



ROADSEC^{TT}

**O MAIOR EVENTO BRASILEIRO DE
HACKING, SEGURANÇA E TECNOLOGIA**

AINDA PODEMOS PROTEGER NOSSOS DADOS NA ERA DO CYBERWAR ??

Paulo Veloso

O QUE É CYBERWAR??

“É o emprego, por entidades ou terroristas, de técnicas de destruição ou incapacitação de redes computacionais de informação.”

Agência Brasileira de Inteligência

“É o emprego de técnicas e conhecimentos em sistemas computacionais e intrusão de redes, com objetivos variados, visando geralmente a paralisação de serviços essenciais, incapacitação de redes computacionais e/ou roubo de informações privadas.”

Agência Brasileira de Inteligência

Paulo Veloso – Vulgo EU

Transição dos mundos



Analógico



Digital

Transição dos mundos



Energia



Telecom



Transportes

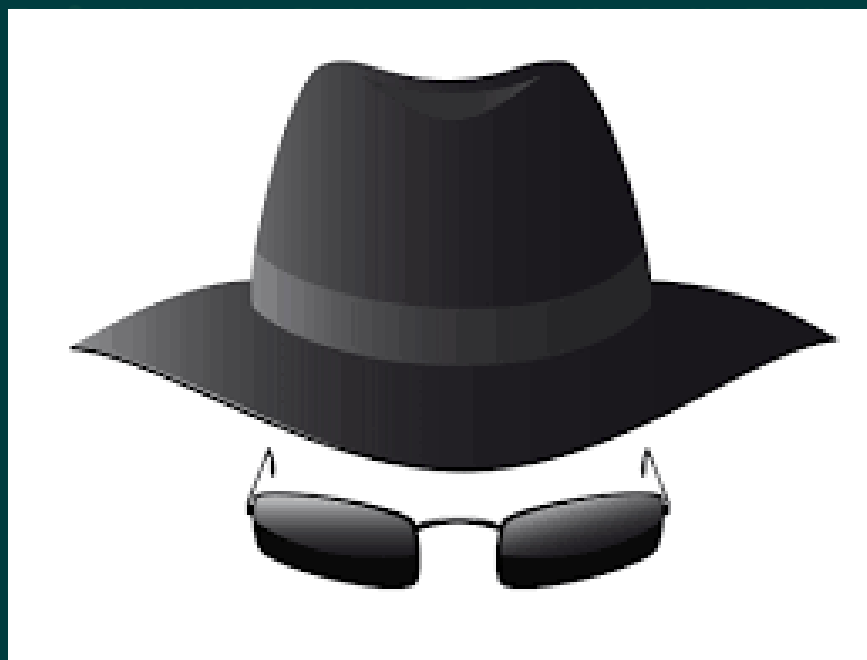
Dependência Tecnológica





Hacker Ético

Black Hats Hackers



Novos Cenários de Ameaças



Novos Cenários de Ameaças

APTs

ZERO DAY

RAMSONWARE

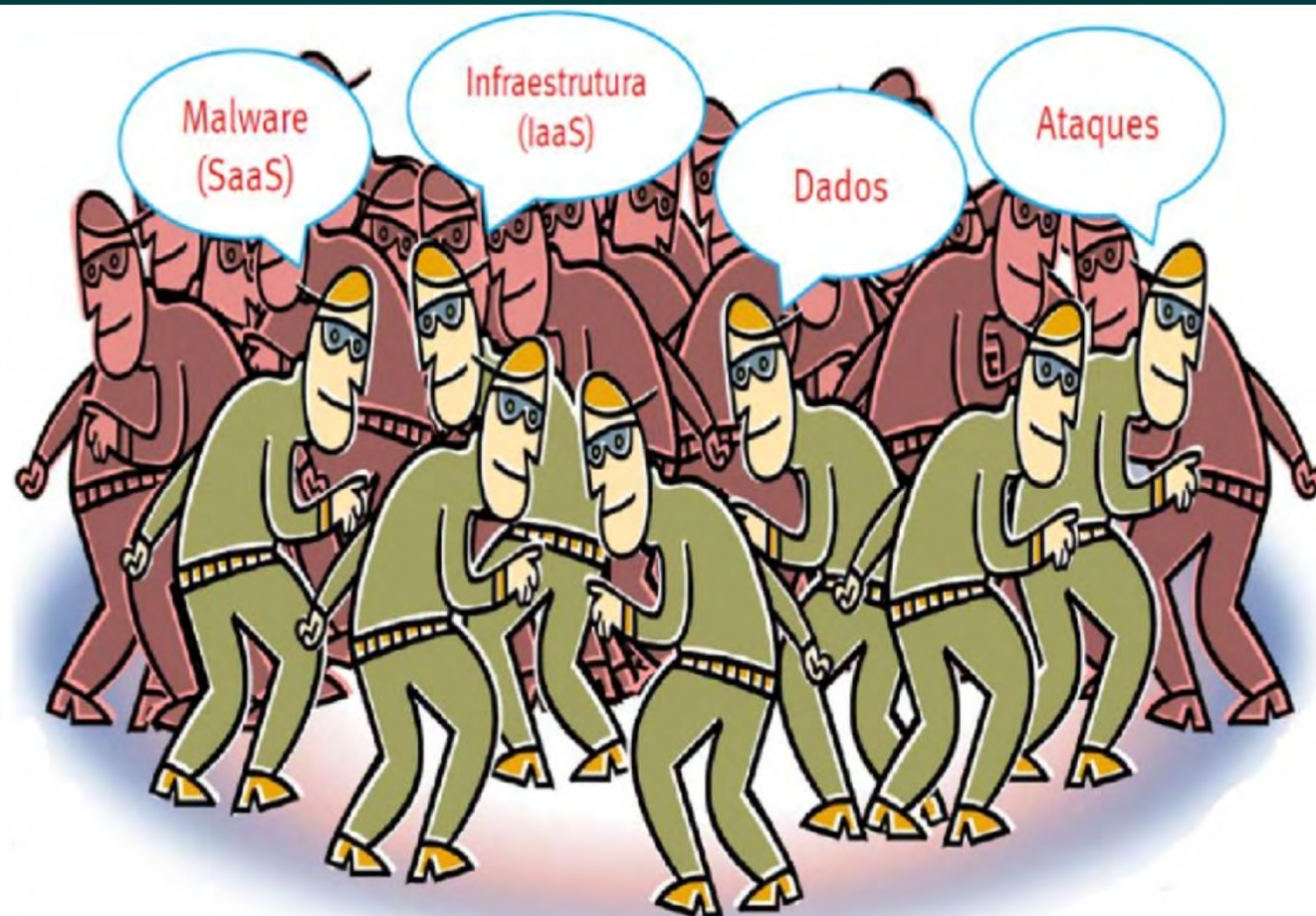


Novos Cenários de Ameaças

Novo Serviço:

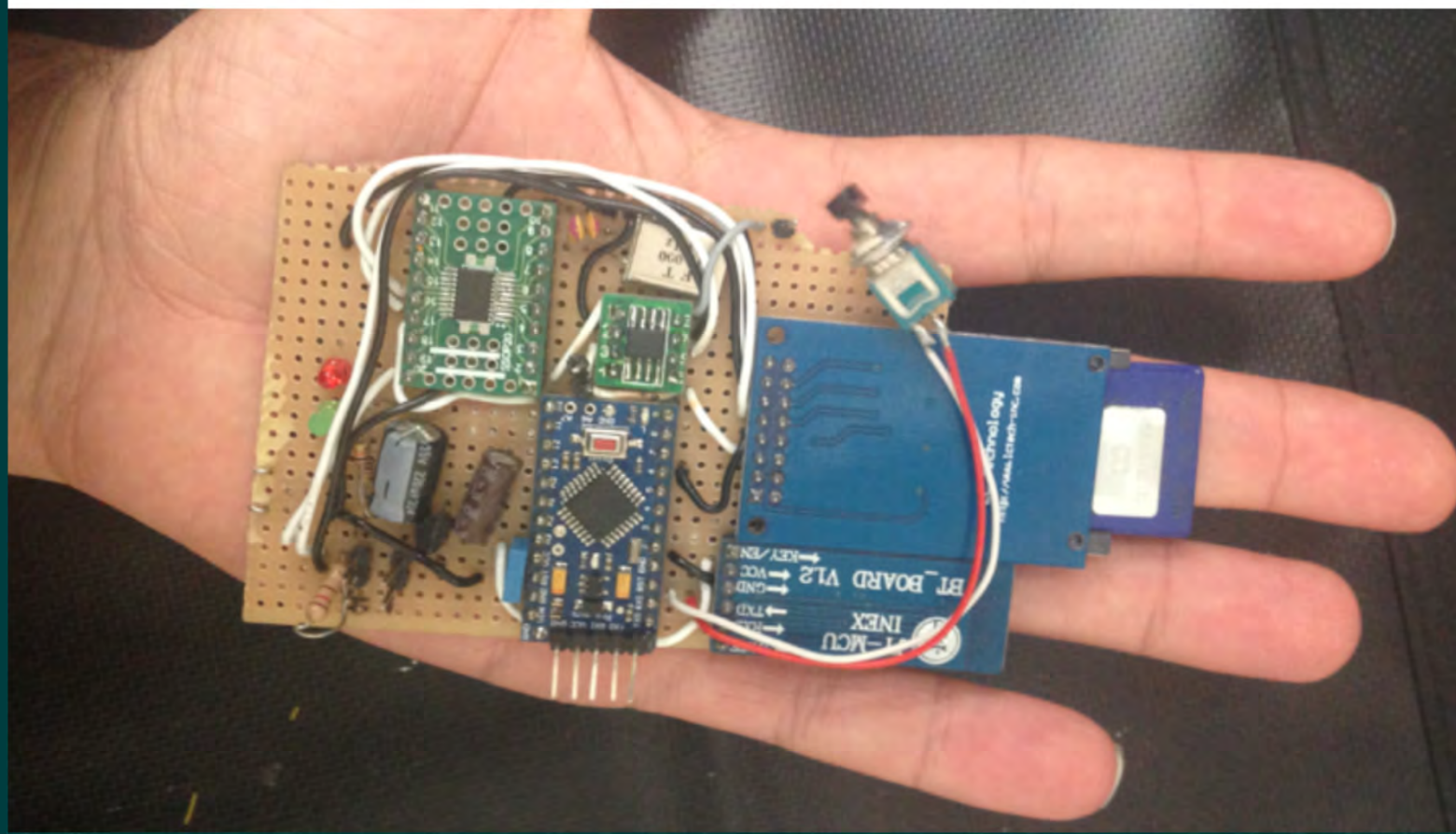
FAAS

Fraude as a Service



27/04/2015

Hacking a Car remotely with \$20 iPhone sized Device



Fraude as a Service

NEWS

SEARCH CARDS

SUPPORT TICKETS

PAYMENTS

EXIT

×

Shopping cart:
0 item(s).
0 rubles

Account balance:
5 rubles

Account status:
USER

Your account

Your cards (0)

Payments

Personal info

Information

FAQ / Help

BIN List

Flags of the World

World Country
Information

ISO 3166 Country
Code List

CARDS


Searching by BINs: 404658 405219 412709 412899 421723 427138 427533 430093 430187 431656 442813 471586 471588 521899 540550 540554 540598 541065 541363 541480 542164 542379 542418 542655 546616 547233 548530 548559 548688 548691 556709, CVV2: , City: , State: , Country: .

REFINE SEARCH

NN	PAN	CVV2	EXPDATE	NAME	ADDRESS	CITY	STATE	ZIP	COUNTRY	PHONE	PRICE	
551	5466160#####	###	03/2010	████	████	Cary	NC	27511	US	919-4#####	35.00	<input type="checkbox"/>
552	5424180#####		03/2009	████	██ ave	floral park	NY	11001	US	5163#####	14.00	<input type="checkbox"/>
553	5424180#####	###	05/2009	████	████ Way	Castro Valley	CA	94546	US	5105#####	35.00	<input type="checkbox"/>
554	5410654#####	###	07/2009	████	████ NW #th	Oklahoma City	OK	73118	US	4055#####	35.00	<input type="checkbox"/>
555	5424180#####	###	02/2008	████	████ o-s	Niagara Falls	NY	14304	US	7162#####	35.00	<input type="checkbox"/>
556	5424180#####	###	08/2009	████	████ Pala	San Jose	CA	95123	US	4082#####	35.00	<input type="checkbox"/>
557	5466160#####	###	04/2010	████	██ Road	Pond Eddy	NY	12770	US	9172#####	35.00	<input type="checkbox"/>
558	5466160#####	###	04/2010	████	██ Ave	Trumbull	CT	06611	US	203-4#####	35.00	<input type="checkbox"/>
559	5424180#####	###	07/2008	████	████ Court	leesburg	VA	20176	US	703-4#####	35.00	<input type="checkbox"/>
560	5466160#####	###	10/2008	████	██ Trail	Congers	NY	10920	US	8452#####	35.00	<input type="checkbox"/>
561	5424180#####	###	04/2009	████	██ Street	East Palatka	FL	32131	US	9046#####	35.00	<input type="checkbox"/>

Fraude as a Service

US\$ 20/1.000
infecções

 Load your software to thousand computers. ABC INSTALL SERVICE.

Load your trojan, DDoS-bot, Spam-bot, etc. to thousand computers. Very simple, like ABC.

Fresh, clean and cheap installs.

1) MIX. Top countries - US, TR, x-USSR. Minimum order - 1000 loads.
till 5k - 23\$ per 1k
5-10k - 21\$ per 1k
10k+ - 20\$ per 1k

2) Clean countries. Minimum order - 500 loads.
USA - from 130\$ per 1k
DE - from 200\$ per 1k
UK - from 270\$ per 1k

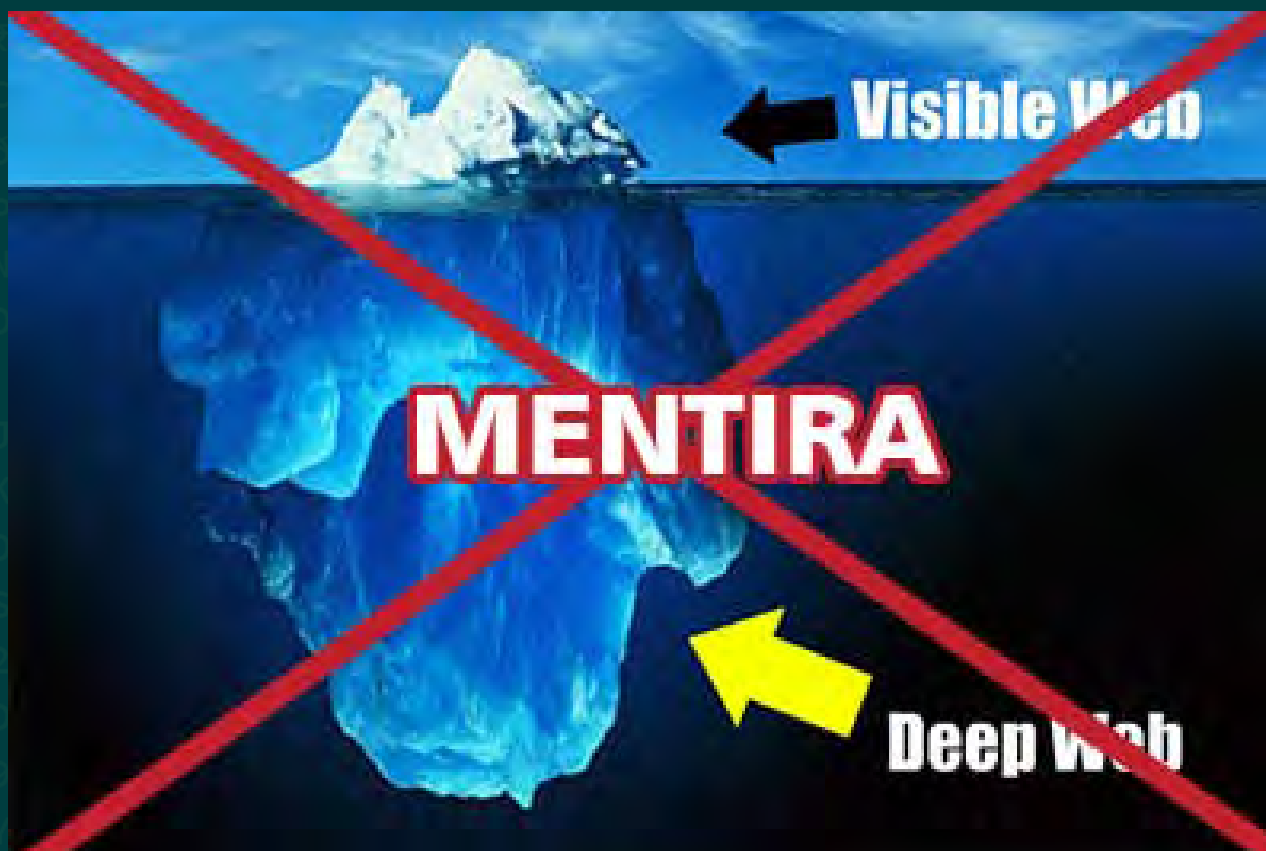
An iceberg floating in a dark blue ocean under a clear blue sky. The tip of the iceberg is visible above the water, while the much larger, submerged portion is visible below the surface. The text "Deep Web" is overlaid on the submerged part of the iceberg.

Deep Web



27/04/2015

Deep Web



Los niveles de la Internet Profunda

Nivel 1



Aquí se ubican las páginas más comunes de la red, y que son visitadas frecuentemente sin problemas.

Nivel 2

TARINGA!

MEGA

En este nivel se encuentran páginas para descarga de material pirata, así como foros con material explícito.

Nivel 3



Aunque es algo muy usual en gran número de usuarios, los torrents y descargas masivas son parte de este nivel.

Nivel 4

The Hidden Wiki

Para entrar a este nivel es necesario el uso de TOR. Aquí está la Hidden Wiki, y directorios con libros y material de descarga.

Nivel 5



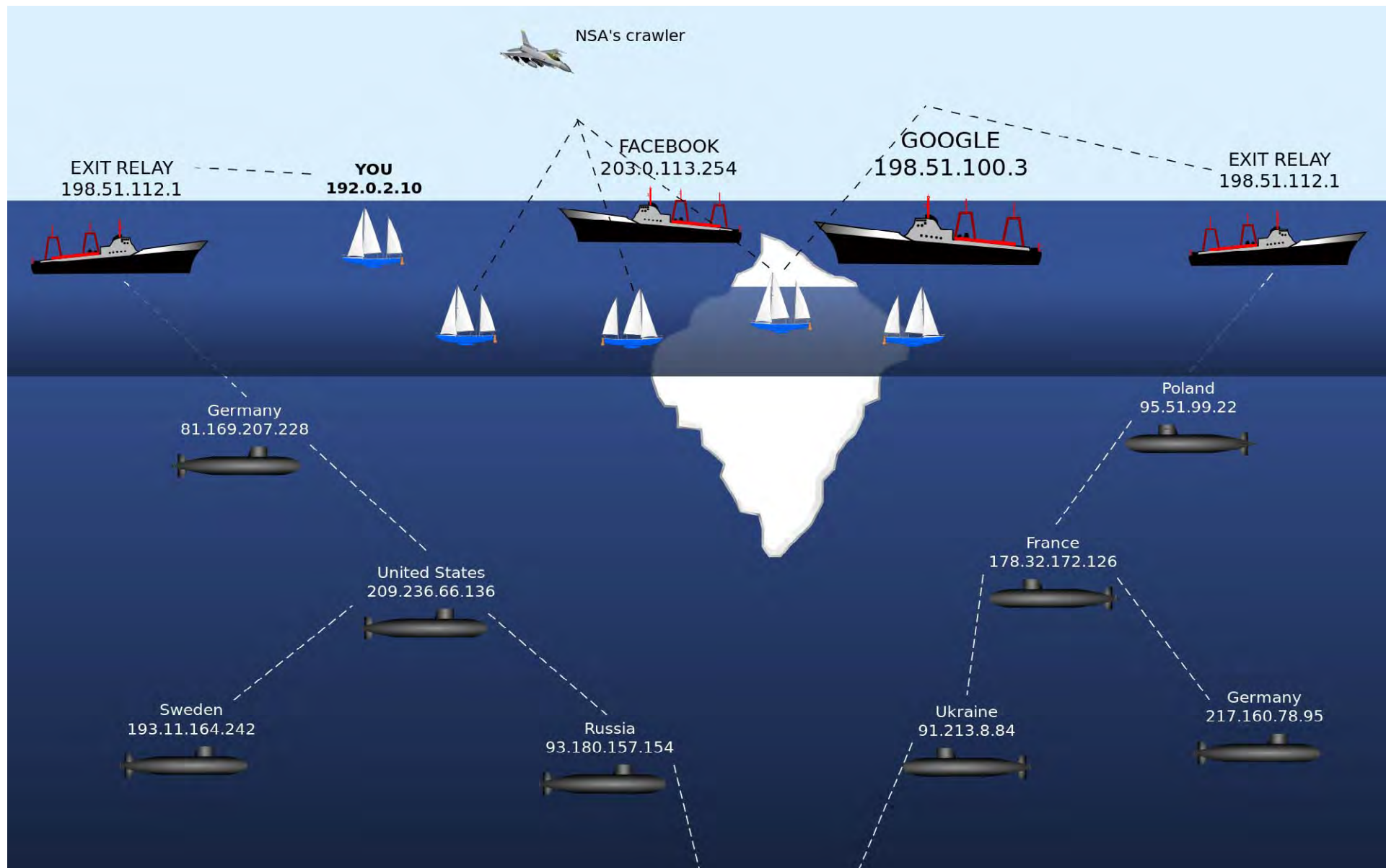
Foros Onion Chan, portales con material pornográfico infantil, hackers a sueldo, venta de objetos robados y drogas.

Nivel 6



El nivel más clasificado, llamado Islas Marianas. Se cree que aquí están las redes gubernamentales con acceso restringido.

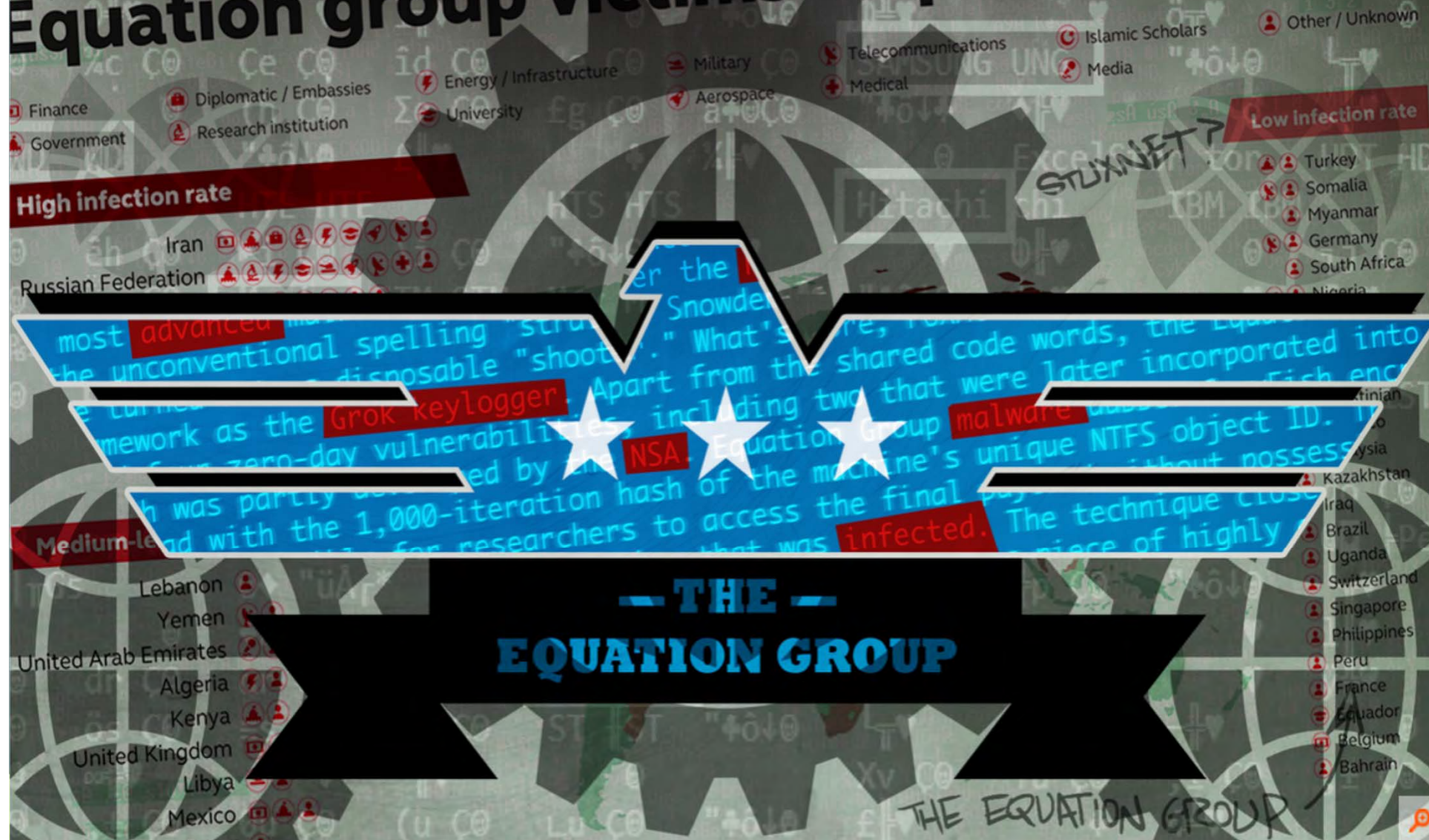
EL HERALDO



Nossos amigos americanos...



Equation group victims map



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

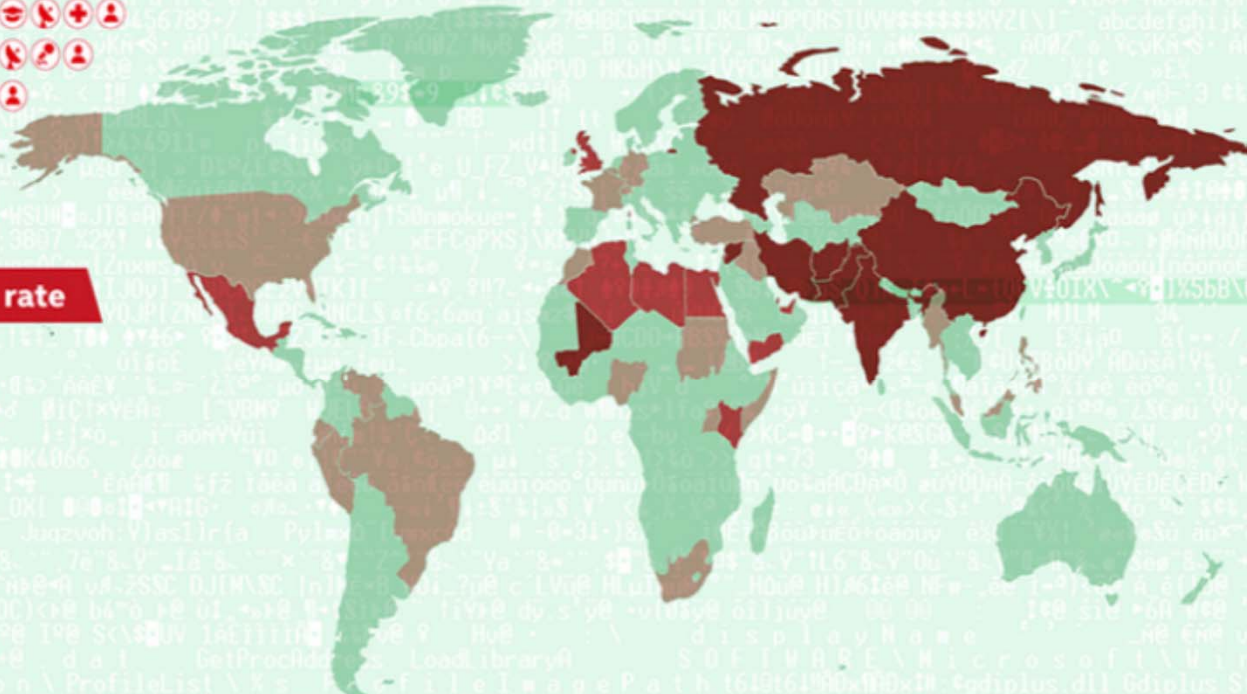
- Iran
- Russian Federation
- Pakistan
- Afghanistan
- India
- China
- Syria
- Mali

Medium-level infection rate

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

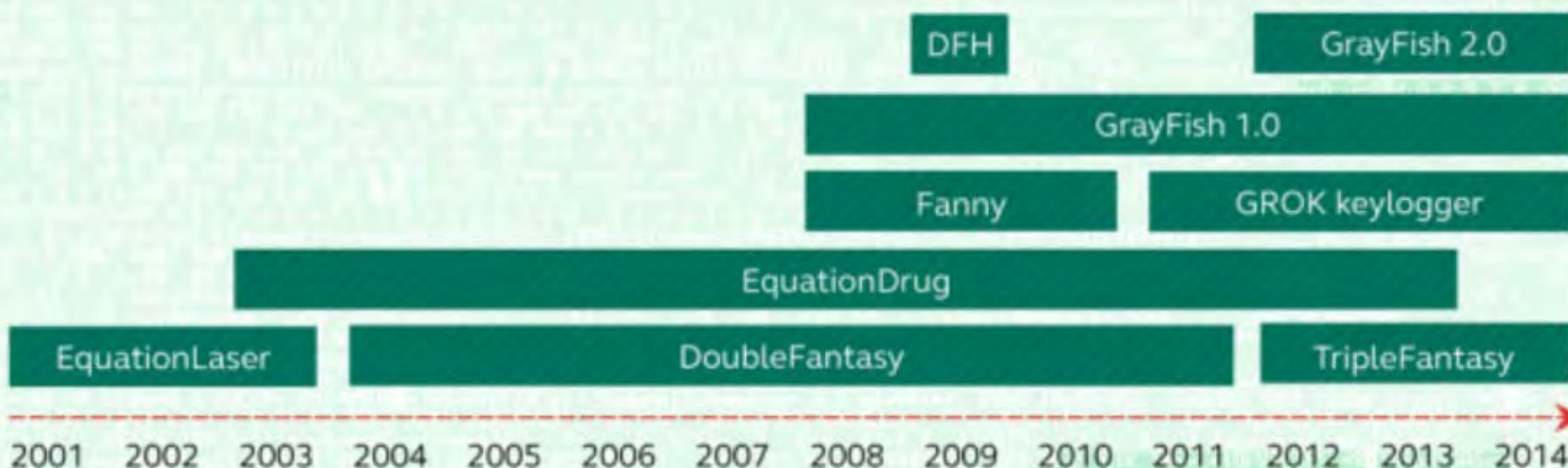
Low infection rate

- 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



Plataforma Equation

Equation group's malware timeline



- The Fanny timeline is based on C&C server IP activity
- TripleFantasy compilation timestamps seem to be fake, graph based on compiler versions and C&C registrations
- EquationDrug appears to have been replaced with Grayfish in somewhere in 2013; development started earlier
- DFH refers to "Disk from Houston"

Plataforma Equation

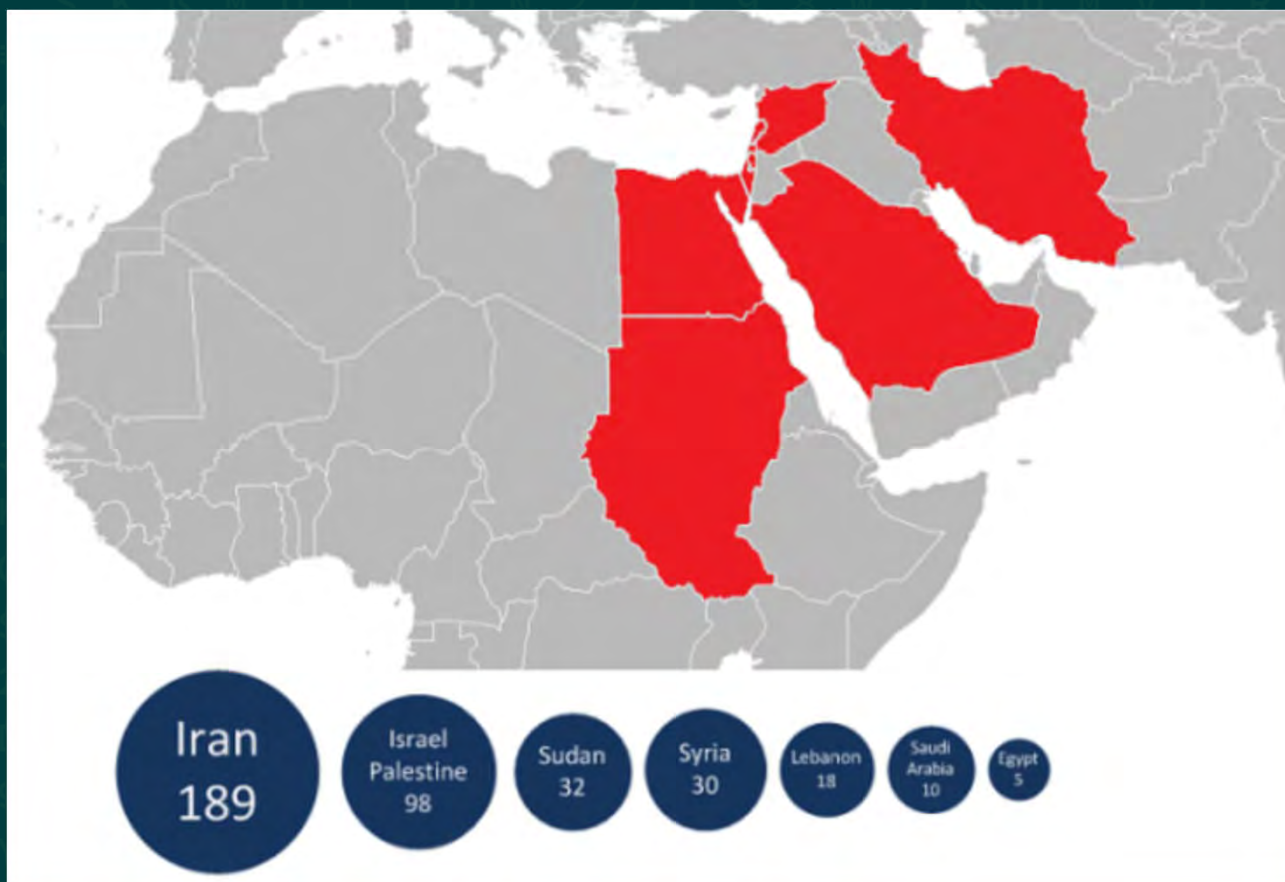


Stuxnet/Duqu

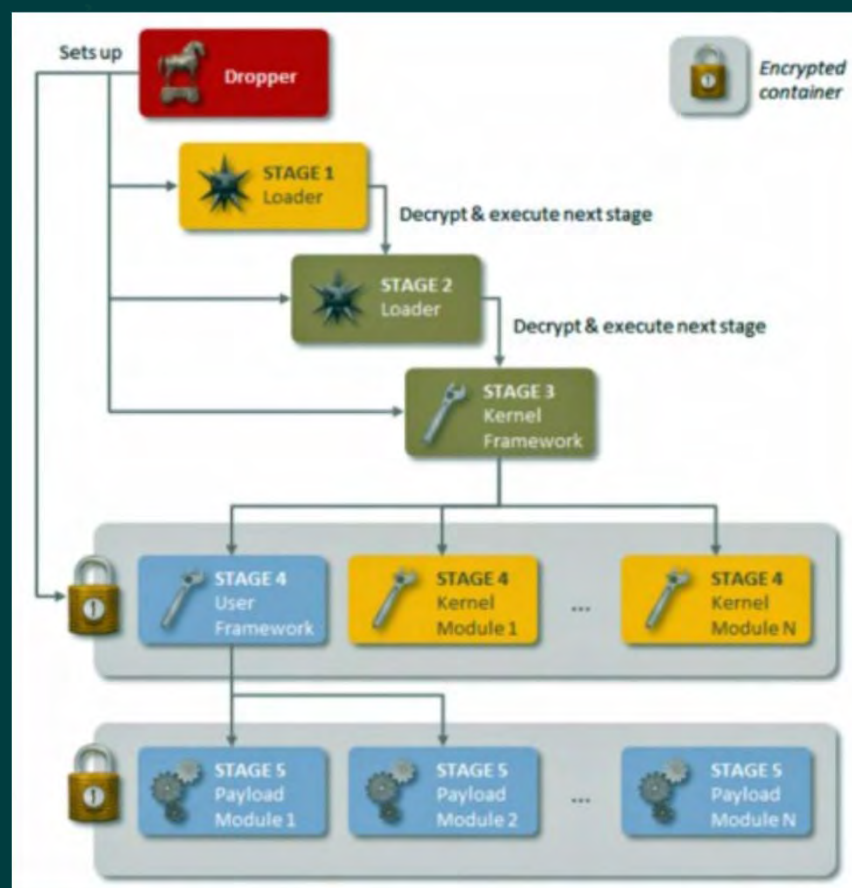
Evolution of Stuxnet replication

Evolution	Replication Technique	0.500	1.001	1.100	1.101
	Step 7 project files	X	X	X	X
0.5	USB through Step 7 project files	X			
0.5	USB through Autorun		X		
0.5	USB through CVE-2010-2568			X	X
1.0	Network shares		X	X	X
1.1	Windows Server RPC		X	X	X
1.1	Printer spooler		X	X	X
1.x	WinCC servers		X	X	X
	Peer-to-peer updating through mailslots	X			
	Peer-to-peer updating through RPC		X	X	X

Flame/Flamer



Regin



AURORAGOLD

Quero todas as ligações de celular do mundo possíveis de serem interceptadas!

- Conseguiram no final de 2013, com a quebra do A5/1, algoritmo de criptografia usado pelas operadoras para roaming. Mas faltava chamadas locais...

AURORAGOLD

gemalto[✱]
security to be free



**AINDA PODEMOS PROTEGER NOSSOS
DADOS NA ERA DO CYBERWAR ??**

Criptografia ainda é a solução



Diretor e ex-CEO do Google, Eric Schmidt



“A única solução para acabar com a vigilância do governo é criptografar tudo.”

Mas faça certo !!

Mesma chave de criptografia usada 28 mil vezes



Redes Sociais = Falta de privacidade



Não compartilhe chaves



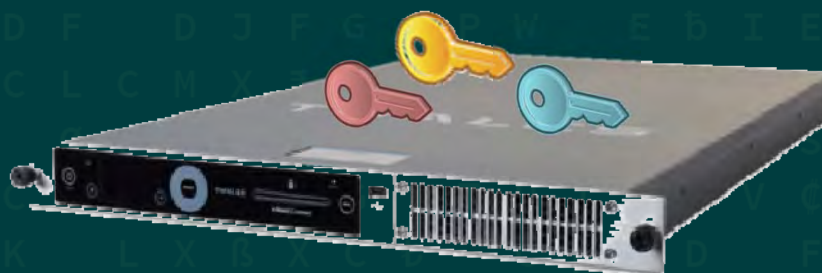
Troque periodicamente suas chaves...



Sempre tenha mais de um custodiante das chaves...



**Guarde suas chaves em local
seguro...de preferência um HSM**



“a arte da guerra nos ensina a não confiar na probabilidade de o inimigo não estar vindo, mas na nossa própria prontidão para recebê-lo; não na chance de ele não nos atacar, mas sim no fato de que fizemos a nossa posição inatacável”

SUN TZU



Paulo Veloso

Twitter: @paulovello

E-mail: paulo@pveloso.com



ROADSEC

Obrigado!