Cyber 4.0

Kovelin Naidoo

LAY OF THE LAND

> THOSE WHO DO NOT KNOW THE PLANS OF COMPETITORS CANNOT PREPARE ALLIANCES. THOSE WHO DO NOT KNOW THE LAY OF THE LAND CANNOT MANEUVER THEIR FORCES. THOSE WHO DO NOT USE LOCAL GUIDES CANNOT TAKE ADVANTAGE OF THE GROUND.

SUN TZU

> “I’M HERE TO TELL YOU THAT YOUR CYBER SYSTEMS CONTINUE TO FUNCTION AND SERVE YOU NOT DUE TO THE EXPERTISE OF YOUR SECURITY STAFF BUT SOLELY DUE TO THE SUFFERANCE OF YOUR OPPONENTS.

Brian Snow, 2012.
Head of Information Assurance NSA

STANDARD BANK COMPUTER WAS HACKED IN R300m ATM FRAUD HIT - report

2016-06-30 11:03
Gareth van Zyl, Fin24

TWO GHANAIANS ARRESTED FOR ALLEGEDLY HACKING BANK ACCOUNTS

According to the police, the syndicate transferred money from its coffers to the personal accounts of some other customers. Afterwards, they connived with the customers to withdraw the money.

2016-10-21
Kwasi Gyamfi Asiedu

KENYA REVENUE AUTHORITY 'LOST $39m TO HACKER'

ORGANISED CRIME

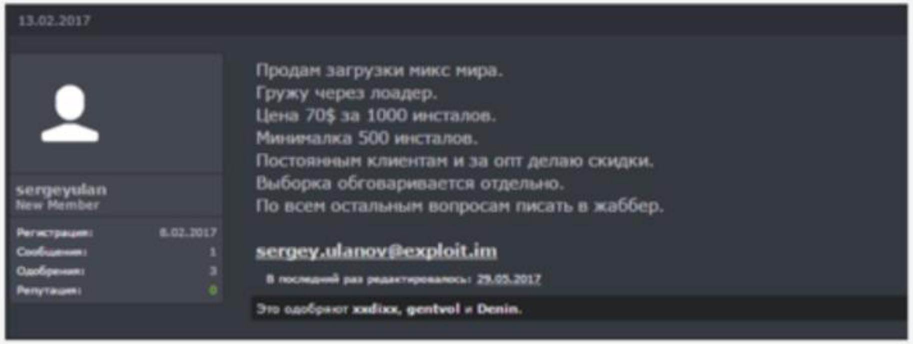
Background + Context

World’s first encrypted wireless Communication network

Real world innovation:
Narco submarines
8 tons on board minimum

NEXT GENERATION MALWARE

PAY-PER-INSTALL



13.02.2017

sergeyulan
New Member

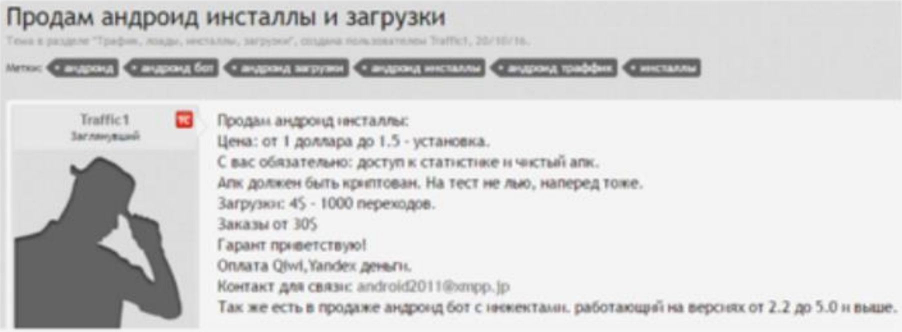
Регистрация:	8.02.2017
Сообщения:	1
Одобрения:	3
Репутация:	0

Продам загрузки микс мира.
Гружу через лоадер.
Цена 70$ за 1000 инсталов.
Минималка 500 инсталов.
Постоянным клиентам и за опт делаю скидки.
Выборка обговаривается отдельно.
По всем остальным вопросам писать в жаббер.

sergey.ulanov@exploit.im

В последний раз редактировалось: 29.05.2017

Это одобряют xxdixx, gentvol и Denin.



Продам андроид инсталлы и загрузки

Тема в разделе "Трафик, лоады, инсталлы, загрузки", создана пользователем Traffic1, 20/10/16.

Метки: андроид · андроид бот · андроид загрузки · андроид инсталлы · андроид траффик · инсталлы

Traffic1
Заглянувший

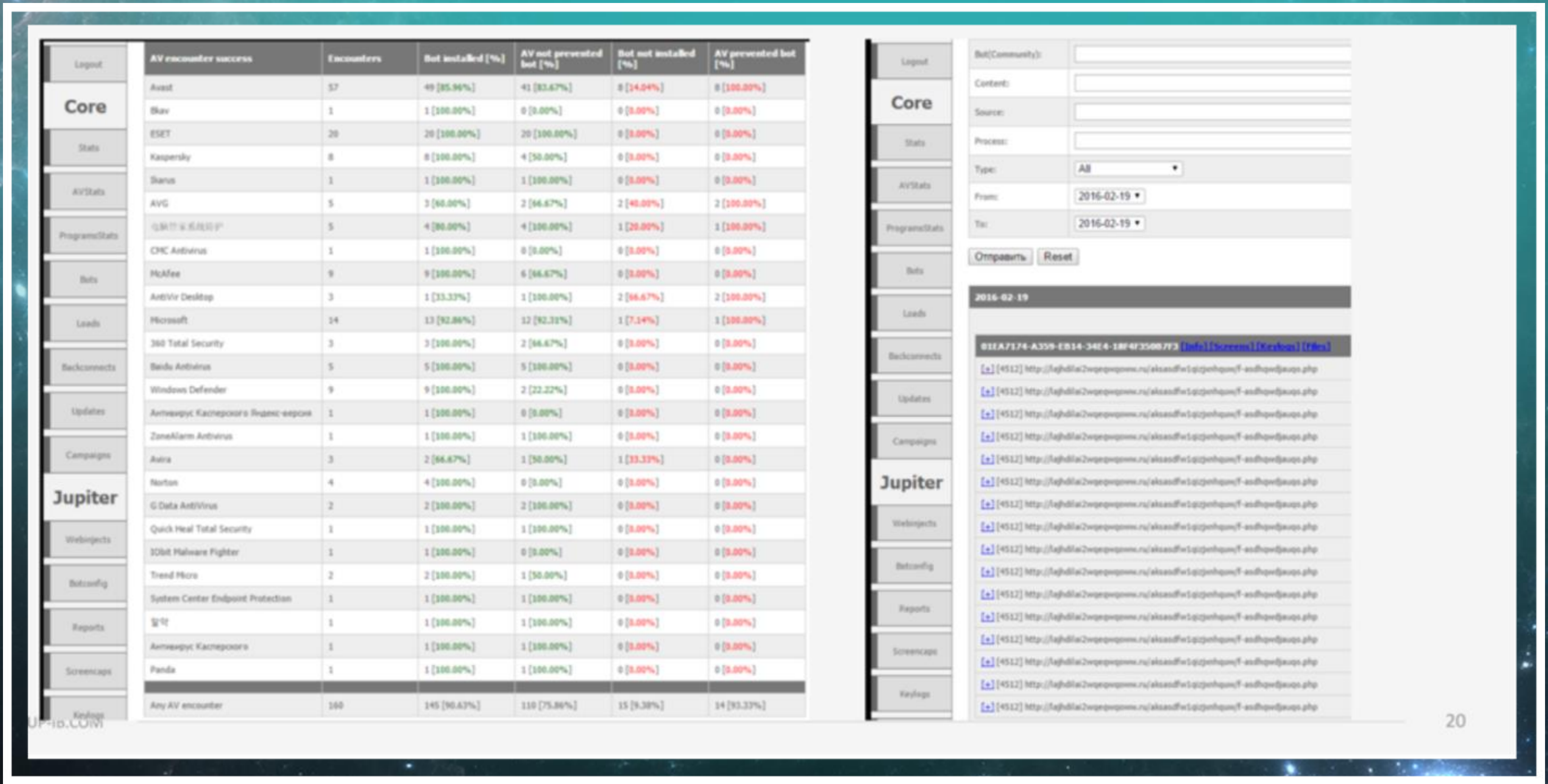
Продам андроид инсталлы:
Цена: от 1 доллара до 1.5 - установка.
С вас обязательно: доступ к статистике и чистый апк.
Апк должен быть криптован. На тест не лью, наперед тоже.
Загрузки: 4$ - 1000 переходов.
Заказы от 30$
Гарант приветствую!
Оплата Qiwi,Yandex деньги.
Контакт для связи: android2011@xmpp.jp
Так же есть в продаже андроид бот с инжектами. работающий на версиях от 2.2 до 5.0 и выше.

Selling mix world downloads.
Loads through the loader.
The price is 70 $ for 1000 installs.
Minimal 500 installations.
To regular customers and for wholesale I make discounts.
The sample is negotiated separately.
For all other questions, write to the jabber.

Sergey.ulanov@exploit.im

Selling android installations:
Price: from 1 dollar to 1.5 - installation.
With you it is necessary: access to statistics and clean apk.
The apk must be crypted. On the test I do not pour, in advance, too.
Downloads: $ 4 - 1000 conversions.
Orders from $ 30
Garant greetings!
Payment Qiwi, Yandex money.
Contact for communication: android2011@xmpp.jp
There is also an android bot with injections on sale. Working on versions from 2.2 to 5.0 and higher.

MALWARE ASSURANCE



AV encounter success	Encounters	Bot installed [%]	AV not prevented bot [%]	Bot not installed [%]	AV prevented bot [%]
Avast	57	49 [85.96%]	41 [83.67%]	8 [14.04%]	8 [100.00%]
Bkav	1	1 [100.00%]	0 [0.00%]	0 [0.00%]	0 [0.00%]
ESET	20	20 [100.00%]	20 [100.00%]	0 [0.00%]	0 [0.00%]
Kaspersky	8	8 [100.00%]	4 [50.00%]	0 [0.00%]	0 [0.00%]
Ikarus	1	1 [100.00%]	1 [100.00%]	0 [0.00%]	0 [0.00%]
AVG	5	3 [60.00%]	2 [66.67%]	2 [40.00%]	2 [100.00%]
[illegible]	5	4 [80.00%]	4 [100.00%]	1 [20.00%]	1 [100.00%]
CMC Antivirus	1	1 [100.00%]	0 [0.00%]	0 [0.00%]	0 [0.00%]
McAfee	9	9 [100.00%]	6 [66.67%]	0 [0.00%]	0 [0.00%]
AntiVir Desktop	3	1 [33.33%]	1 [100.00%]	2 [66.67%]	2 [100.00%]
Microsoft	14	13 [92.86%]	12 [92.31%]	1 [7.14%]	1 [100.00%]
360 Total Security	3	3 [100.00%]	2 [66.67%]	0 [0.00%]	0 [0.00%]
Baidu Antivirus	5	5 [100.00%]	5 [100.00%]	0 [0.00%]	0 [0.00%]
Windows Defender	9	9 [100.00%]	2 [22.22%]	0 [0.00%]	0 [0.00%]
Антивирус Касперского Яндекс-версия	1	1 [100.00%]	0 [0.00%]	0 [0.00%]	0 [0.00%]
ZoneAlarm Antivirus	1	1 [100.00%]	1 [100.00%]	0 [0.00%]	0 [0.00%]
Avira	3	2 [66.67%]	1 [50.00%]	1 [33.33%]	0 [0.00%]
Norton	4	4 [100.00%]	0 [0.00%]	0 [0.00%]	0 [0.00%]
G Data AntiVirus	2	2 [100.00%]	2 [100.00%]	0 [0.00%]	0 [0.00%]
Quick Heal Total Security	1	1 [100.00%]	1 [100.00%]	0 [0.00%]	0 [0.00%]
IObit Malware Fighter	1	1 [100.00%]	0 [0.00%]	0 [0.00%]	0 [0.00%]
Trend Micro	2	2 [100.00%]	1 [50.00%]	0 [0.00%]	0 [0.00%]
System Center Endpoint Protection	1	1 [100.00%]	1 [100.00%]	0 [0.00%]	0 [0.00%]
알약	1	1 [100.00%]	1 [100.00%]	0 [0.00%]	0 [0.00%]
Антивирус Касперского	1	1 [100.00%]	1 [100.00%]	0 [0.00%]	0 [0.00%]
Panda	1	1 [100.00%]	1 [100.00%]	0 [0.00%]	0 [0.00%]
Any AV encounter	160	145 [90.63%]	110 [75.86%]	15 [9.38%]	14 [93.33%]

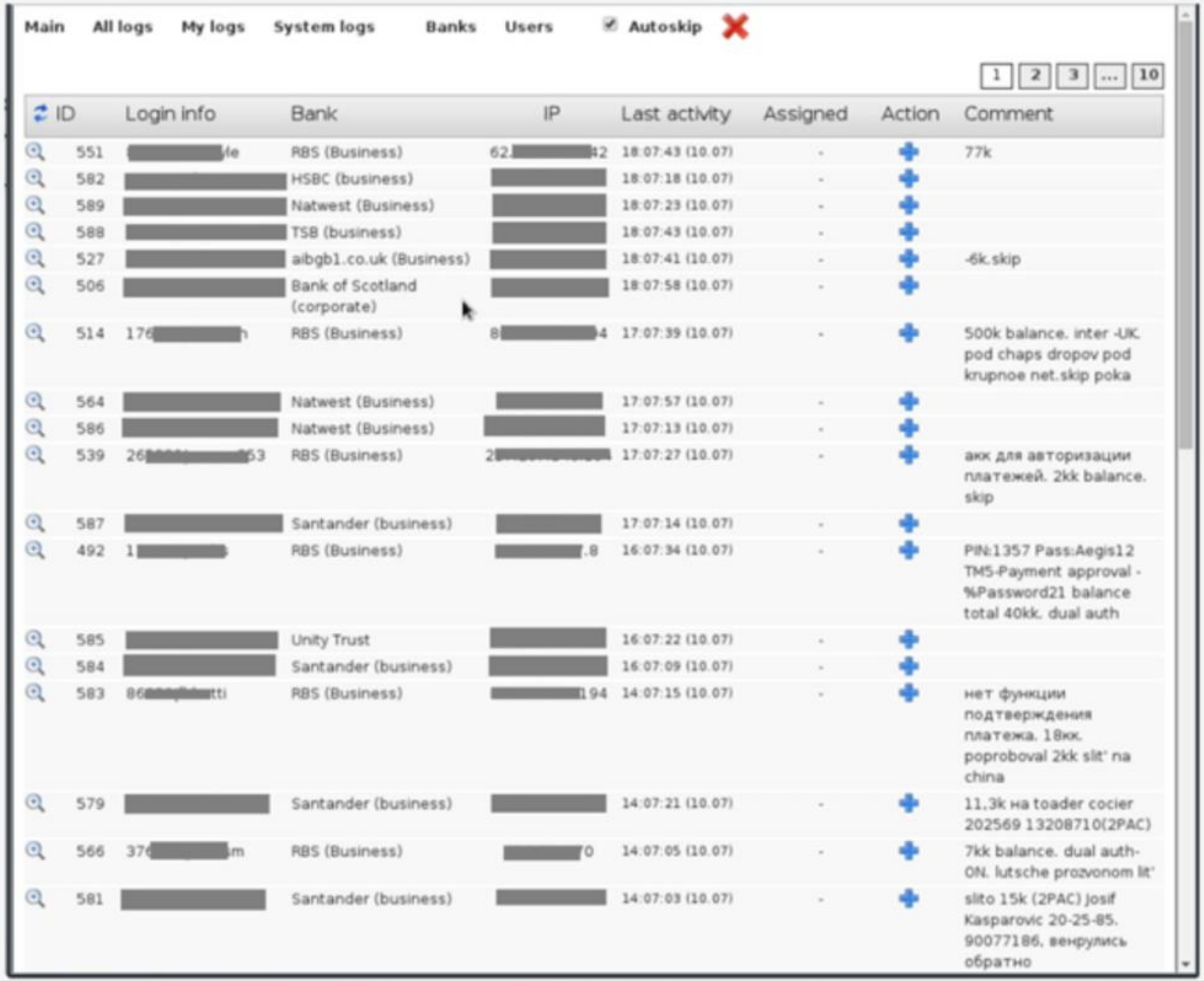
Bot(Community):	
Content:	
Source:	
Process:	
Type:	All ▾
From:	2016-02-19 ▾
To:	2016-02-19 ▾

2016-02-19

01EA7174-A359-EB14-34E4-18F4F35087F3 [Info] [Screens] [Keylogs] [Files]

```
[+] [4512] http://lajhdilai2wqeqwqoww.ru/aksasdfw1qizjenhquwf-asdhqwdjauqs.php
[+] [4512] http://lajhdilai2wqeqwqoww.ru/aksasdfw1qizjenhquwf-asdhqwdjauqs.php
[+] [4512] http://lajhdilai2wqeqwqoww.ru/aksasdfw1qizjenhquwf-asdhqwdjauqs.php
[+] [4512] http://lajhdilai2wqeqwqoww.ru/aksasdfw1qizjenhquwf-asdhqwdjauqs.php
[+] [4512] http://lajhdilai2wqeqwqoww.ru/aksasdfw1qizjenhquwf-asdhqwdjauqs.php
[+] [4512] http://lajhdilai2wqeqwqoww.ru/aksasdfw1qizjenhquwf-asdhqwdjauqs.php
[+] [4512] http://lajhdilai2wqeqwqoww.ru/aksasdfw1qizjenhquwf-asdhqwdjauqs.php
[+] [4512] http://lajhdilai2wqeqwqoww.ru/aksasdfw1qizjenhquwf-asdhqwdjauqs.php
[+] [4512] http://lajhdilai2wqeqwqoww.ru/aksasdfw1qizjenhquwf-asdhqwdjauqs.php
[+] [4512] http://lajhdilai2wqeqwqoww.ru/aksasdfw1qizjenhquwf-asdhqwdjauqs.php
[+] [4512] http://lajhdilai2wqeqwqoww.ru/aksasdfw1qizjenhquwf-asdhqwdjauqs.php
[+] [4512] http://lajhdilai2wqeqwqoww.ru/aksasdfw1qizjenhquwf-asdhqwdjauqs.php
[+] [4512] http://lajhdilai2wqeqwqoww.ru/aksasdfw1qizjenhquwf-asdhqwdjauqs.php
[+] [4512] http://lajhdilai2wqeqwqoww.ru/aksasdfw1qizjenhquwf-asdhqwdjauqs.php
[+] [4512] http://lajhdilai2wqeqwqoww.ru/aksasdfw1qizjenhquwf-asdhqwdjauqs.php
[+] [4512] http://lajhdilai2wqeqwqoww.ru/aksasdfw1qizjenhquwf-asdhqwdjauqs.php
```

BUSINESS INTELLIGENCE VALUE ADD



ID	Login info	Bank	IP	Last activity	Assigned	Action	Comment
551	[redacted]le	RBS (Business)	62.[redacted]42	18:07:43 (10.07)	-	✚	77k
582	[redacted]	HSBC (business)	[redacted]	18:07:18 (10.07)	-	✚	
589	[redacted]	Natwest (Business)	[redacted]	18:07:23 (10.07)	-	✚	
588	[redacted]	TSB (business)	[redacted]	18:07:43 (10.07)	-	✚	
527	[redacted]	aibgb1.co.uk (Business)	[redacted]	18:07:41 (10.07)	-	✚	-6k.skip
506	[redacted]	Bank of Scotland (corporate)	[redacted]	18:07:58 (10.07)	-	✚	
514	176[redacted]h	RBS (Business)	8[redacted]4	17:07:39 (10.07)	-	✚	500k balance. inter -UK. pod chaps dropov pod krupnoe net.skip poka
564	[redacted]	Natwest (Business)	[redacted]	17:07:57 (10.07)	-	✚	
586	[redacted]	Natwest (Business)	[redacted]	17:07:13 (10.07)	-	✚	
539	26[redacted]53	RBS (Business)	2[redacted]	17:07:27 (10.07)	-	✚	акк для авторизации платежей. 2kk balance. skip
587	[redacted]	Santander (business)	[redacted]	17:07:14 (10.07)	-	✚	
492	1[redacted]	RBS (Business)	[redacted].8	16:07:34 (10.07)	-	✚	PIN:1357 Pass:Aegis12 TMS-Payment approval - %Password21 balance total 40kk. dual auth
585	[redacted]	Unity Trust	[redacted]	16:07:22 (10.07)	-	✚	
584	[redacted]	Santander (business)	[redacted]	16:07:09 (10.07)	-	✚	
583	86[redacted]tti	RBS (Business)	[redacted]194	14:07:15 (10.07)	-	✚	нет функции подтверждения платежа. 18кк. poproboval 2kk slit' na china
579	[redacted]	Santander (business)	[redacted]	14:07:21 (10.07)	-	✚	11,3k на toader cocier 202569 13208710(2PAC)
566	37[redacted]m	RBS (Business)	[redacted]0	14:07:05 (10.07)	-	✚	7kk balance. dual auth-ON. lutsche prozvonom lit'
581	[redacted]	Santander (business)	[redacted]	14:07:03 (10.07)	-	✚	slito 15k (2PAC) Josif Kasparovic 20-25-85. 90077186. венрулись обратно

Balance is 500 thousand pounds, inter-UK, for money mules (now such money mules now). Skip for now.

Account for authorization of payments, balance is 2 million pounds

No function of payment approval. Balance is 18 million pounds. Tried to transfer 2 million to China

Balance is 15 million pounds, dual authorization off. No opportunity to establish sort code for transfer. It is better to ring out

THREAT ACTORS

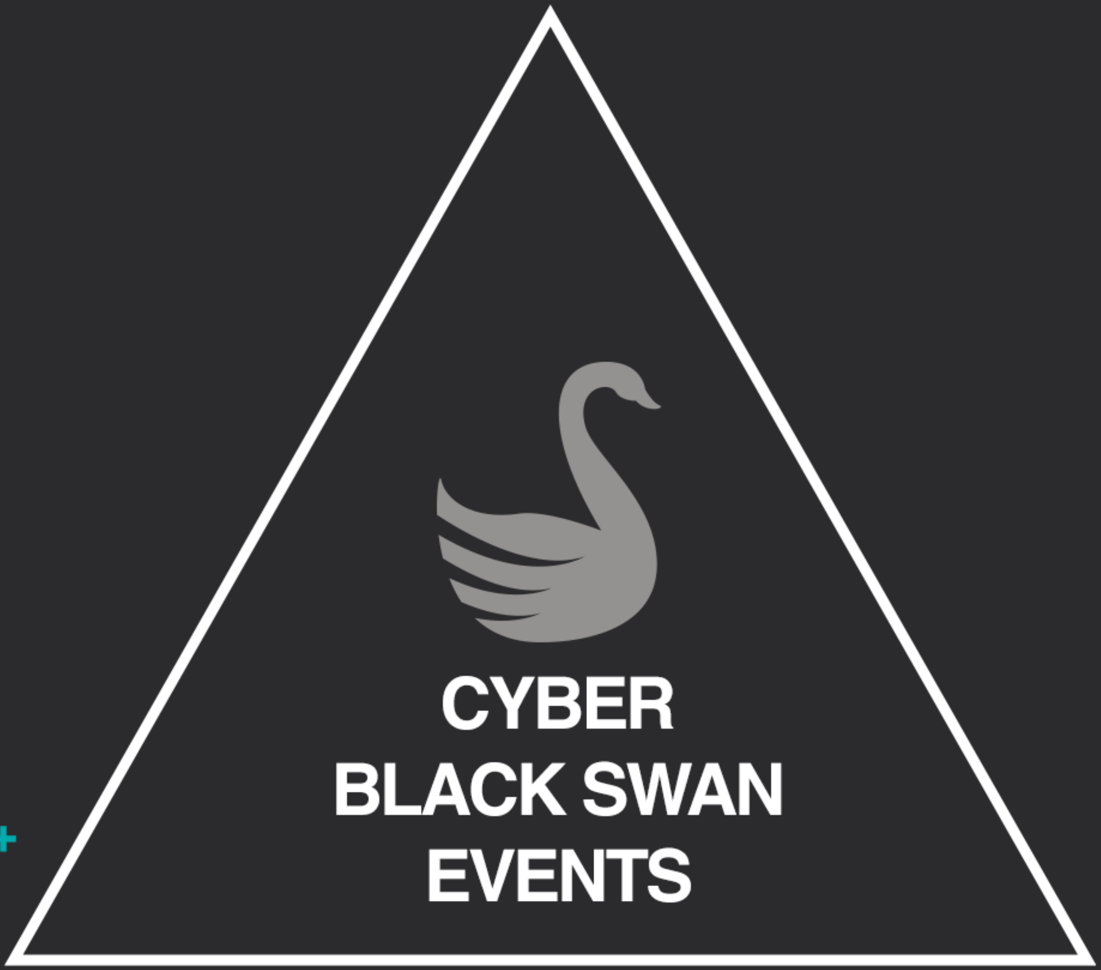
NATION STATES

MOTIVATED
BY PROFIT

MOTIVATED
BY CAUSE

THREE FORCES OF CYBER EFFECT (3FC)

MOORE'S LAW



CYBER
BLACK SWAN
EVENTS

1
Mechanization, water power, steam power

2
Mass production, assembly line, electricity

3
Computer and automation

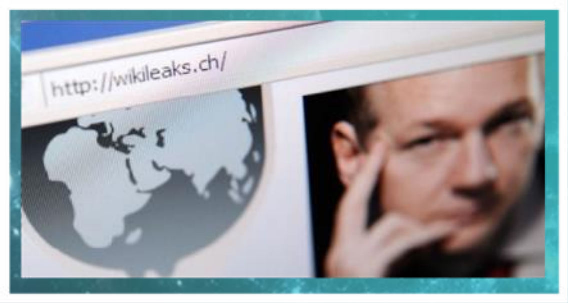
4
Cyber Physical Systems

ECONOMIC +
POLITICAL
CLIMATE

4TH
INDUSTRIAL
REVOLUTION

http://blog.cyberelders.org/2017/08/three-forces-of-cyber-effect.html

LAY OF THE LAND



ASSANGE EFFECT

SNOWDEN EFFECT

ATTACK SURFACE COMPLEXITY

ASSANGE EFFECT

SNOWDEN EFFECT

ATTACK SURFACE COMPLEXITY

ATTACK SURFACE COMPLEXITY

1991 - 10,239 lines of code

2017 - 33,580,696

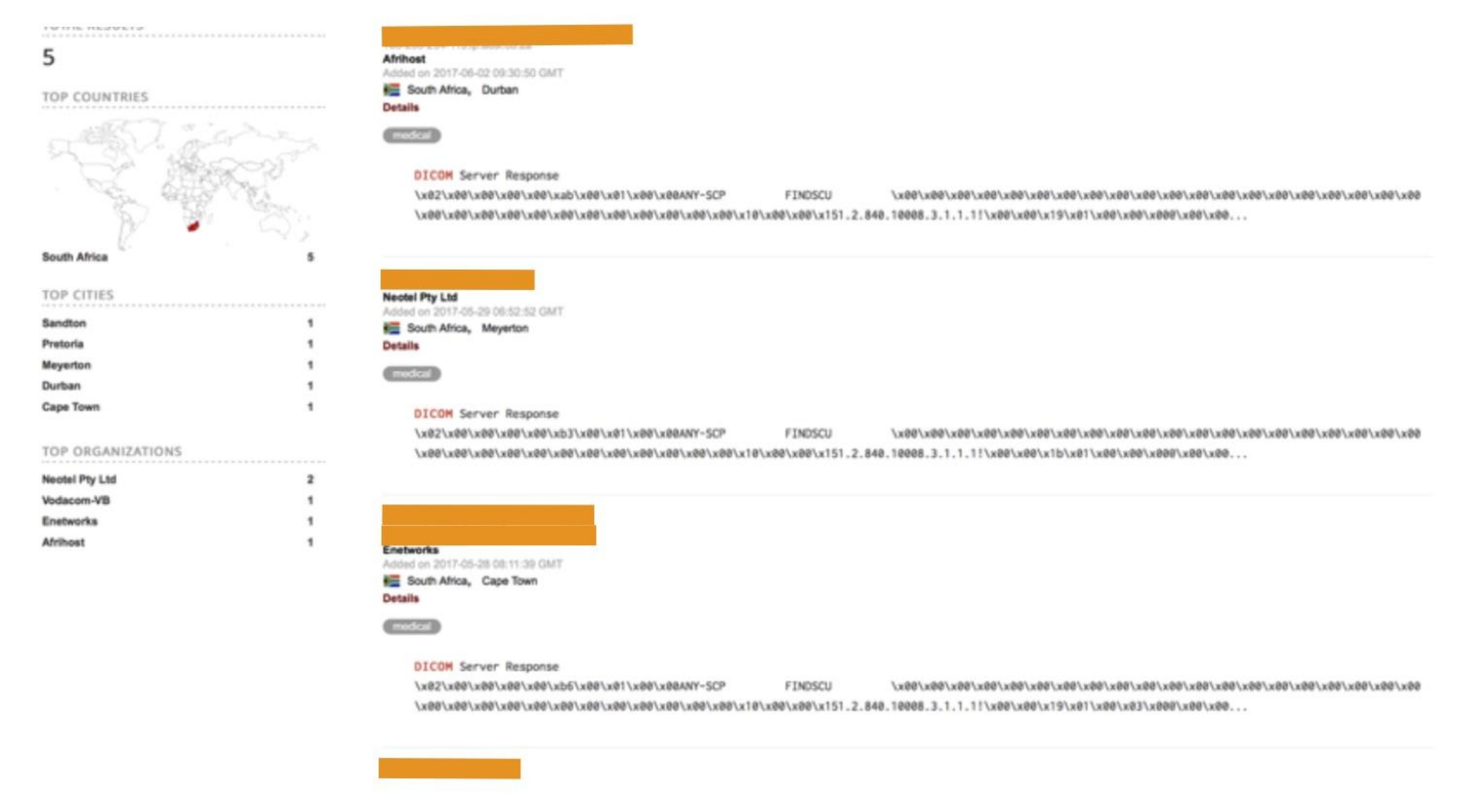
LOC % bugs?

20M lines of code

https://www.openhub.net/p/linux

ATTACK SURFACE COMPLEXITY

MEDICAL



TOTAL RESULTS

5

TOP COUNTRIES

South Africa	5

TOP CITIES

Sandton	1
Pretoria	1
Meyerton	1
Durban	1
Cape Town	1

TOP ORGANIZATIONS

Neotel Pty Ltd	2
Vodacom-VB	1
Enetworks	1
Afrihost	1

[redacted]

Afrihost

Added on 2017-06-02 09:30:50 GMT

South Africa, Durban

Details

```
DICOM Server Response
\x02\x00\x00\x00\x00\xab\x00\x01\x00\x00ANY-SCP         FINDSCU         \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x10\x00\x00\x151.2.840.10008.3.1.1.1!\x00\x00\x19\x01\x00\x00\x000\x00\x00...
```

[redacted]

Neotel Pty Ltd

Added on 2017-05-29 06:52:52 GMT

South Africa, Meyerton

Details

```
DICOM Server Response
\x02\x00\x00\x00\x00\xb3\x00\x01\x00\x00ANY-SCP         FINDSCU         \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x10\x00\x00\x151.2.840.10008.3.1.1.1!\x00\x00\x1b\x01\x00\x00\x000\x00\x00...
```

[redacted]

Enetworks

Added on 2017-05-28 08:11:39 GMT

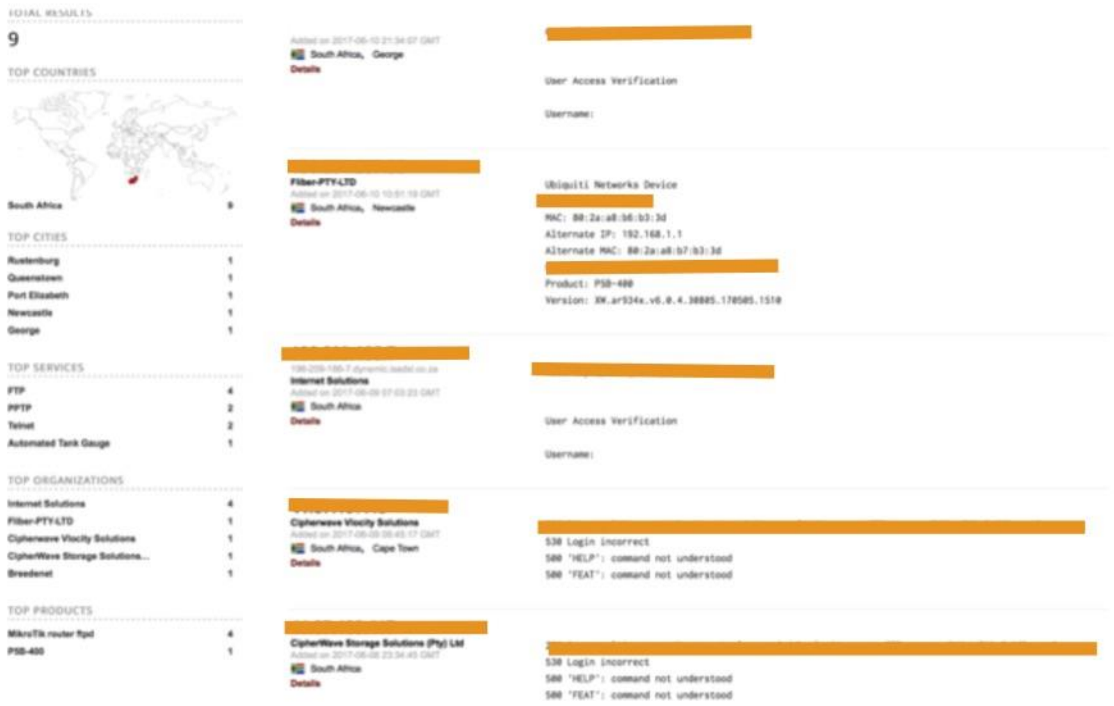
South Africa, Cape Town

Details

```
DICOM Server Response
\x02\x00\x00\x00\x00\xb6\x00\x01\x00\x00ANY-SCP         FINDSCU         \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x10\x00\x00\x151.2.840.10008.3.1.1.1!\x00\x00\x19\x01\x00\x03\x000\x00\x00...
```

[redacted]

FILLING STATIONS



TOTAL RESULTS

9

TOP COUNTRIES

South Africa	9

TOP CITIES

Rustenburg	1
Queenstown	1
Port Elizabeth	1
Newcastle	1
George	1

TOP SERVICES

FTP	4
PPTP	2
Telnet	2
Automated Tank Gauge	1

TOP ORGANIZATIONS

Internet Solutions	4
Fiber-PTY-LTD	1
Cipherwave Viocity Solutions	1
CipherWave Storage Solutions...	1
Breedenet	1

TOP PRODUCTS

MikroTik router ftpd	4
PSB-400	1

Added on 2017-06-10 21:34:07 GMT
South Africa, George
Details

```
[redacted]

User Access Verification

Username:
```

[redacted]
Fiber-PTY-LTD
Added on 2017-06-10 10:51:19 GMT
South Africa, Newcastle
Details

```
Ubiquiti Networks Device
[redacted]
MAC: 80:2a:a8:b6:b3:3d
Alternate IP: 192.168.1.1
Alternate MAC: 80:2a:a8:b7:b3:3d
[redacted]
Product: PSB-400
Version: XW.ar934x.v6.0.4.30805.170505.1510
```

[redacted]
196-209-186-7.dynamic.isadsl.co.za
Internet Solutions
Added on 2017-06-09 07:03:23 GMT
South Africa
Details

```
[redacted]

User Access Verification

Username:
```

[redacted]
Cipherwave Viocity Solutions
Added on 2017-06-09 06:45:17 GMT
South Africa, Cape Town
Details

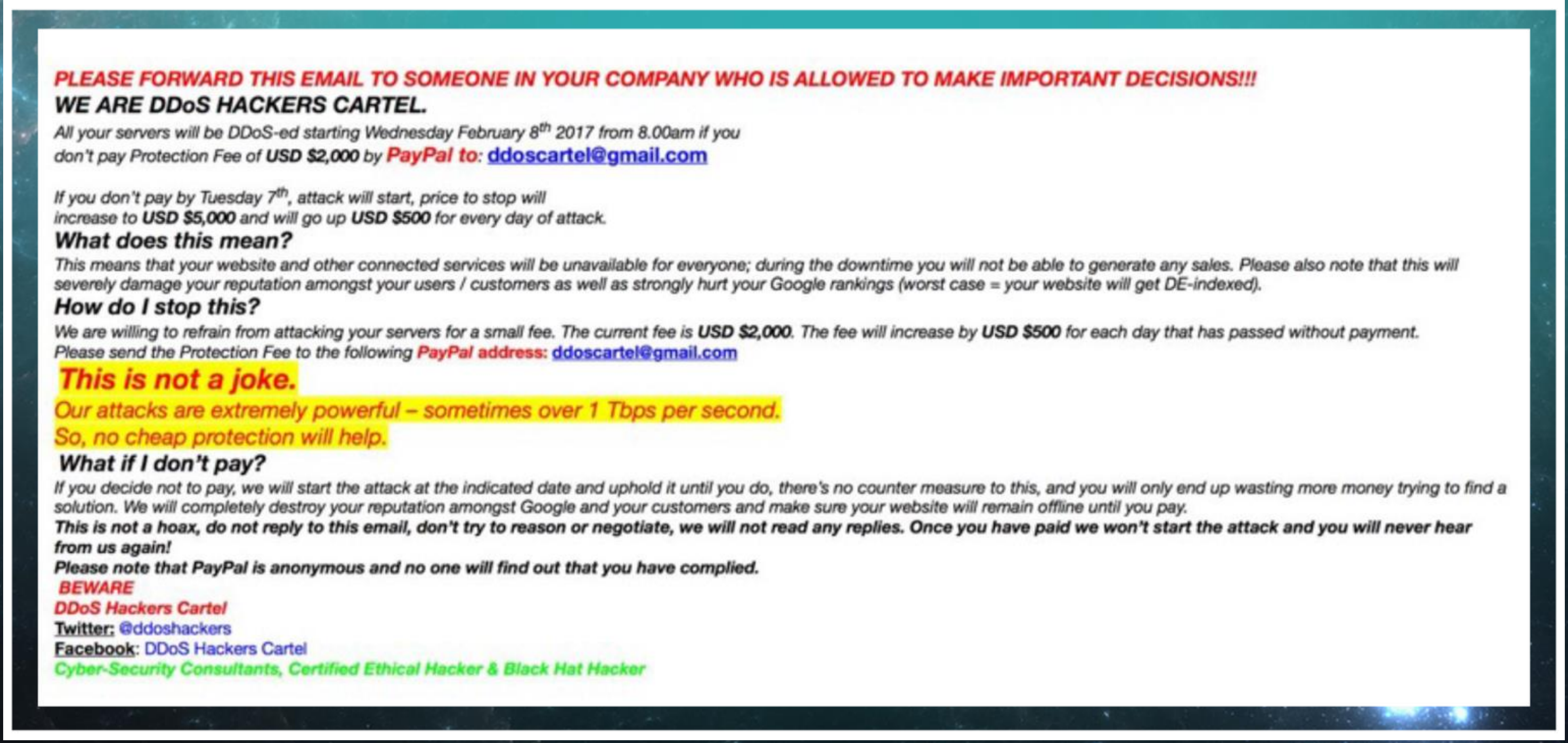
```
[redacted]
530 Login incorrect
500 'HELP': command not understood
500 'FEAT': command not understood
```

[redacted]
CipherWave Storage Solutions (Pty) Ltd
Added on 2017-06-08 23:34:45 GMT
South Africa
Details

```
[redacted]
530 Login incorrect
500 'HELP': command not understood
500 'FEAT': command not understood
```

Z5020
Tank Gauge 0.25 %
4750
O.L.E. (UK) LTD
ATEX
Zone 2
O.L.E. Tank Gauge Display
Ex
ZONE 2
This device is suitable for ATEX Zone 2 installation.
Mains power shall be 50 mm from intrinsically safe circuits.
Connection to Atex Zone 0/1 shall be by way of suitable barrier for both Level / Volume measurement sensor as well as Bund Alarm sensor if fitted.
Any cable junctions shall be by way of certified enclosures.
O.L.E. (UK) LTD
CE

DDOS & IOT



PLEASE FORWARD THIS EMAIL TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE IMPORTANT DECISIONS!!!

WE ARE DDoS HACKERS CARTEL.

*All your servers will be DDoS-ed starting Wednesday February 8th 2017 from 8.00am if you don't pay Protection Fee of **USD $2,000** by* **PayPal to:** ddoscartel@gmail.com

*If you don't pay by Tuesday 7th, attack will start, price to stop will increase to **USD $5,000** and will go up **USD $500** for every day of attack.*

What does this mean?

This means that your website and other connected services will be unavailable for everyone; during the downtime you will not be able to generate any sales. Please also note that this will severely damage your reputation amongst your users / customers as well as strongly hurt your Google rankings (worst case = your website will get DE-indexed).

How do I stop this?

*We are willing to refrain from attacking your servers for a small fee. The current fee is **USD $2,000**. The fee will increase by **USD $500** for each day that has passed without payment. Please send the Protection Fee to the following* **PayPal address:** ddoscartel@gmail.com

This is not a joke.

Our attacks are extremely powerful – sometimes over 1 Tbps per second.

So, no cheap protection will help.

What if I don't pay?

If you decide not to pay, we will start the attack at the indicated date and uphold it until you do, there's no counter measure to this, and you will only end up wasting more money trying to find a solution. We will completely destroy your reputation amongst Google and your customers and make sure your website will remain offline until you pay.

This is not a hoax, do not reply to this email, don't try to reason or negotiate, we will not read any replies. Once you have paid we won't start the attack and you will never hear from us again!

Please note that PayPal is anonymous and no one will find out that you have complied.

BEWARE

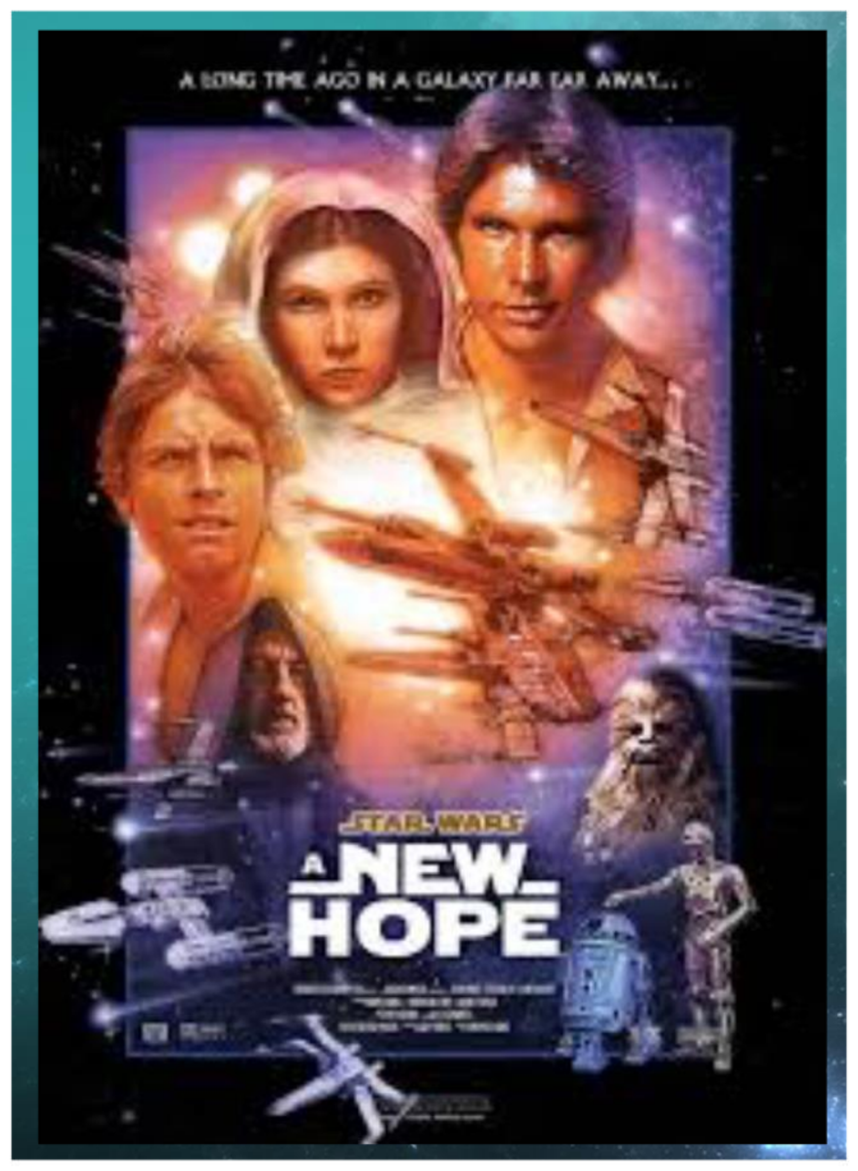
DDoS Hackers Cartel

Twitter: @ddoshackers

Facebook: DDoS Hackers Cartel

Cyber-Security Consultants, Certified Ethical Hacker & Black Hat Hacker

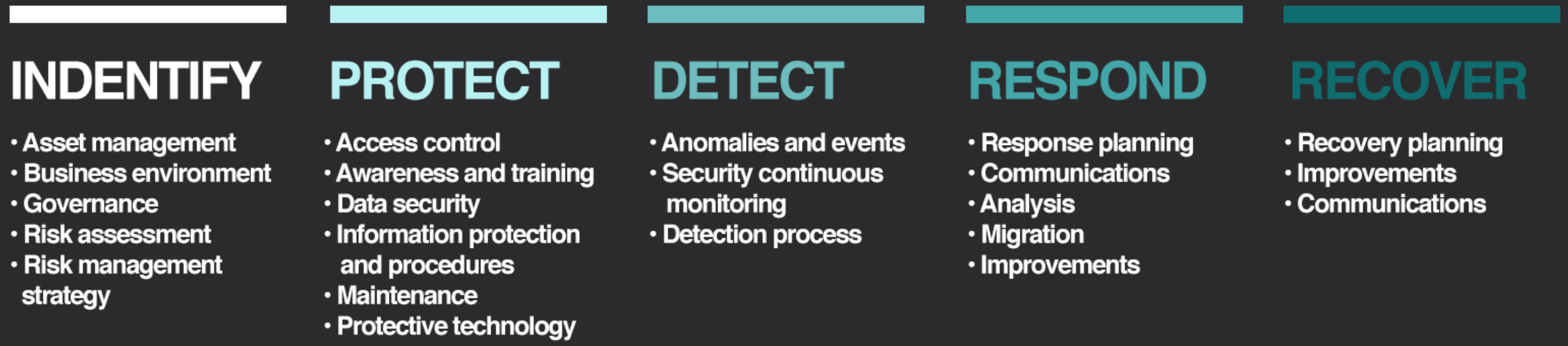
THERE IS HOPE…



FOG OF WAR

FOCUS AND A CHANGE IN THINKING

- **80 / 20 / Reality**
- **Bias**
- **Advocatus Diaboli**
- **4ThIR Building blocks**
- **Security as enabler**



INDENTIFY
- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

PROTECT
- Access control
- Awareness and training
- Data security
- Information protection and procedures
- Maintenance
- Protective technology

DETECT
- Anomalies and events
- Security continuous monitoring
- Detection process

RESPOND
- Response planning
- Communications
- Analysis
- Migration
- Improvements

RECOVER
- Recovery planning
- Improvements
- Communications

THANK YOU

@kovelin

http://blog.cyberelders.org