4. Password: diespe123
- 5.
6. 1. Torrent
7. <http://ge.tt/...>
8. <http://rghost.net/...>
9. <http://rmdown.com/link.php?hash=1439570...>
10. <http://netload.in/dateiSwxIU761...>
- 11.
12. 2. Mega
13. <https://mega.co.nz/#!xdhktQZ1CKml...>
14. <https://mega.co.nz/#!8VJQFQpA!ZpwA...>
15. <https://mega.co.nz/#!dYZxzDYY!raW5...>
16. <https://mega.co.nz/#!NIpXXTZT!A64x...>
17. <https://mega.co.nz/#!AcA2W3Cb!mtYU...>
18. <https://mega.co.nz/#!9YI2xJAY!wgGT...>
19. <https://mega.co.nz/#!NIIWnTCQ!reJI...>
20. <https://mega.co.nz/#!hUh0gLYB!gDwn...>
21. <https://mega.co.nz/#!pVYBLiB!k7es...>
22. <https://mega.co.nz/#!sUZjEBBI!FsaY...>
23. <https://mega.co.nz/#!VR4mVTSZ!vP-x...>
24. <https://mega.co.nz/#!xFQmhCaD!NwCd...>
25. <https://mega.co.nz/#!4JBR1DAT!woCz...>
26. <https://mega.co.nz/#!EAJgSaSR!yAG5...>
27. <https://mega.co.nz/#!1UQJyTKZY!AUMy...>
28. https://mega.co.nz/#!8Ap2FS4B!eR_d...
29. <https://mega.co.nz/#!1IABABgR!cCuQ...>
30. <https://mega.co.nz/#!0NJRkSrD!Fcs8...>
31. <https://mega.co.nz/#!5RYmxbRD!i8Lx...>
32. <https://mega.co.nz/#!VVZ3BBqC!2goJ...>

Cyberkendra.com

Cyberkendra.com

هل الحماية مهمة؟


Linked **in**

117 Million Users

لينكدان LinkedIn

TheRealDeal All I want to order... Q Go

Home / Information and Fraud / Databases / LinkedIn 167M



LinkedIn

167M

By peace_of_mind (100.0%) Level 1 (14)

0 5.0000 / BTC 5.0000

in stock.

Postage Option

Escrow Yes, escrow by RealDeal is available.

Class Digital

Ships From Worldwide



هل الحماية مهمة؟

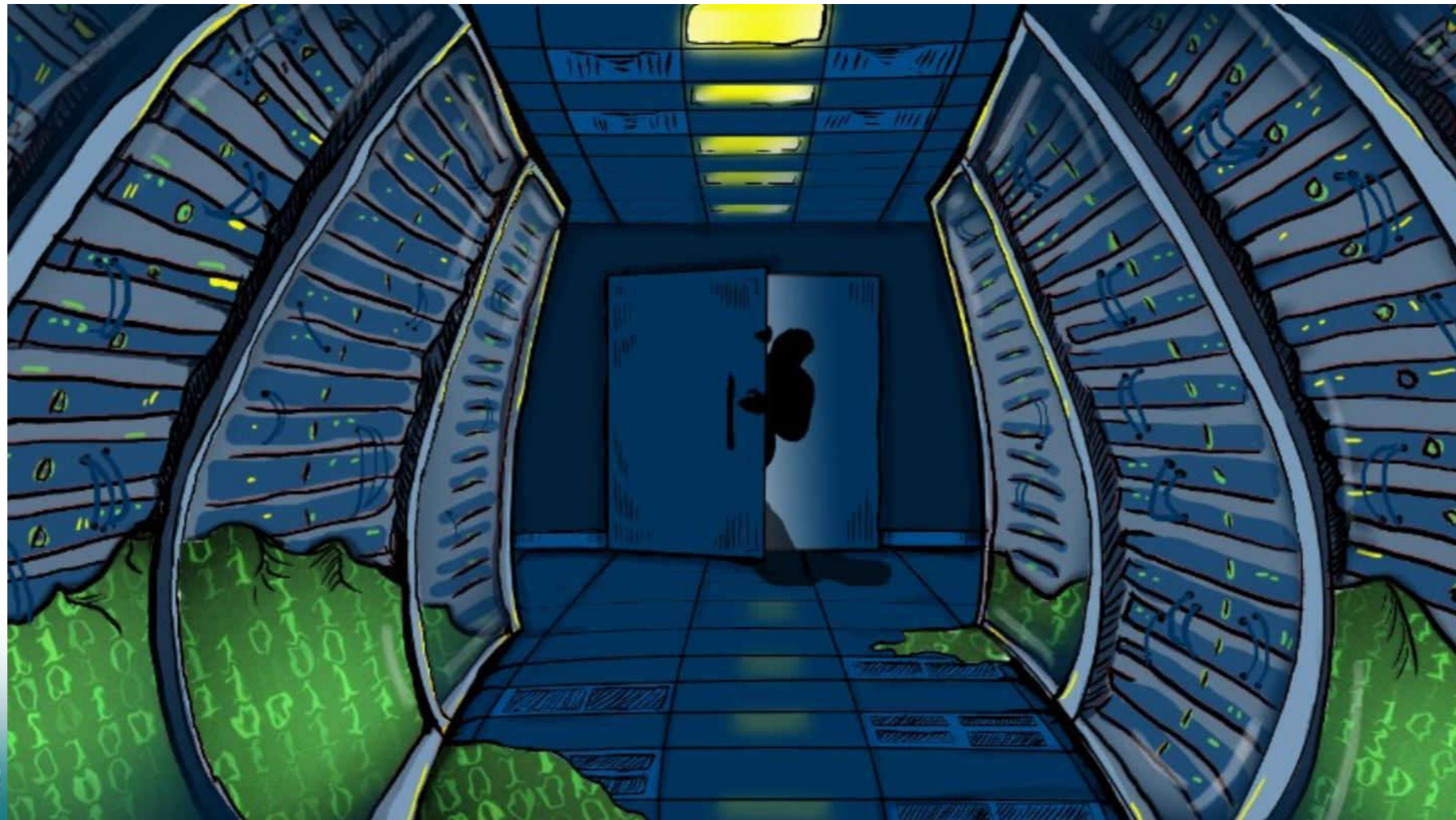


Dropbox

دروب بوكس Dropbox

69 Million Accounts

Passwords+Info

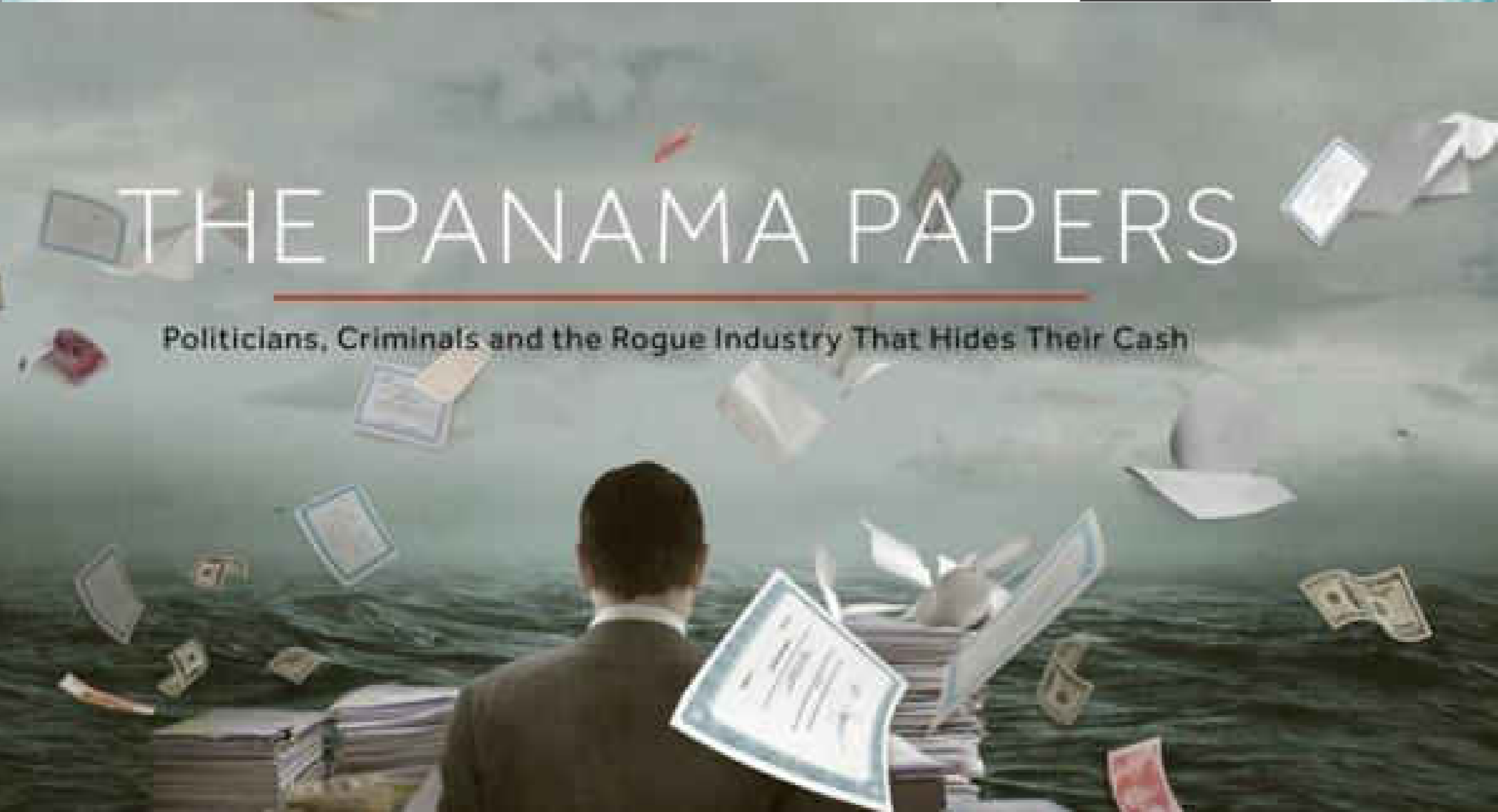


وثائق - بانما



THE PANAMA PAPERS

Politicians, Criminals and the Rogue Industry That Hides Their Cash



أمان وإختراق الأنظمة



بجميع الإختراقات، يمكن تقسيمها إلى طريقتين أساسيتين:



- **داخلي** 
- عن طريق المستخم
- **USB**
- الاجهزة الاخرى بالشبكة العادية او الاسلكية
- أجهزة الشبكة كالطابعات او التلفونات



الإنترنت، وهي الأغلب والأكثر وطرق إختراق الكثير من إختراقات الحرب الإلكترونية او الشخصية، عن طريق:

• **خارجي** 

- البريد
- زيارة موقع
- تحميل برنامج
- قبول إضافة غير معروفة وقبول ملف او رابط ويستخدمونها الحكومات



الإختراق



المجموعات

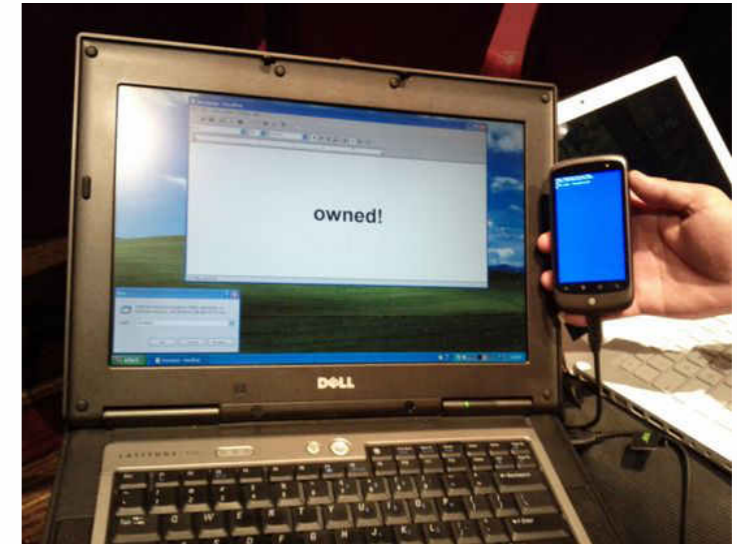
أنواع الإختراق؟

الأفراد



STC
الاتصالات السعودية

موبايلي
mobily



Ransomware

تشفير البيانات



Cryptographic Locker



30gb of personal documents and files on this computer or device have just been encrypted. Encrypted means you will not be able to access your files anymore, until they are decrypted. Your original files have been deleted, these can be recovered as described below. Click on "View encrypted files" to see a list of files that got encrypted.

The encryption was done with a unique generated encryption key (using AES-128). The only way to decrypt your files, is to obtain your private key and IV.

The private key, which will allow you to decrypt and get your original files back, is stored on our server. Each time the timer hits zero, the total costs will raise with the starting price.

To receive your private key, you need to pay the amount of bitcoin displayed left of this window (costs). You need to send the amount of bitcoins to the bitcoin address at the bottom of this window.

After the purchase is made, please wait a few minutes for confirmation of the bitcoins. After the bitcoins are confirmed, click the 'check payment and receive keys' button. Your keys will appear in the textboxes. After that, you simply click 'decrypt using keys', your files will be decrypted and restored to their original location.

You can easily delete this software, but know that without it, you will never be able to get your original files back.

For more information on how to buy and send bitcoin, click 'Next page'.

View encrypted files

Time until costs raise

18:12:42

Cost: 0.2 btc

Fee: 0 btc

Check payment and receive keys

Key: [] IV: []

Decrypt using keys

<< Previous Page

Next Page >>

Send bitcoins to this bitcoin address [] Copy

Last check: 2/9/2014 15:33:42

Ransomware



تشفير بيانات مستشفى!

45 bitcoins (about \$18,500)



A screenshot of a website interface. At the top, there is a navigation bar with a logo on the left and several menu items. Below the navigation bar, the main content area features a grid of four red buttons, each with white text. The buttons are arranged in two columns and two rows. The text on the buttons is partially legible but appears to be placeholder or generic text. Below each button, there are several lines of small, illegible text. The overall layout is clean and modern.

A screenshot of a video player. The video shows a man in a white shirt standing in front of a blue background with a white cross and the letters "US". The man is holding a small object in his hands. The video player has a blue border and a white title bar. The title bar contains the text "WIDE WORLD OF PHOTONICS". The video player is set against a blue background with a white cross and the letters "US".

@Castnology
www.castnology.com



10:28

#WannaCry

testfile.exe

Desert.jpg

Jellyfish.jpg

setup

Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

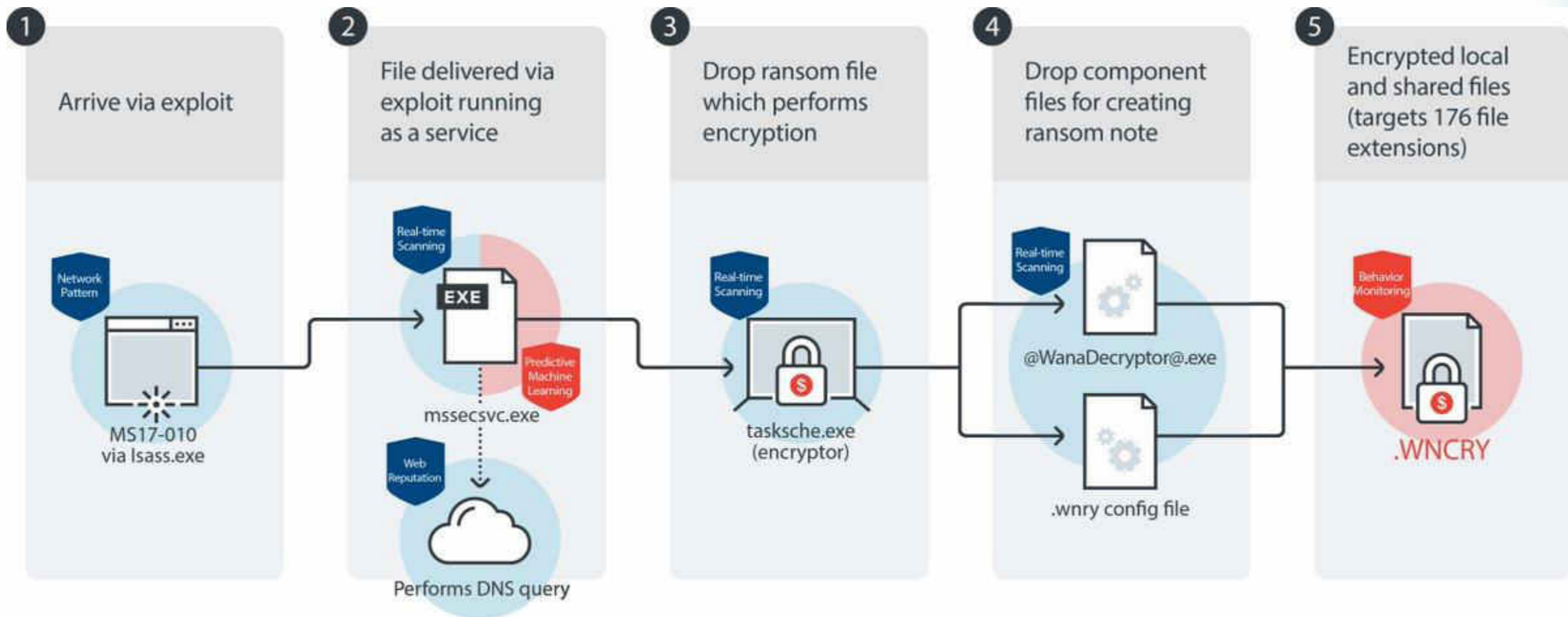
Payment will be raised on
5/18/2017 10:10:28
Time Left
02:23:59:45

Your files will be lost on
5/22/2017 10:10:28
Time Left
06:23:59:45

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

#WannaCry



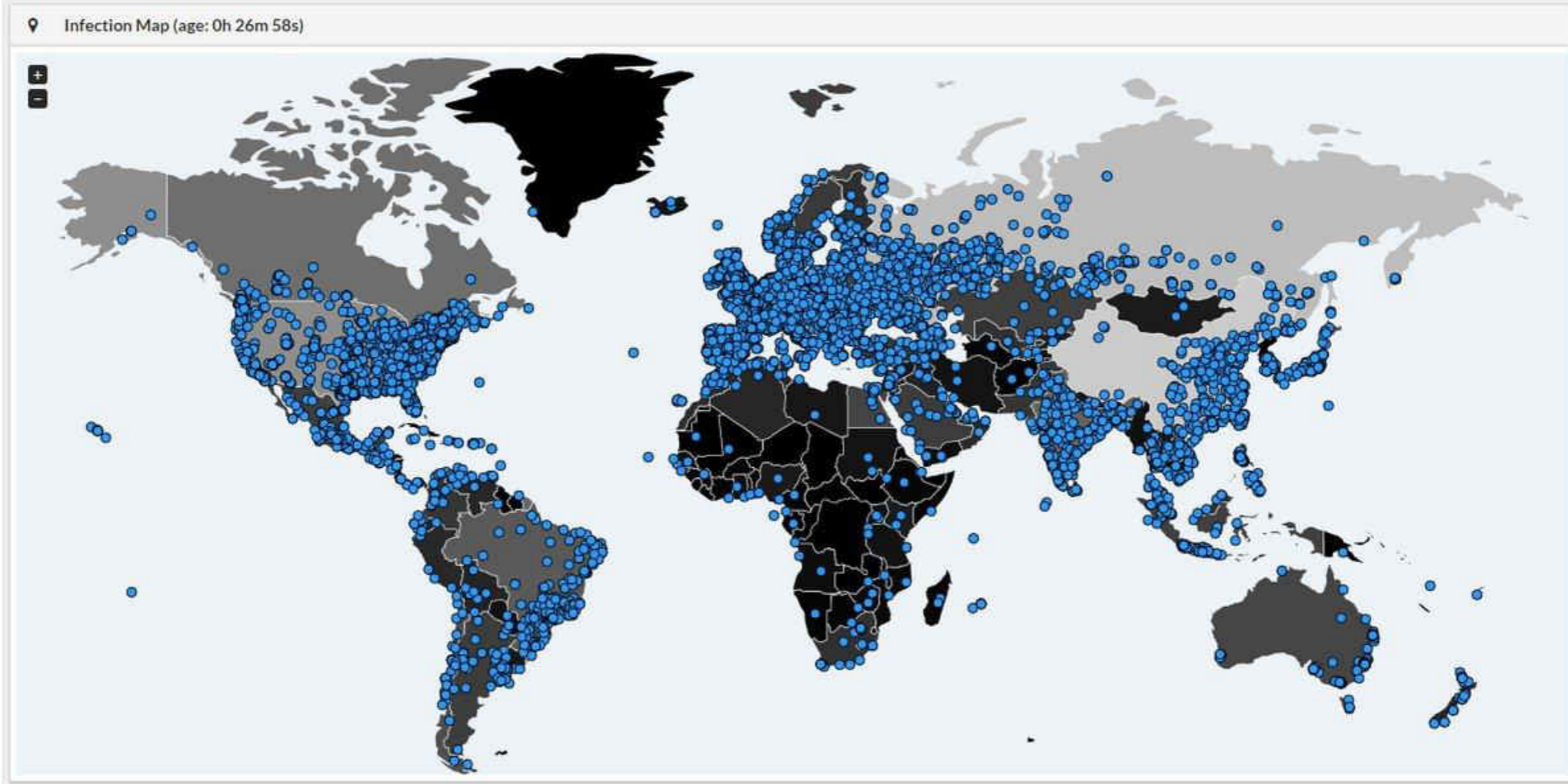
PROACTIVE PROTECTION
Behavior Monitoring
Predictive machine learning

ADDITIONAL SOLUTIONS
Network pattern
Real-time scanning
Web reputation





#WannaCry





#WannaCry

 **bitcoin**

1 Bitcoin equals

7264.04 Saudi Riyal

1	Bitcoin
7264.04	Saudi Riyal



الهندسة الاجتماعية



Phishing



Social Engineering



الهندسة الاجتماعية - أساليب متبعة



- نشر المعلومات البنكية أو الخاصة
- فتح الملفات الغير آمنة
- العلاقات المجهولة
- استغلال المواضيع الساخنة
- استغلال موضوع الأمن الرقمي وضعف
- الخبرة التقنية للضحية
- اصطياذ كلمات السر
- خيانة الثقة

- الرسائل المجهولة
- الدعايات الكاذبة
- المكالمات من مجهولين لتسجيل
- المعلومات
- البحث في المهملات
- استغلال عواطف الضحية
- استغلال الشائعات



الوقاية من الوقوع ضحية للهندسة الاجتماعية

● احرص على خصوصيتك وعدم نشر معلومات شخصية عن نفسك

● لا تشارك كلمة السرّ خاصتك مع الآخرين

● لا تشارك أسماء أو عناوين حساباتك مع غير المعنيين

● لا تثق بأحد

● أبقى حذرا طول الوقت

● تحقق من شخصية من يرأسك

● التحقق من المرفقات في الرسائل.

● في حال رغبتك بفتح أي ملف أو رابط





Insiders



Gmail™
by Google



حماية البيانات داخل المنظمات

أنظمة مكافحة
الفيروسات

التوعية الأمنية للموظفين



حماية البيانات داخل المنظمات

TechCampus



www.TechCampus.com



حماية البيانات داخل المنظمات

الكود الآمن

secure Source
Code

الاختبارات الأمنية للأنظمة

security penetration testing



 TM
closed source

VS

 TM
open source



حماية البيانات داخل المنظمات



تشفير البيانات (العملاء والموظفين) والبيانات المهمة



Encryption and Decryption.

Vormetric
Data Security

DATA LOCKER
SIMPLY SECURE

GOLD LOCKTM
MOBILE & CYBER SECURITY SOLUTIONS



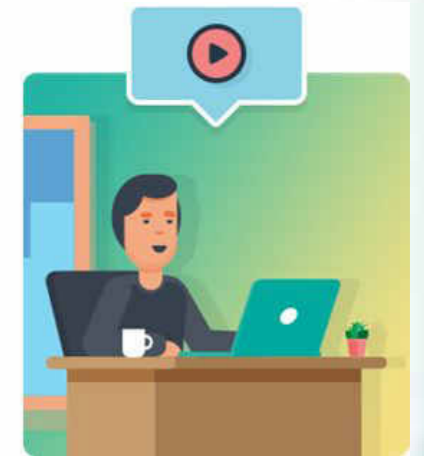
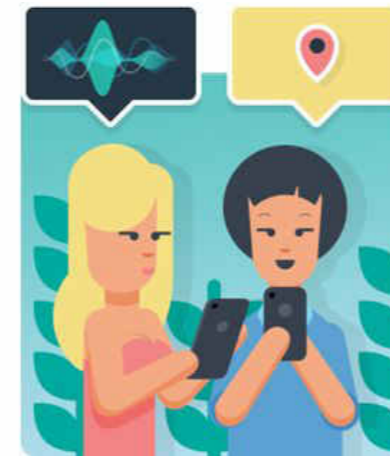
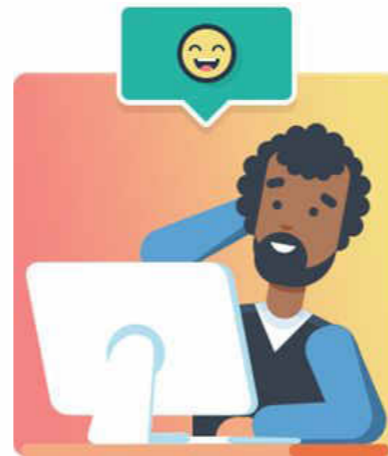
حماية البيانات داخل المنظمات

المحادثات الآمنة داخل المنظمات

تطبيق TrusteApp

هو تطبيق للهواتف الذكية مثل الايفون، الاندرويد، وايضا للويب، ومصمم للجهات الحكومية والشركات الخاصة وذلك لتبادل الرسائل والصور والفيديو والرسائل الصوتية بشكل آمن. تطبيق TrusteApp يوفر التشفير الكامل بين المستخدمين وايضا يطبق البصمة لإثبات التحقق الثنائي وايضا اثبات المصادقية بين المستخدمين. تطبيق TrusteApp يضمن أن الرسائل المتبادلة بين المستخدمين ترسل وتستقبل بسرية تامة وتكون محفوظة في قاعدة بيانات تلك الجهة.

<https://trusteapp.com/>



حماية البيانات داخل المنظمات

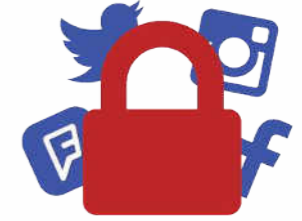
التأكد من تحديث الأنظمة باستمرار

النسخ الاحتياطية



حماية البيانات داخل المنظمات

الشبكات الاجتماعية والخصوصية



التحقق الثنائي



4ET%1ge6



1234



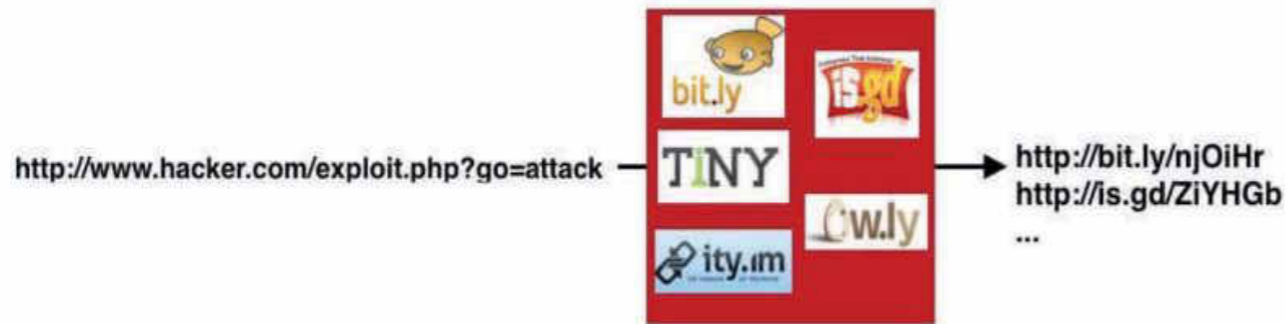
LastPass ****



حماية البيانات داخل المنظمات

عدم فتح الروابط المشبوهة من البريد

فحص USBs و اجهزة التخزين
قبل الإستخدام



يجب فحص الملف قبل تحميل المرفقات

 **virustotal**



مواقع تدعم التحقق الثنائي

Two Factor Auth (2FA)

List of websites and whether or not they support 2FA.

Add your own favorite site by submitting a pull request on the [GitHub repo](#).

Q Search websites



Backup and Sync



Banking



Cloud Computing



Communication



Cryptocurrencies



Developer



Domains



Education



Email



Entertainment



Finance



Food



Gaming



Government



Health

<https://twofactorauth.org/>





الإختراق الاخلاقي والأمن الإلكتروني

Ethical Hacking and Cyber Security



ياسر العصفير

@Alosefer



شكراً

