بسم اللّه 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
- اسئلة 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 والفلبين

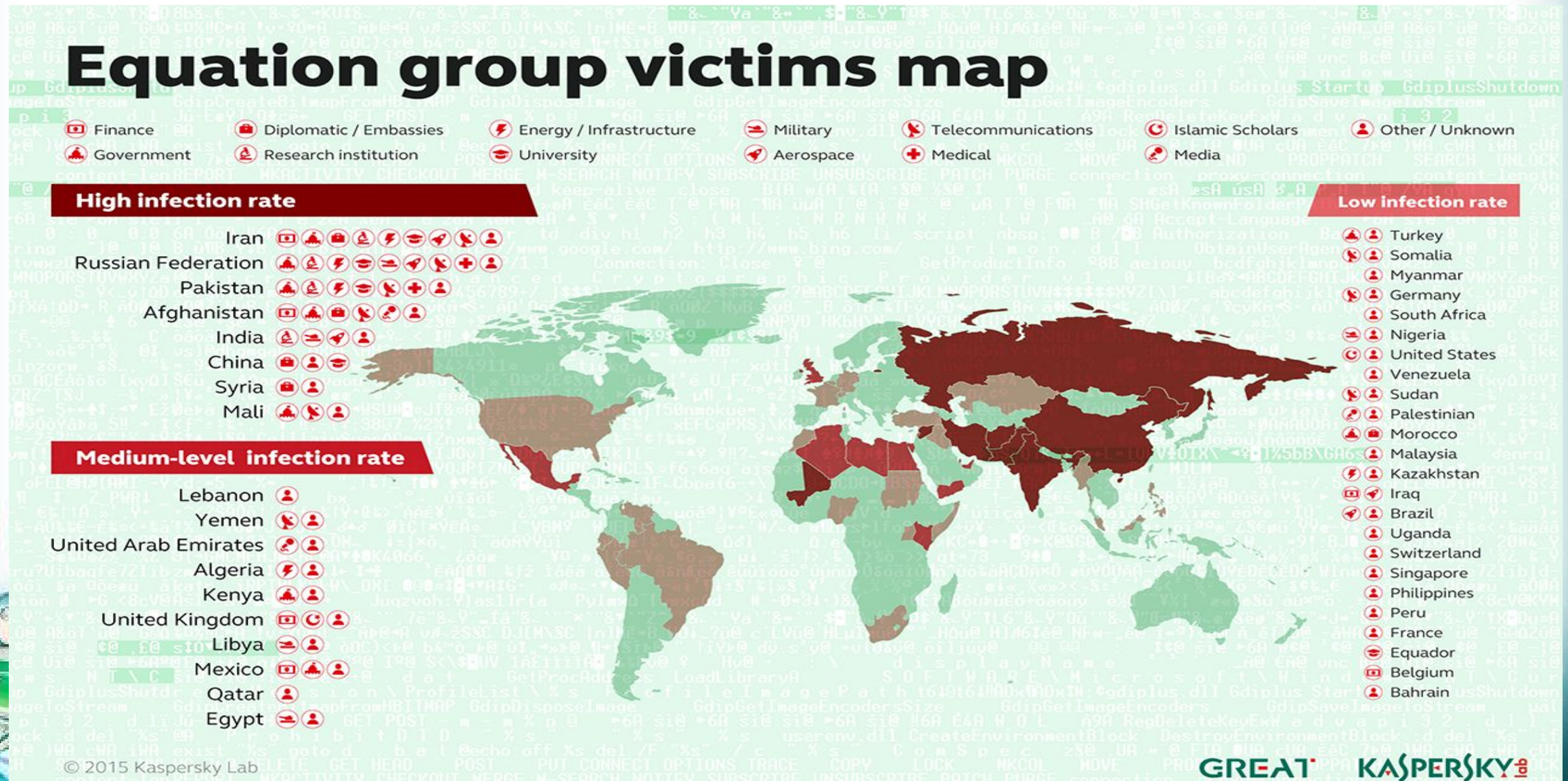
وغيرها بإجمالي سرقة =

٣٣٠ مليون ريال!

هل الحماية مهمة؟

وكالة الأمن القومي الأمريكية

Equation Group



هل الحماية مهمة؟

اختراق وكالة الأمن القومي الأمريكية!!

The Shadow Brokers

هل الحماية مهمة؟

ياهو YAHOO

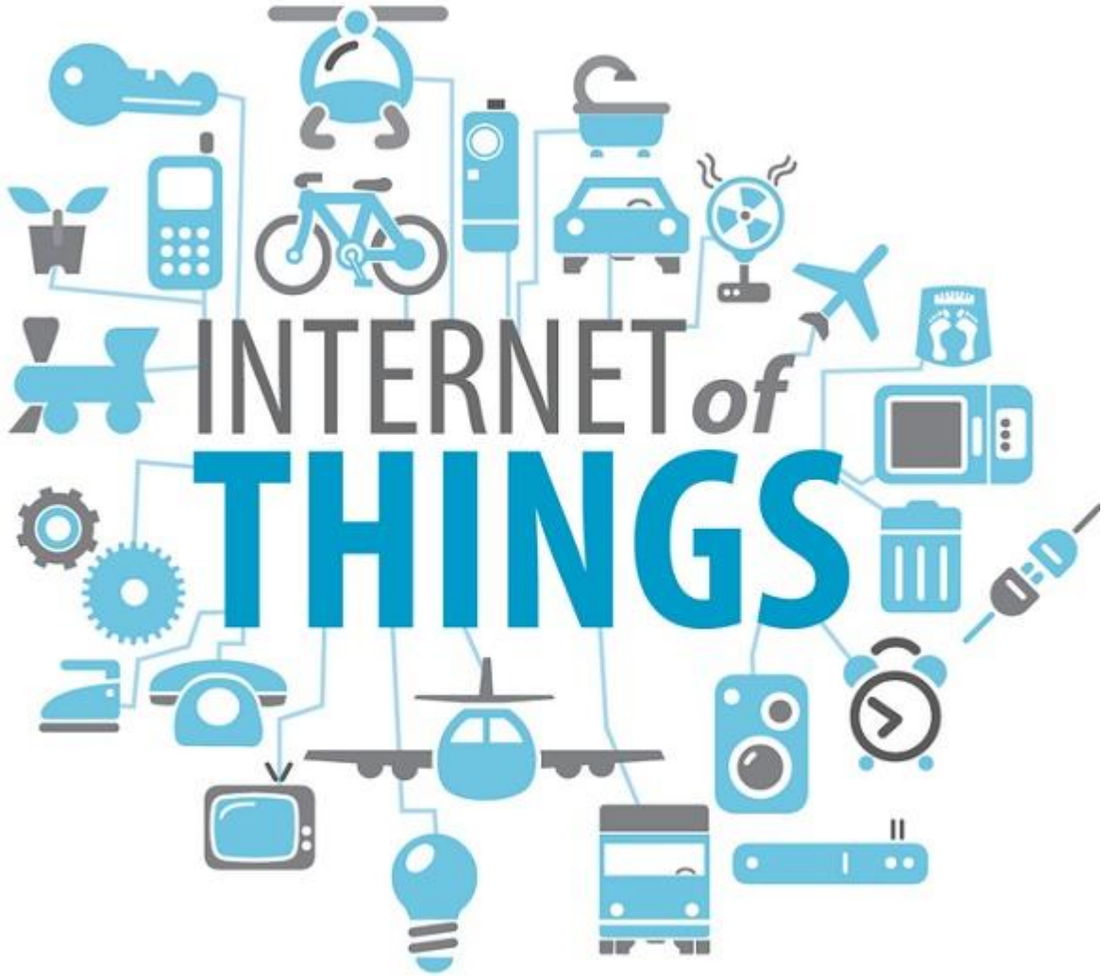
تسريب معلومات 500 مليون مستخدم،

والتنصت على الكل من NSA

هل الحماية مهمة؟

Dyn SM | DNS EMAIL LABS

The DYN DNS



SOUNDCLOUD

PayPal

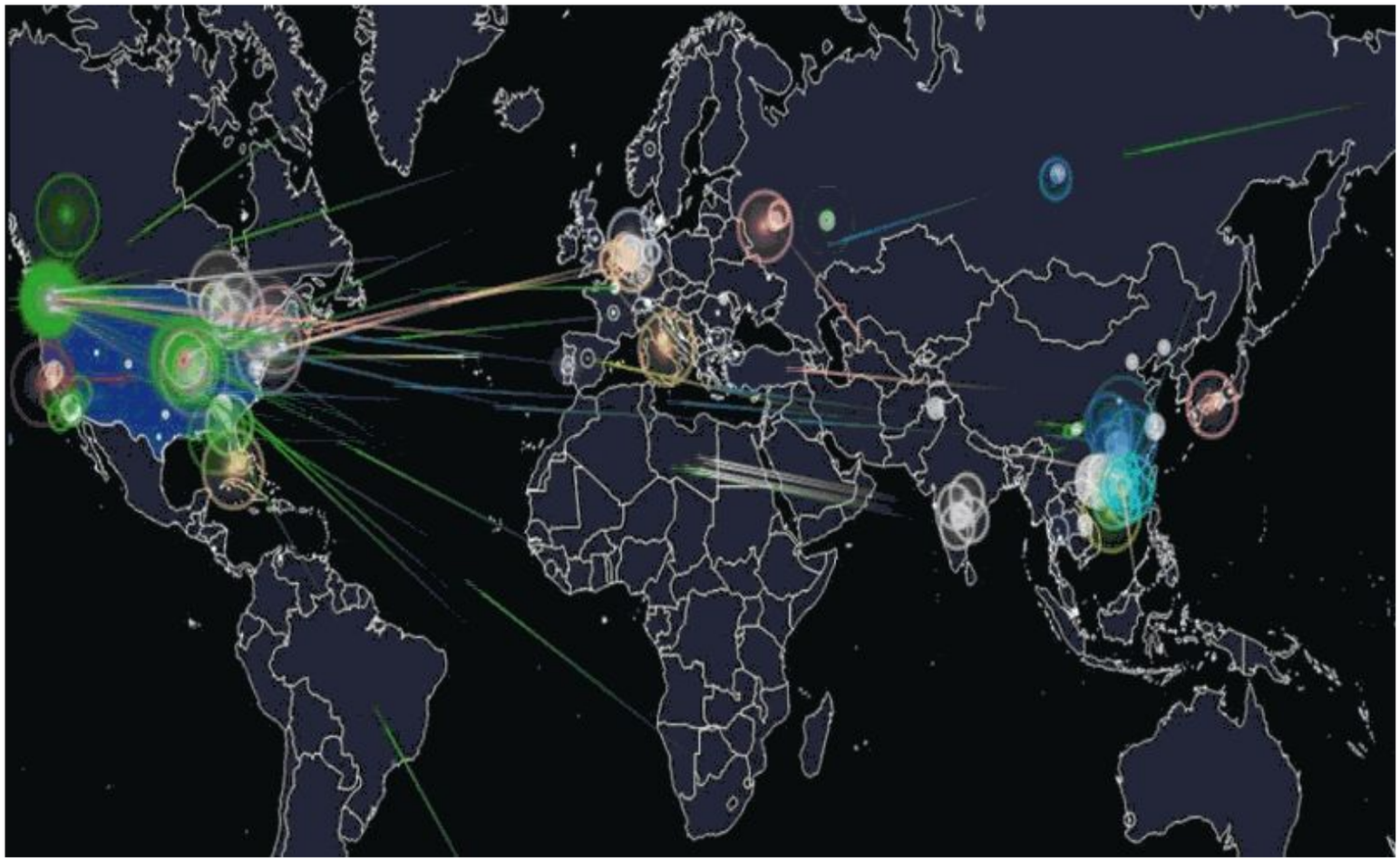
FOX NEWS .com

XBOX

هل الحماية مهمة؟

Dyn SM | DNS EMAIL LABS

The DYN DNS



هل الحماية مهمة؟

خسارة تقدر بـ $1.3 billion

SONY

You can download a part of Sony Pictures internal data the volume of which is tens of Terabytes on the following addresses.
These include many pieces of confidential data.

Cyberkendra.com

Password: diespe123

1. Torrent
http://ge.tt/[redacted]
http://rghost.net/[redacted]
http://rmdown.com/link.php?hash=143957d[redacted]
http://netload.in/dateiSwxiU7G1[redacted]

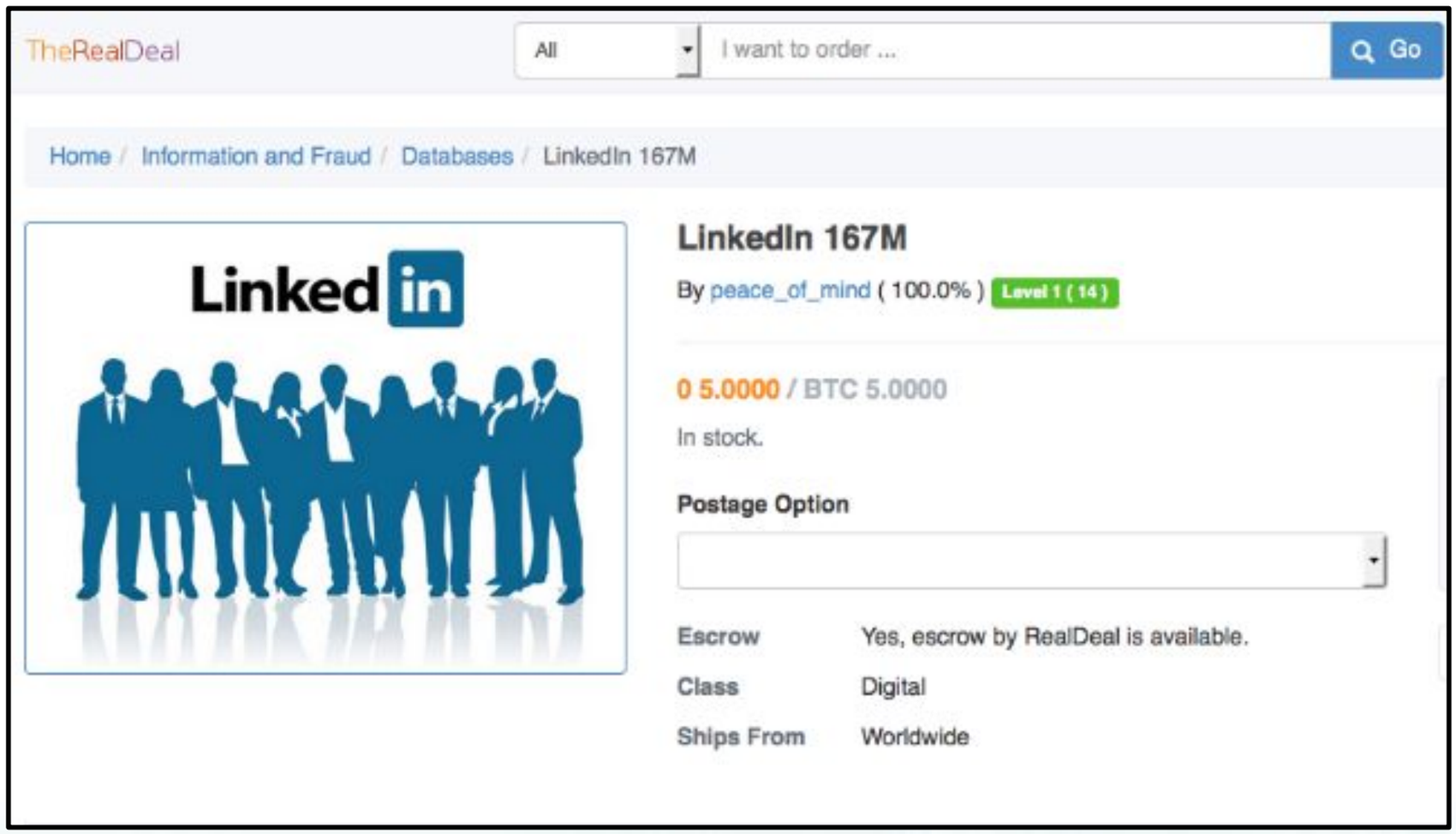
2. Mega
https://mega.co.nz/#!xdhhkTQZ!CKm[redacted]vn6A9bM_JY61WCxU
https://mega.co.nz/#!8VJQFQpA!ZpwA[redacted]DKBju4E7j7yvaLsU
https://mega.co.nz/#!dYZxzDYY!raWS[redacted]bueEjbMoywSH6DqU
https://mega.co.nz/#!NIpXXTZT!A64x[redacted]izhN9MIocNUDKN-I
https://mega.co.nz/#!AcA2WJCb!mtYw[redacted]GYJBQdL-I9R13MfU
https://mega.co.nz/#!9YI2xJAY!wgGT[redacted]Xo2IYWtHN4axU1aY
https://mega.co.nz/#!NIIWnTCQ!reJI[redacted]20WU9Tm4HF9Us9-g
https://mega.co.nz/#!hUh0gLYB!gDwn[redacted]raSZ8tqZblsnkr44
https://mega.co.nz/#!pVYBXLiB!k7es[redacted]HiHiIEk6uNOTybS8
https://mega.co.nz/#!sUZjEBBI!FsaY[redacted]x_Um2-xaIOQ1HUIg
https://mega.co.nz/#!VR4mVTSZ!vP-x[redacted]Y0OPxGz5zWA3f_Hw
https://mega.co.nz/#!xFQmhCaD!NWCd[redacted]zhB3dDDo700FUV5U
https://mega.co.nz/#!4JBR1DAT!woCz[redacted]A1ZO3RwuN3yqRzcA
https://mega.co.nz/#!EAJgSaSR!yAG5[redacted]RHcz7hmM81G0VLwI
https://mega.co.nz/#!UQJyTKZY!AUMw[redacted]6iVCka-icwdPr9WE
https://mega.co.nz/#!8Ap2FS4B!eR_d[redacted]DPnF7ub1dFy_nlgw
https://mega.co.nz/#!lIABABgR!cCuQ[redacted]gQsatrJkKAXwOISA
https://mega.co.nz/#!0NJRkSrD!Fcs8[redacted]q8uRiJa_hGqoW-h8
https://mega.co.nz/#!5RYmxbRD!i8Lx[redacted]_YfTDW1wYOho1O9U
https://mega.co.nz/#!VVZ3BBqC!2goJ[redacted]Nsn5Vc3UpU6mgx8Y

Cyberkendra.com

هل الحماية مهمة؟

لينكدان Linkedin

117 Million Users

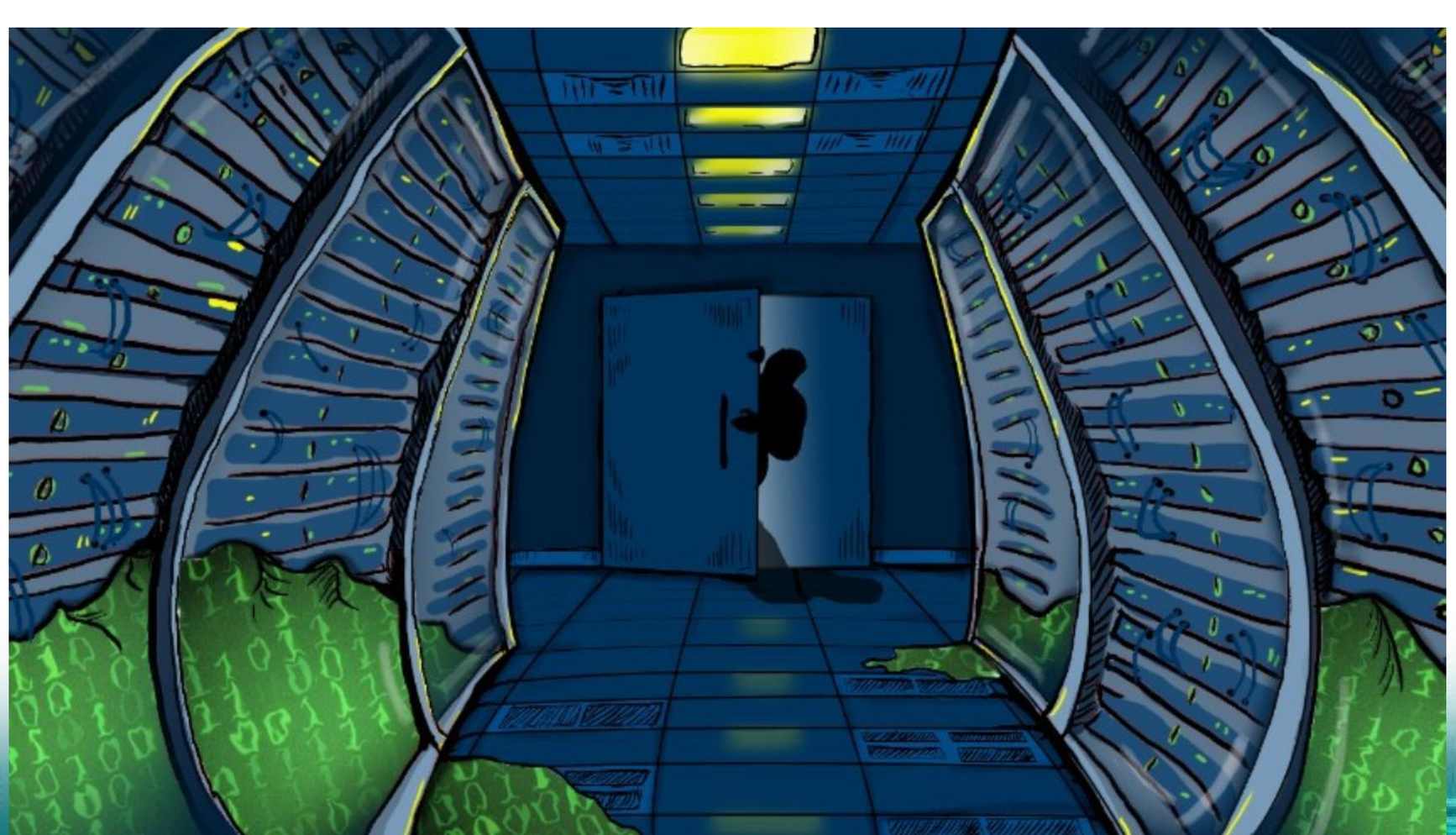


هل الحماية مهمة؟

دروب بوكس Dropbox

69 Million Accounts

Passwords+Info



وثائق ـ 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

خارجي

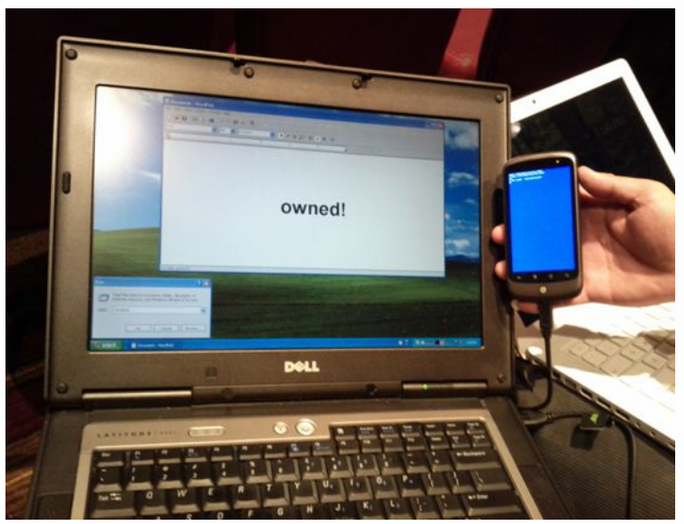
- الإنترنت، وهي الأغلب والأكثر وطرق إختراق الكثير من إختراقات الحرب الإلكترونية او الشخصية، عن طريق:
  - البريد
  - زيارة موقع
  - تحميل برنامج
  - قبول إضافة غير معروفة وقبول ملف او رابط ويستخدمونها الحكومات

الإختراق

أنواع الإختراق؟

الأفراد

المجموعات



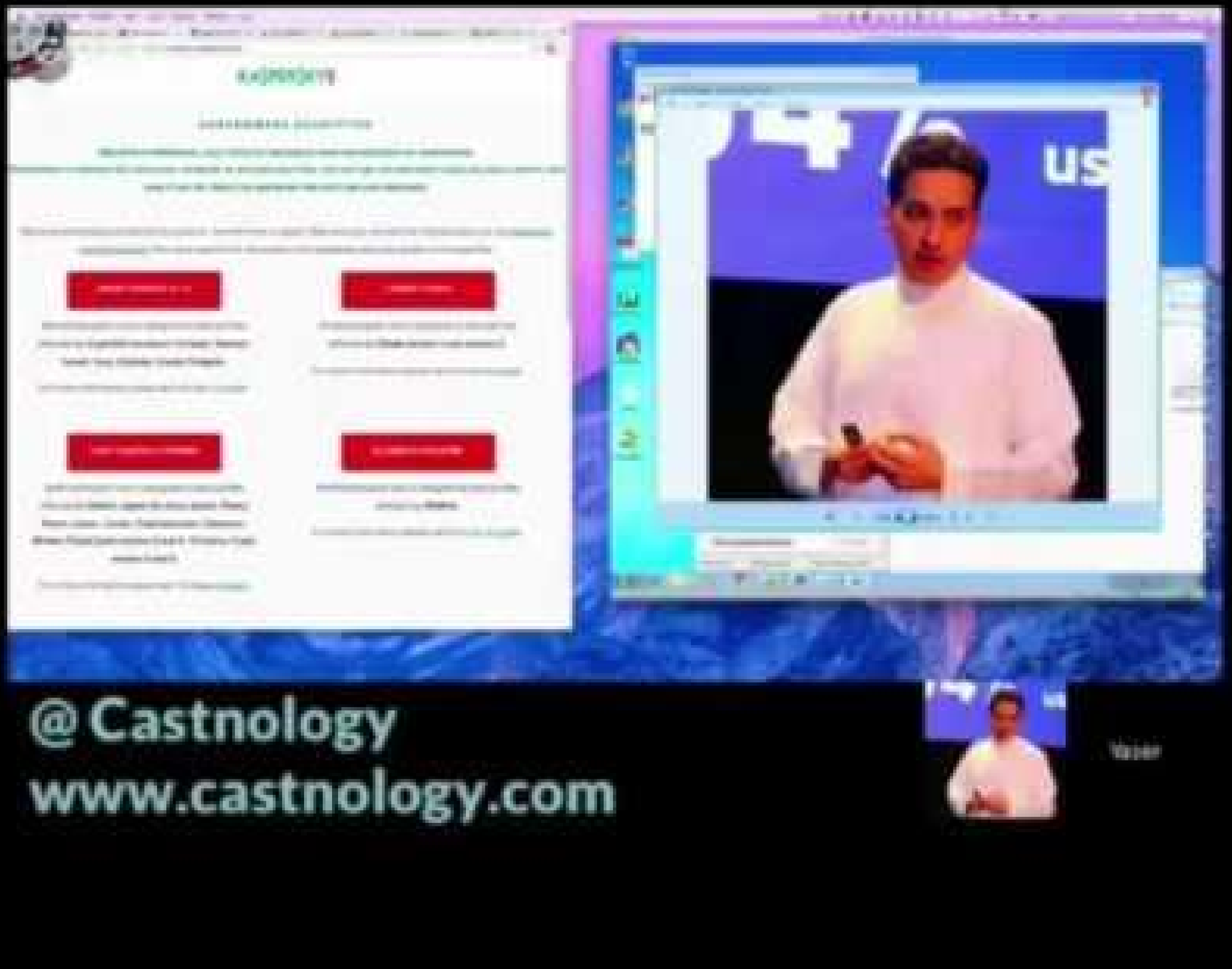
Ransomware

تشفير البيانات

Ransomware

تشفير بيانات مستشفى!

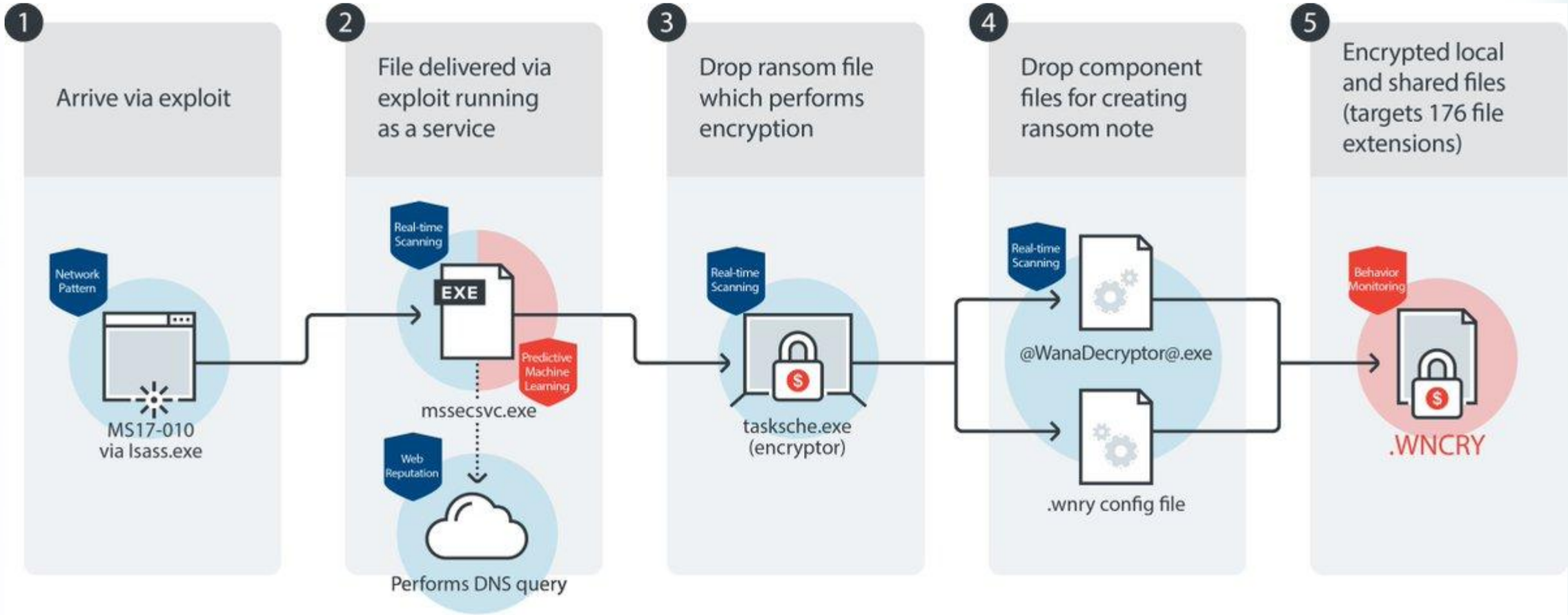
45 bitcoins (about $18,500)


@Castnology
www.castnology.com

#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
Payment will be raised on
5/18/2017 10:10:28
Time Left
02:23:59:46
Your files will be lost on
5/22/2017 10:10:28
Time Left
06:23:59:46
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

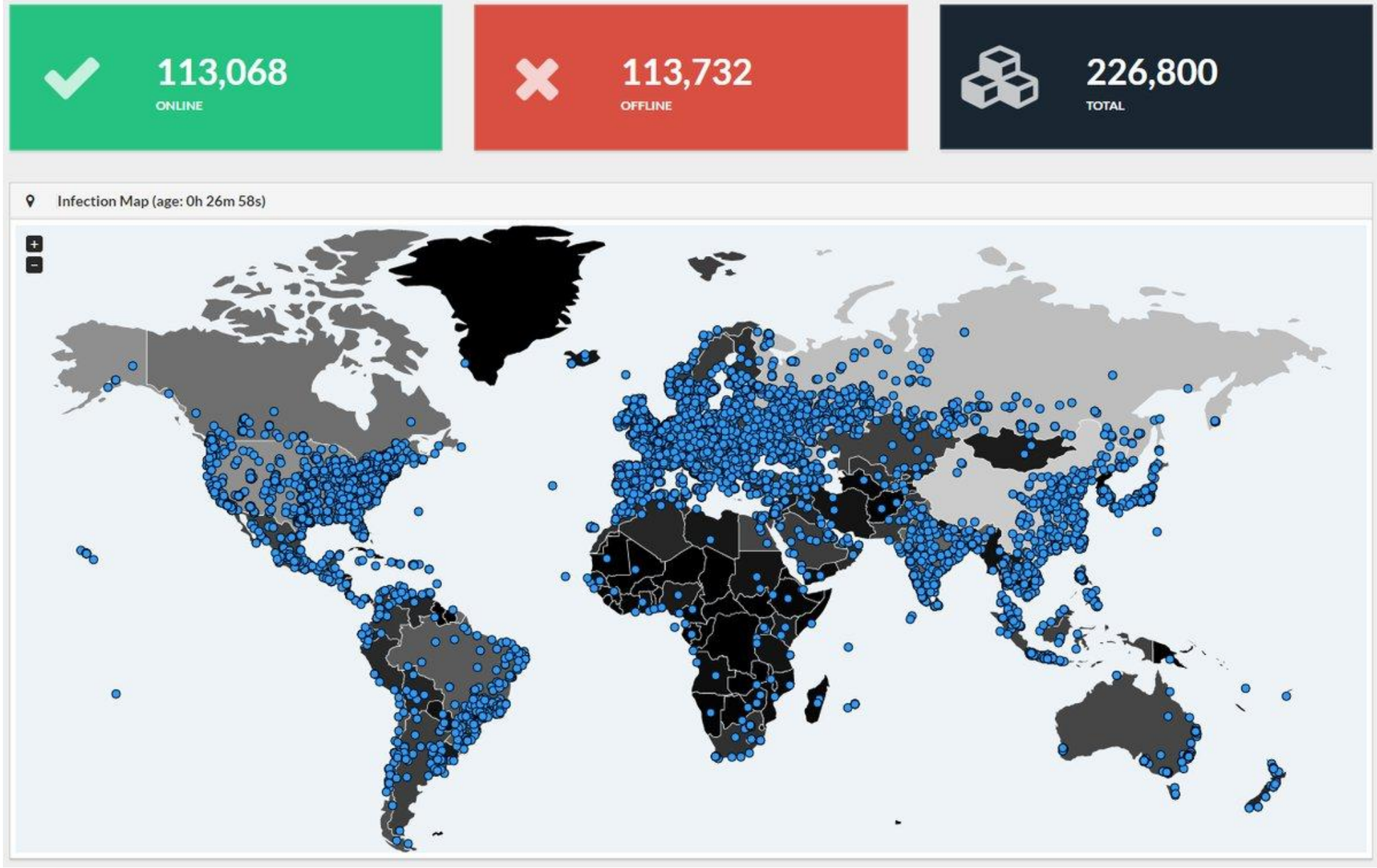
#WannaCry



PROACTIVE PROTECTION
Behavior Monitoring
Predictive machine learning

ADDITIONAL SOLUTIONS
Network pattern
Real-time scanning
Web reputation

#WannaCry


113,068
ONLINE
113,732
OFFLINE
226,800
TOTAL
Infection Map (age: 0h 26m 58s)

#WannaCry

bitcoin

1 Bitcoin equals

7264.04 Saudi Riyal

1	Bitcoin
7264.04	Saudi Riyal

الهندسة الاجتماعية

Social Engineering

الهندسة الاجتماعية - أساليب متبعة

- الرسائل المجهولة
- الدعايات الكاذبة
- المكالمات من مجهولين لتسجيل المعلومات
- البحث في المهملات
- استغلال عواطف الضحية
- استغلال الشائعات
- نشر المعلومات البنكية أو الخاصة
- فتح الملفات الغير آمنة
- العلاقات المجهولة
- استغلال المواضيع الساخنة
- استغلال موضوع الأمن الرقمي وضعف الخبرة التقنية للضحية
- اصطياد كلمات السر
- خيانة الثقة

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 يراسلك
- التحقق من المرفقات في الرسائل.
- في حال رغبتك بفتح أي ملف أو رابط

Insiders

Gmail™ by Google

حماية البيانات داخل المنظمات

التوعية الأمنية للموظفين

أنظمة مكافحة الفيروسات

حماية البيانات داخل المنظمات

TechCampus

www.TechCampus.com

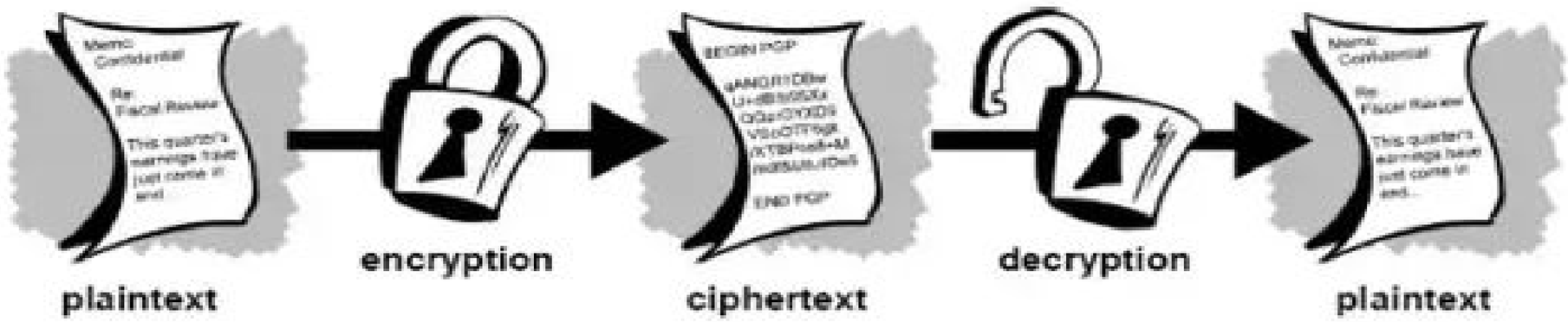
حماية البيانات داخل المنظمات

الكود الآمن
secure Source Code

الاختبارات الأمنية للأنظمة
security penetration testing

حماية البيانات داخل المنظمات

تشفير البيانات (العملاء والموظفين) والبيانات المهمة



Encryption and Decryption.

Vormetric
Data Security

DATALOCKER®
SIMPLY SECURE

GOLD LOCK™
MOBILE & CYBER SECURITY SOLUTIONS

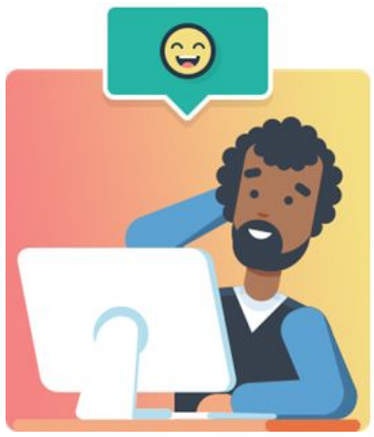
حماية البيانات داخل المنظمات

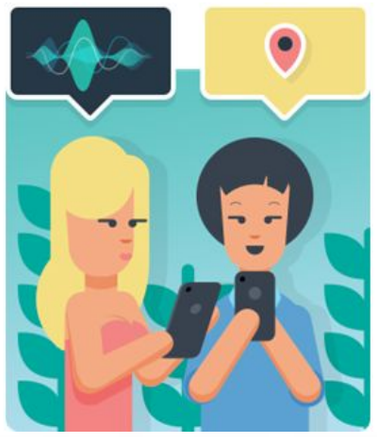
المحادثات الآمنة داخل المنظمات

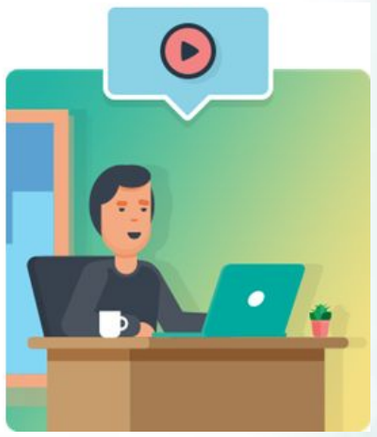
تطبيق TrusteApp

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 المصداقية 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

النسخ الإحتياطية

التأكد من تحديث الأنظمة بإستمرار

حماية البيانات داخل المنظمات

الشبكات الاجتماعية والخصوصية

التحقق الثنائي

4ET%1ge6 ✓

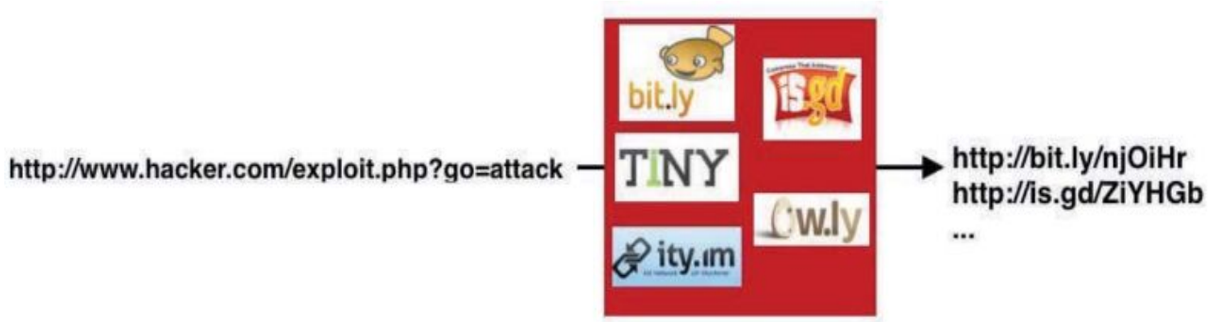
1234 ✗

LastPass ****

حماية البيانات داخل المنظمات

فحص USBs و اجهزة التخزين قبل الإستخدام

عدم فتح الروابط المشبوهة من البريد



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.

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 العصيفير

@Alosefer

شكراً 🤓