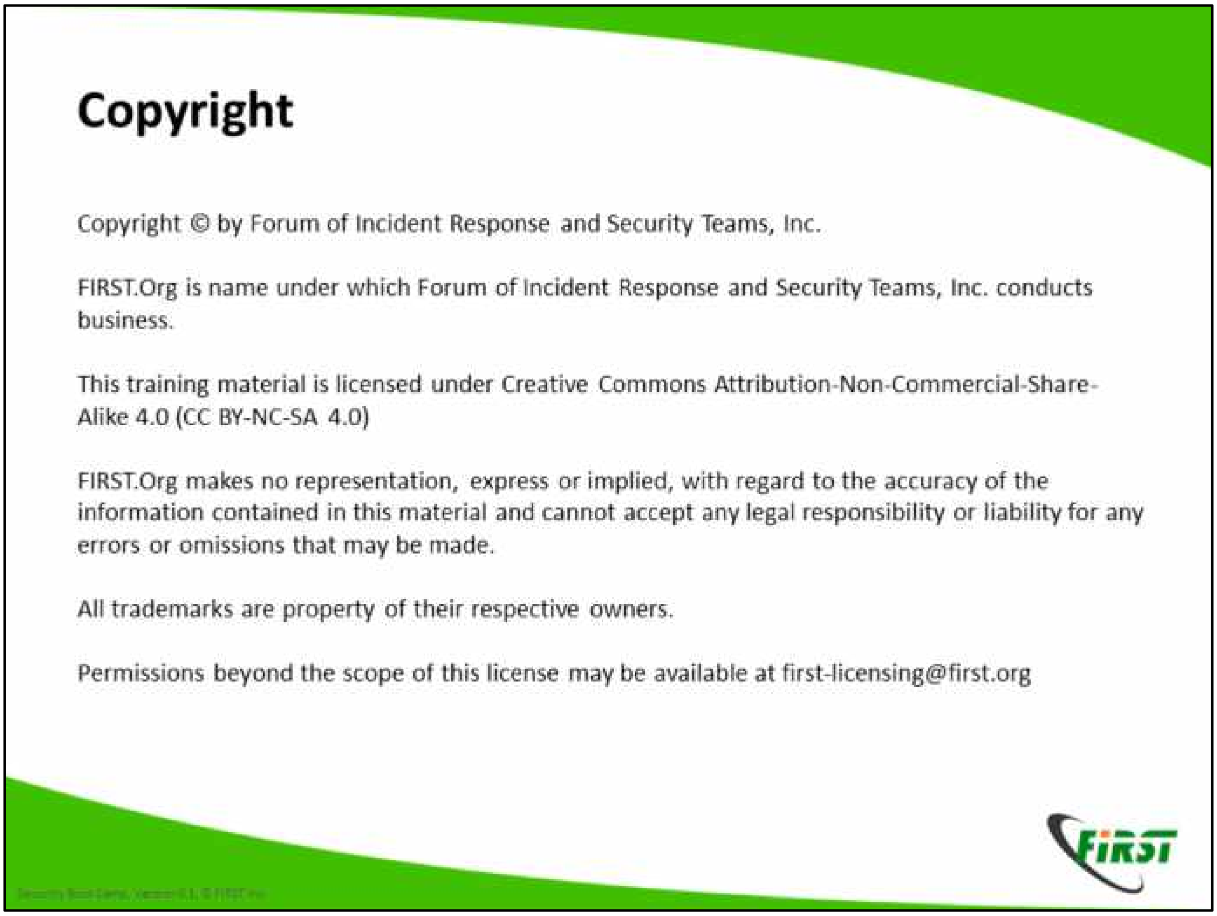
Security Boot Camp

Dr. Serge Droz

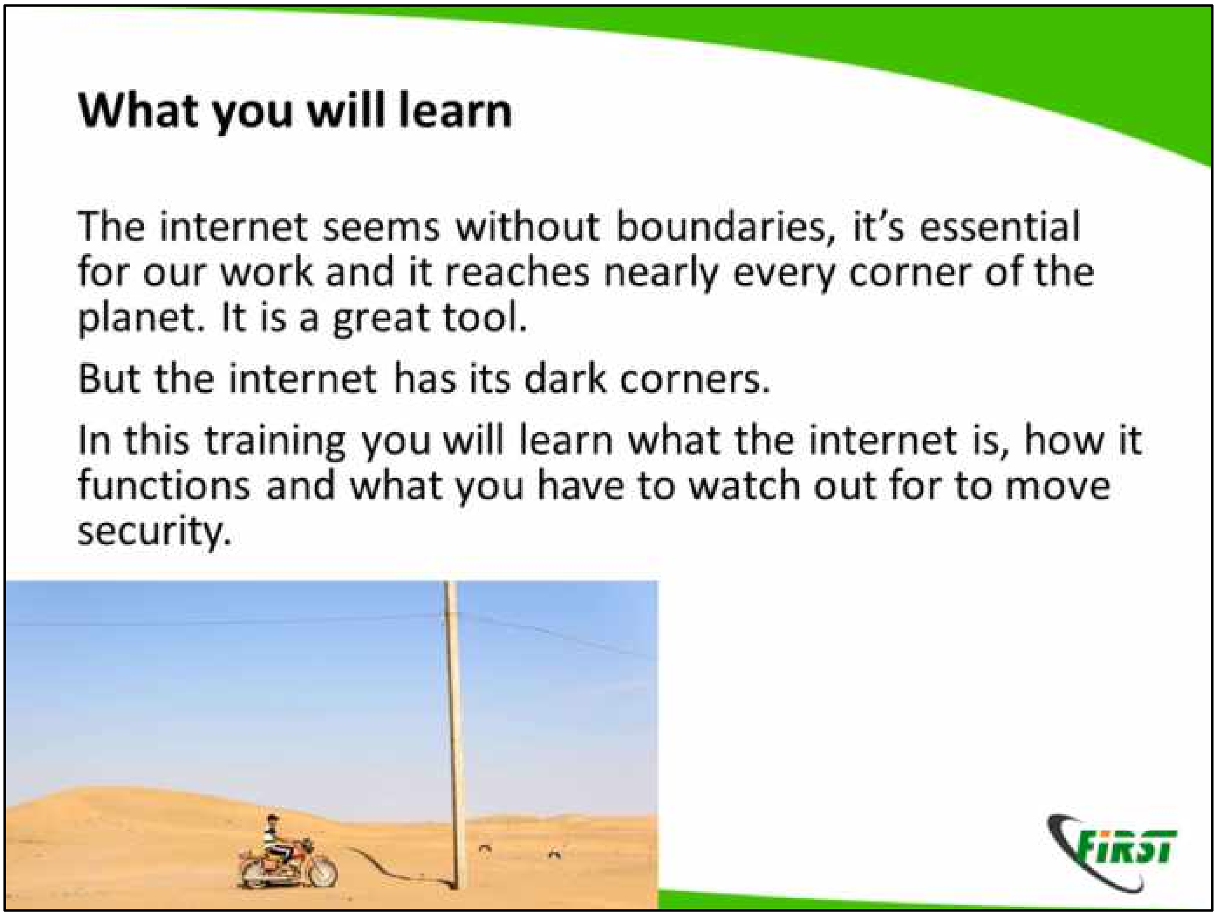
serge.droz@first.org



Copyright

FIRST.Org makes no representation, express or implied, with regard to the accuracy of the information contained in this material and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

FIRST Training materials are available for non-commercial use under a CC license. We would appreciate if you let us know that you use it: Send a mail to first-sec@firtst.org with your feedback



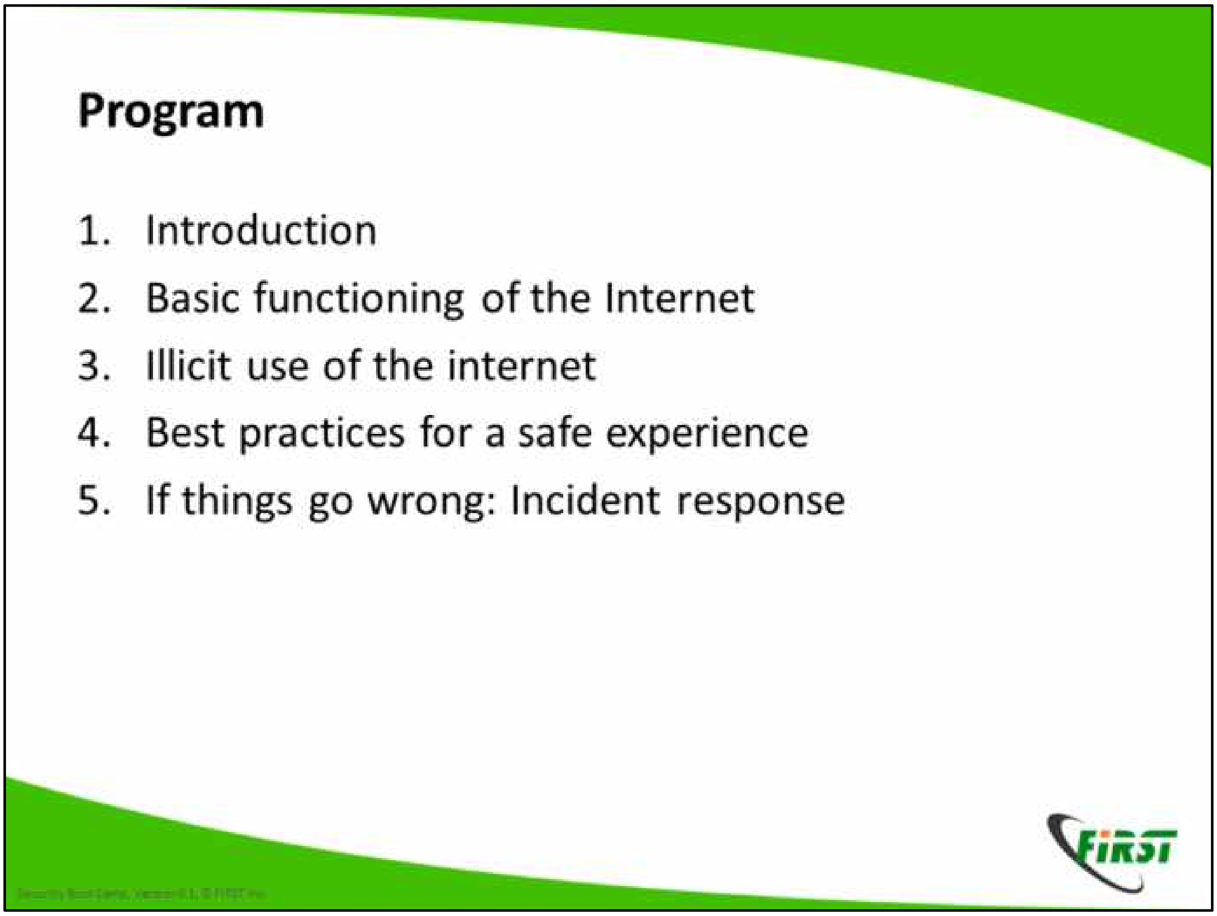
What you will learn

The internet seems without boundaries, it’s essential for our work and it reaches nearly every corner of the planet. It is a great tool.

But the internet has its dark corners.

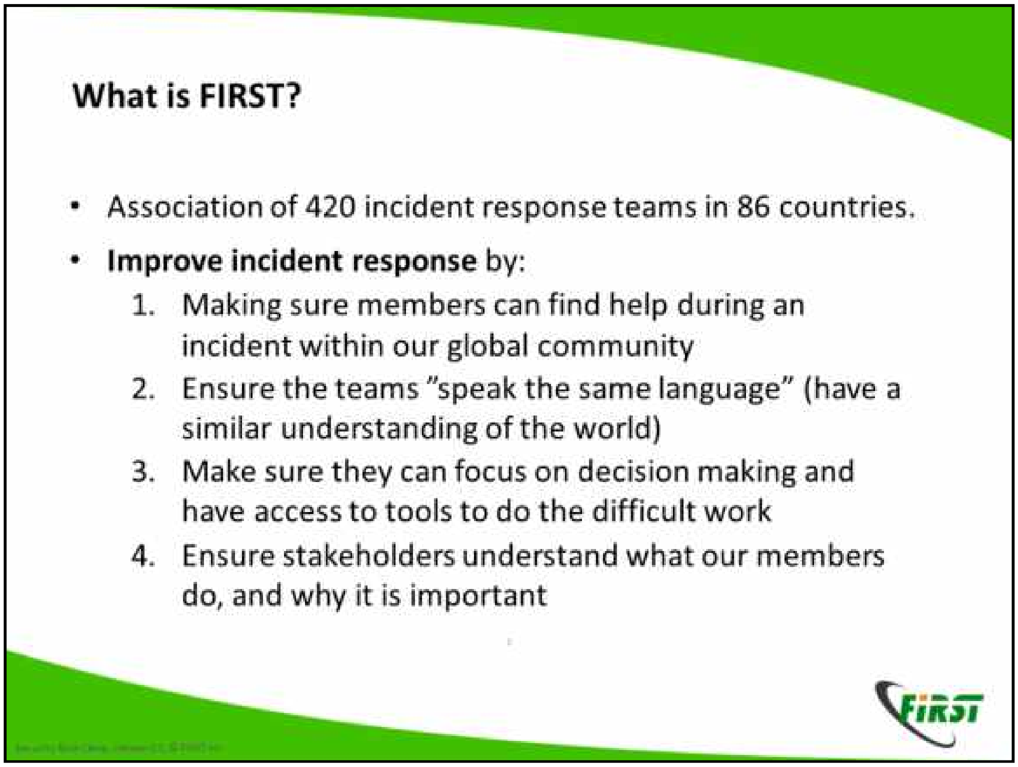
In this training you will learn what the internet is, how it functions and what you have to watch out for to move security.

Foto © Serge Droz, Kara-Kum Desert, Turkmenistan



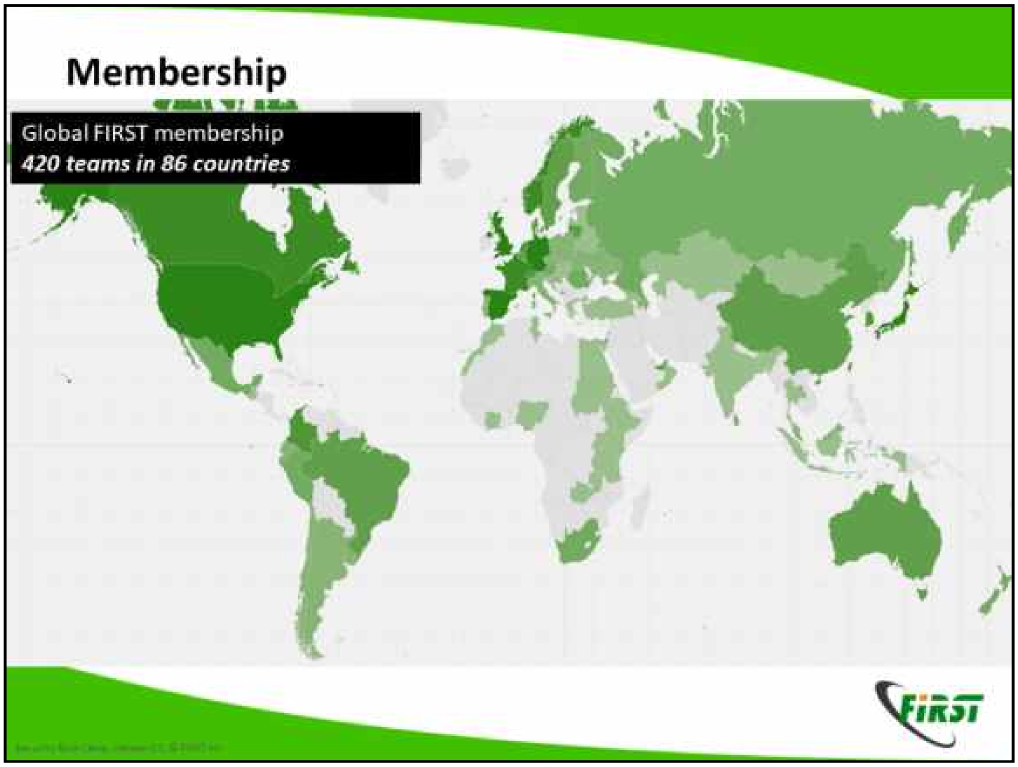
Program

1. Introduction
2. Basic functioning of the Internet
3. Illicit use of the internet
4. Best practices for a safe experience
5. If things go wrong: Incident response



What is FIRST?

- Association of 420 incident response teams in 86 countries.
- **Improve incident response** by:
  1. Making sure members can find help during an incident within our global community
  2. Ensure the teams ”speak the same language” (have a similar understanding of the world)
  3. Make sure they can focus on decision making and have access to tools to do the difficult work
  4. Ensure stakeholders understand what our members do, and why it is important

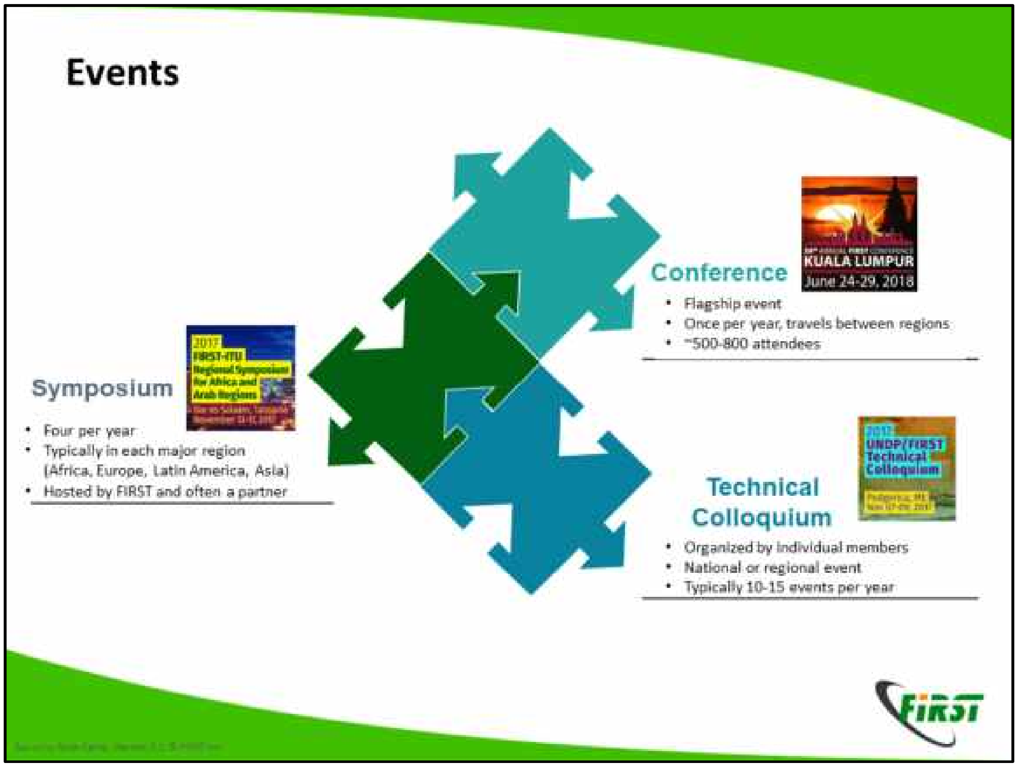


Membership

Global FIRST membership
420 teams in 86 countries

Note to Presenter: You can obtain the latest map / stats here - http://www.first.org/members/map

Today, FIRST is comprised of over 300 members in 70 countries.



KUALA LUMPUR
June 24-29, 2018
2017
FIRST-ITU
Regional Symposium
for Africa and
Arab Regions
2017
UNDP/FIRST
Technical
Colloquium
FIRST

Events

Conference

- Flagship event
- Once per year, travels between regions
- ~500-800 attendees

Symposium

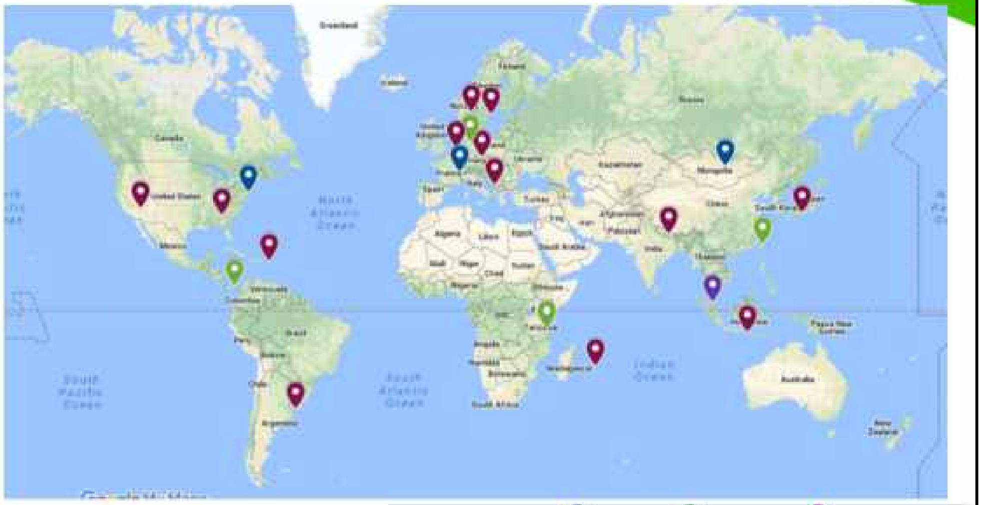
- Four per year
- Typically in each major region (Africa, Europe, Latin America, Asia)
- Hosted by FIRST and often a partner

Technical Colloquium

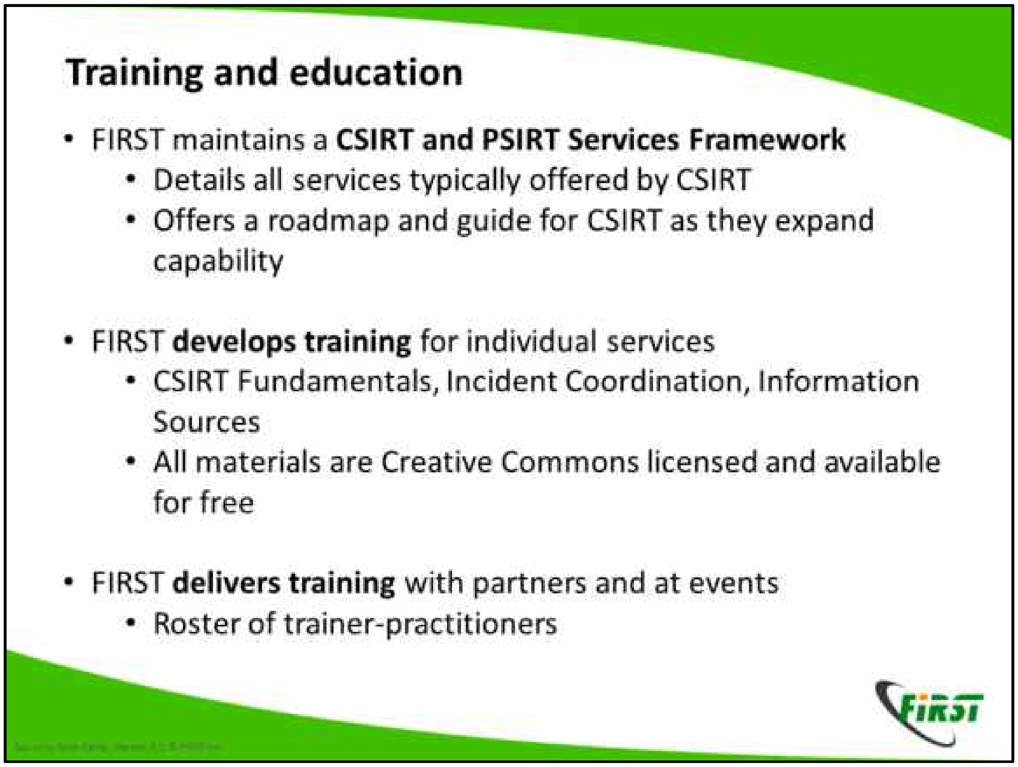
- Organized by individual members
- National or regional event
- Typically 10-15 events per year

FIRST organizes three types of events annually: the conference, up to four symposia, which are typically regional, and many TC’s, which are organized by individual members.

Global events 2017-2018

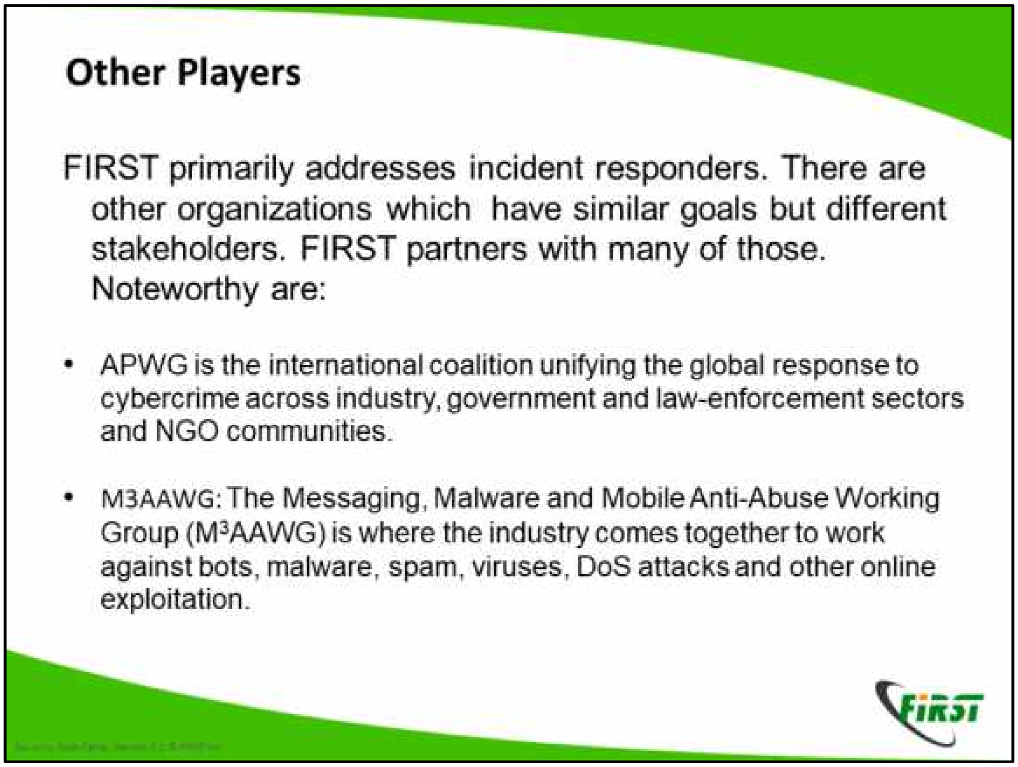


FIRST activity across the world: 🔵 *Training classes* 🟢 *TC's and Symposia* 🟣 *Annual conference 2017,*



Training and education

- FIRST maintains a **CSIRT and PSIRT Services Framework**
  - Details all services typically offered by CSIRT
  - Offers a roadmap and guide for CSIRT as they expand capability
- FIRST **develops training** for individual services
  - CSIRT Fundamentals, Incident Coordination, Information Sources
  - All materials are Creative Commons licensed and available for free
- FIRST **delivers training** with partners and at events
  - Roster of trainer-practitioners



Other Players

FIRST primarily addresses incident responders. There are other organizations which have similar goals but different stakeholders. FIRST partners with many of those. Noteworthy are:

- APWG is the international coalition unifying the global response to cybercrime across industry, government and law-enforcement sectors and NGO communities.
- M3AAWG: The Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG) is where the industry comes together to work against bots, malware, spam, viruses, DoS attacks and other online exploitation.

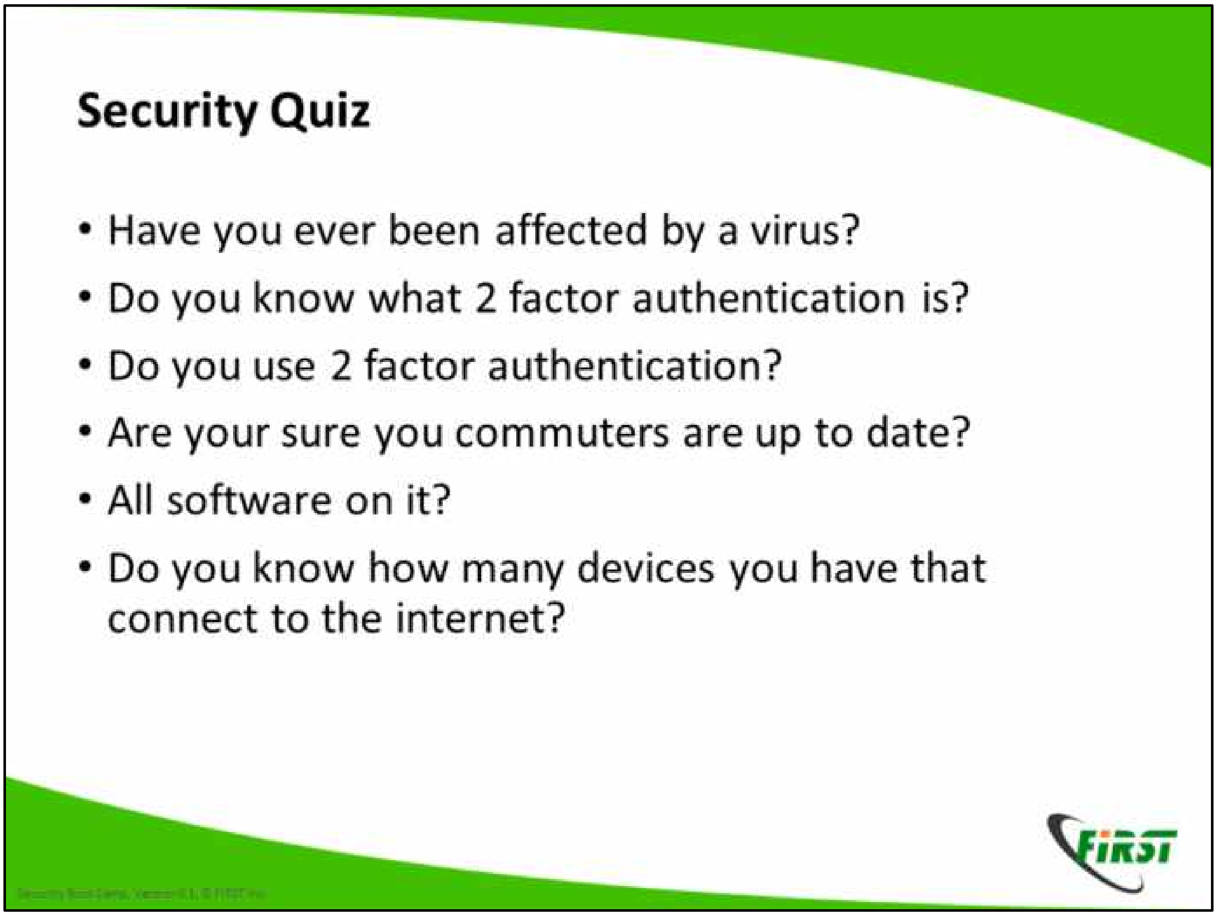
There are other organizations with a similar goal, but a different focus
Antifishing Workign Group APWG, which runs stop.think.connect
The Messaging, Malware and Mobile Anti-Abuse Working Group (M^{3}AAWG)

https://www.flickr.com/photos/psd/4389135567

Introduction round: Rather than everyone saying his name we try to acitvate the group by aksing them a few questions hand have them move to either side of the room, depending on their answer. This visualizes answers and gets people talking.
Possible questions are:

- Do you read more than two-three articles on cybersecurity?
- Who comes from a country with a national CSIRT? Yes/No/I don‘t know

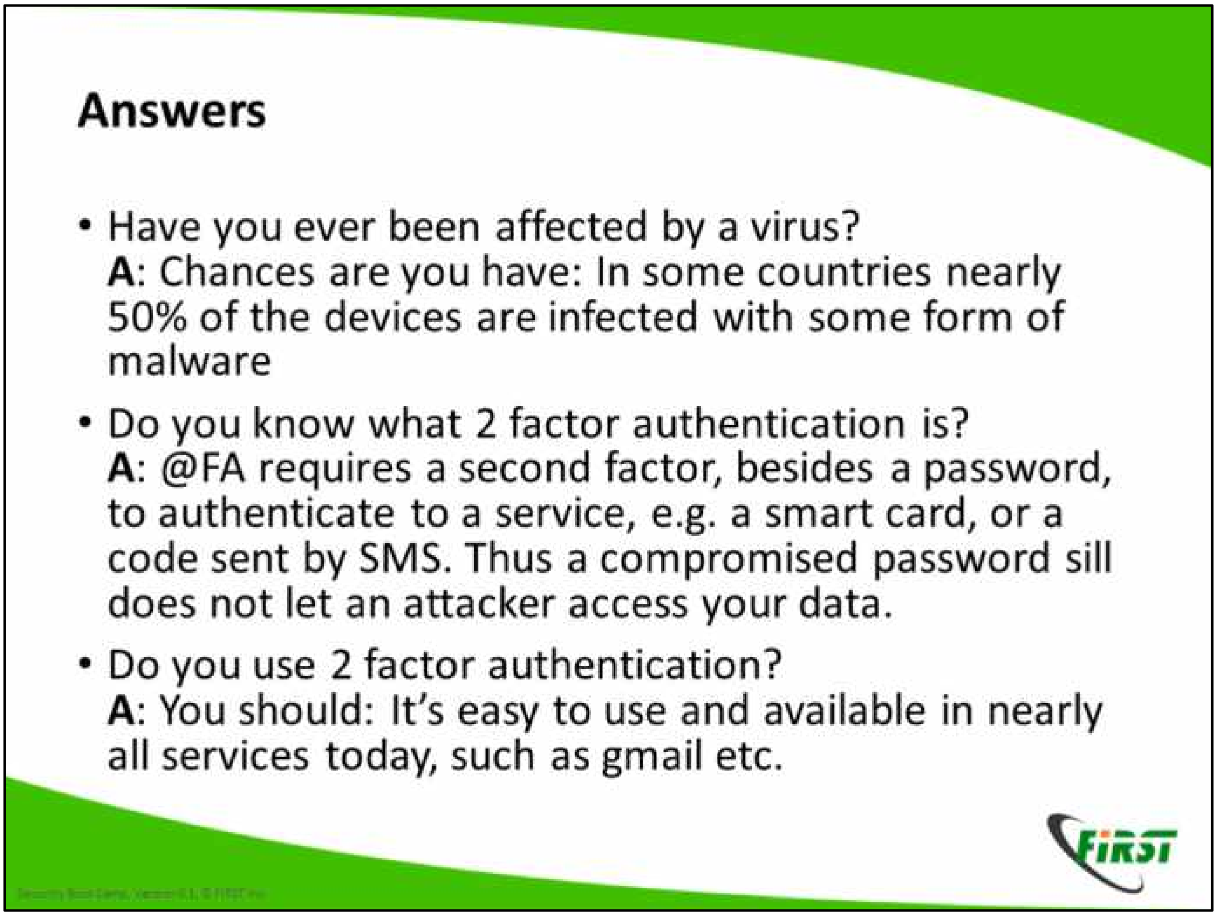
- Who thinks government have a role in cybersecurity?
- Who thinks governments can solve most cybersecurity problems?



Security Quiz

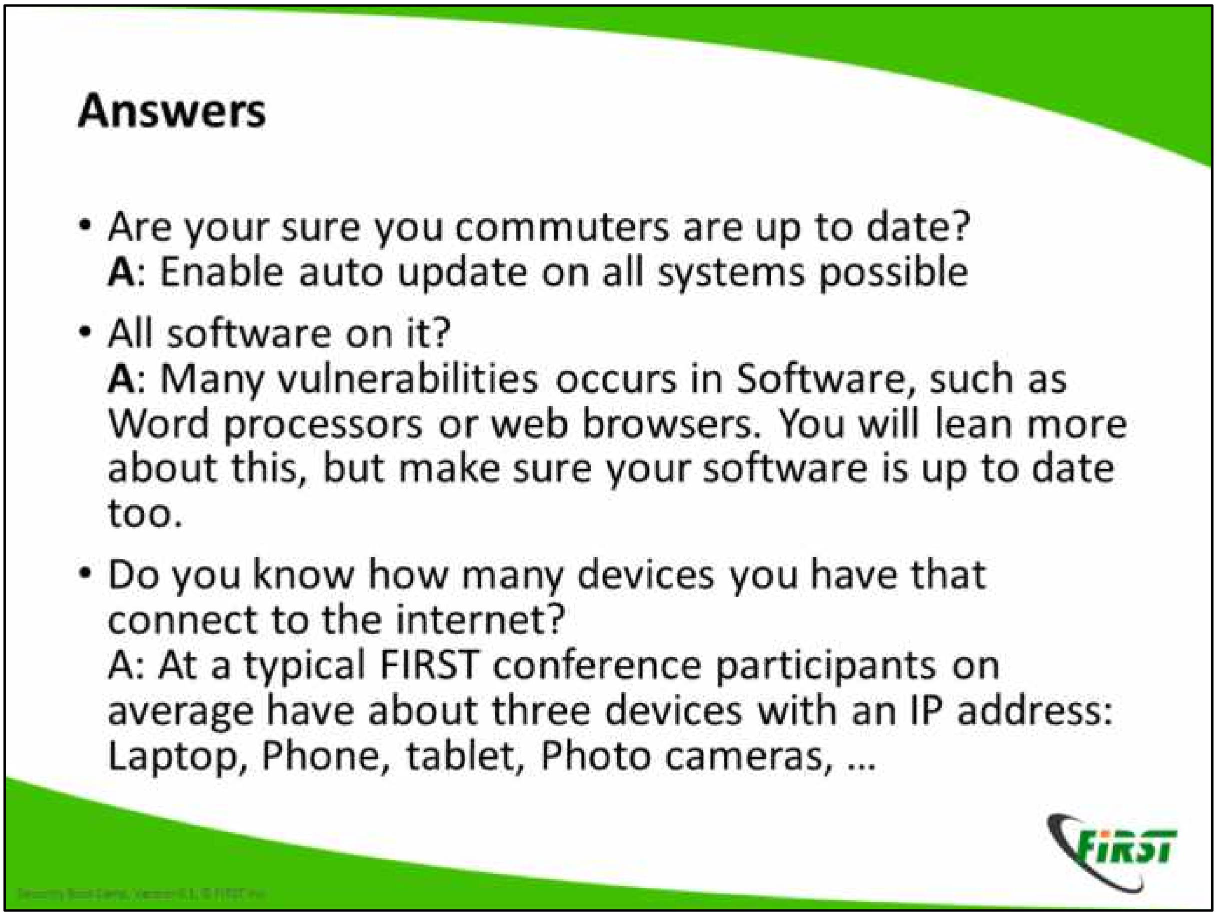
- Have you ever been affected by a virus?
- Do you know what 2 factor authentication is?
- Do you use 2 factor authentication?
- Are your sure you commuters are up to date?
- All software on it?
- Do you know how many devices you have that connect to the internet?

In a classroom situation ask people to group according to answers. In the Video training ask people to reflect abut these question themselves.



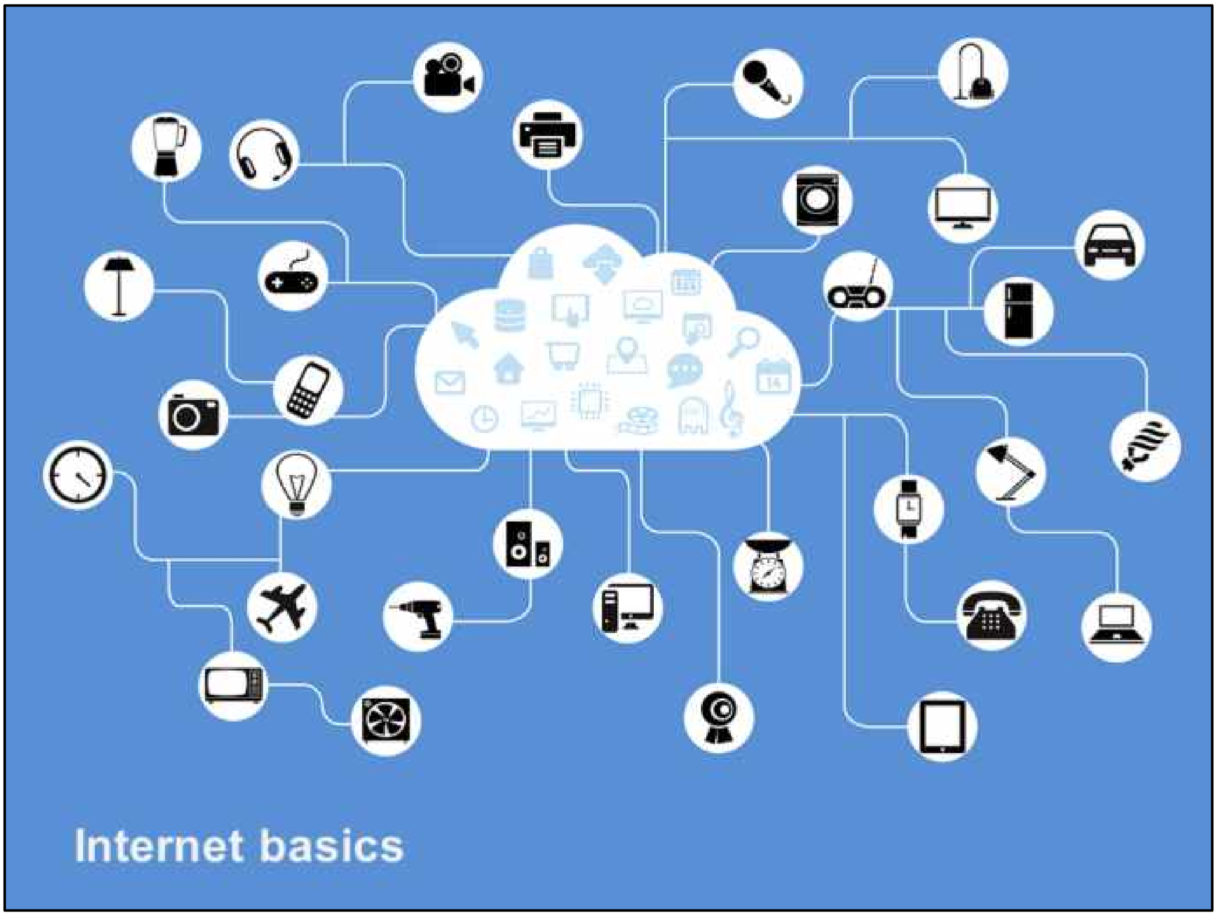
Answers

- Have you ever been affected by a virus?
  A: Chances are you have: In some countries nearly 50% of the devices are infected with some form of malware
- Do you know what 2 factor authentication is?
  A: @FA requires a second factor, besides a password, to authenticate to a service, e.g. a smart card, or a code sent by SMS. Thus a compromised password sill does not let an attacker access your data.
- Do you use 2 factor authentication?
  A: You should: It's easy to use and available in nearly all services today, such as gmail etc.



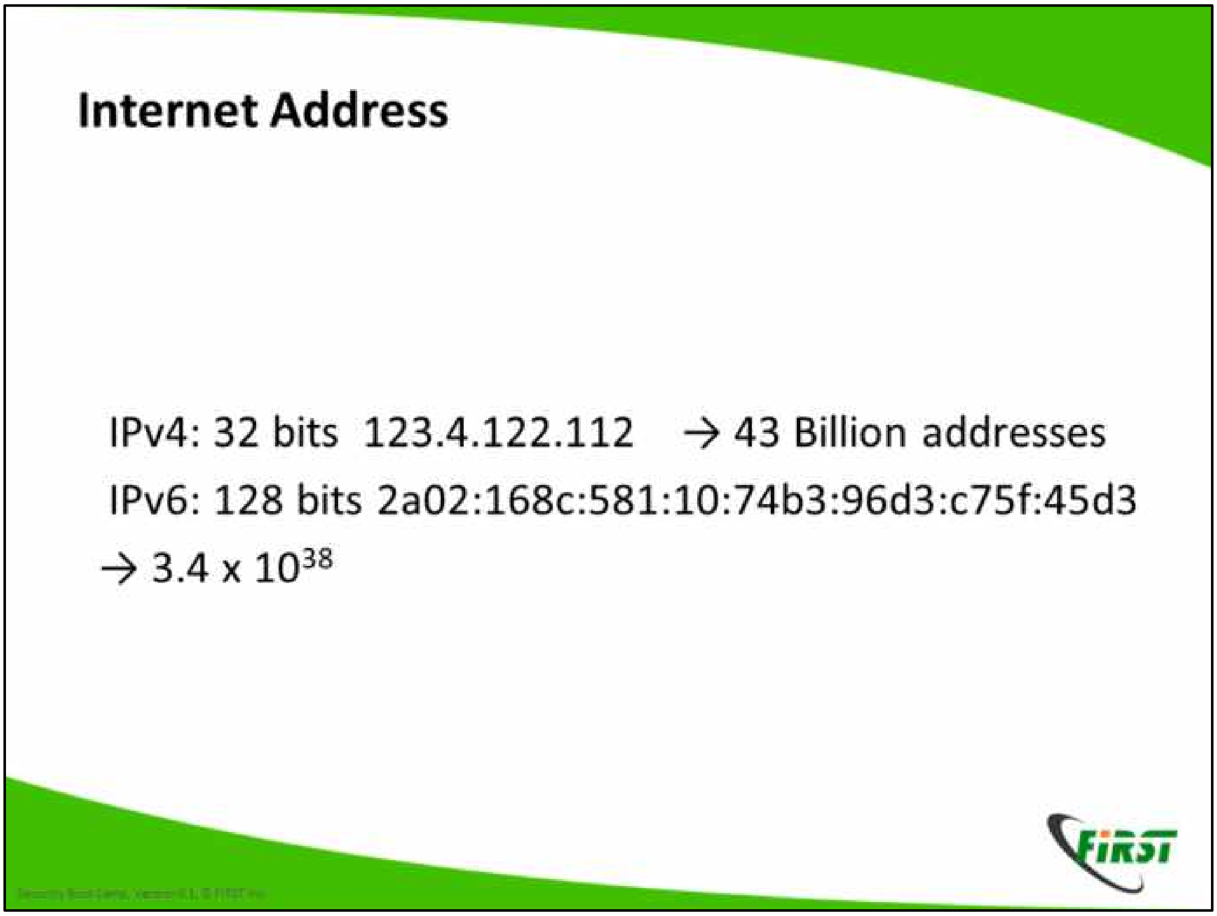
Answers

- Are your sure you commuters are up to date?
  A: Enable auto update on all systems possible
- All software on it?
  A: Many vulnerabilities occurs in Software, such as Word processors or web browsers. You will lean more about this, but make sure your software is up to date too.
- Do you know how many devices you have that connect to the internet?
  A: At a typical FIRST conference participants on average have about three devices with an IP address: Laptop, Phone, tablet, Photo cameras, …



Internet basics

Image: CC0 https://pixabay.com/en/network-iot-internet-of-things-782707/



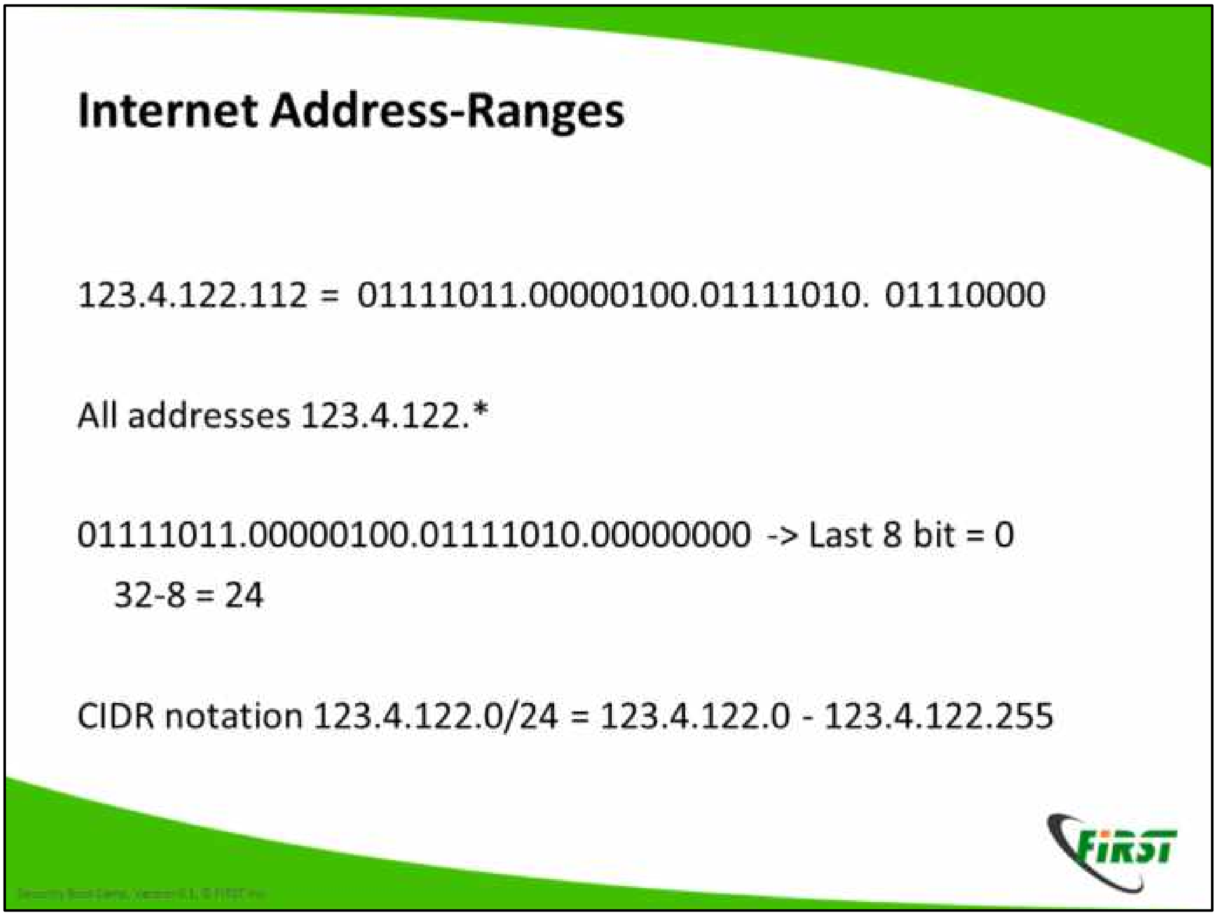
Internet Address

IPv4: 32 bits 123.4.122.112 → 43 Billion addresses

IPv6: 128 bits 2a02:168c:581:10:74b3:96d3:c75f:45d3

→ 3.4×10^{38}

The basic addressing element in the internet is the, well, internet address. Most devices use IPv4 addresses, which have run out.
The IPv6, some tomes called new internet protocol, even though it about as old as the IPv4 protocol uses 128 bits, which allows for plenty of addresses. But this protocol, because it's a bit more complicated is not yet widely used.



Internet Address-Ranges

123.4.122.112 = 01111011.0000100.01111010. 01110000

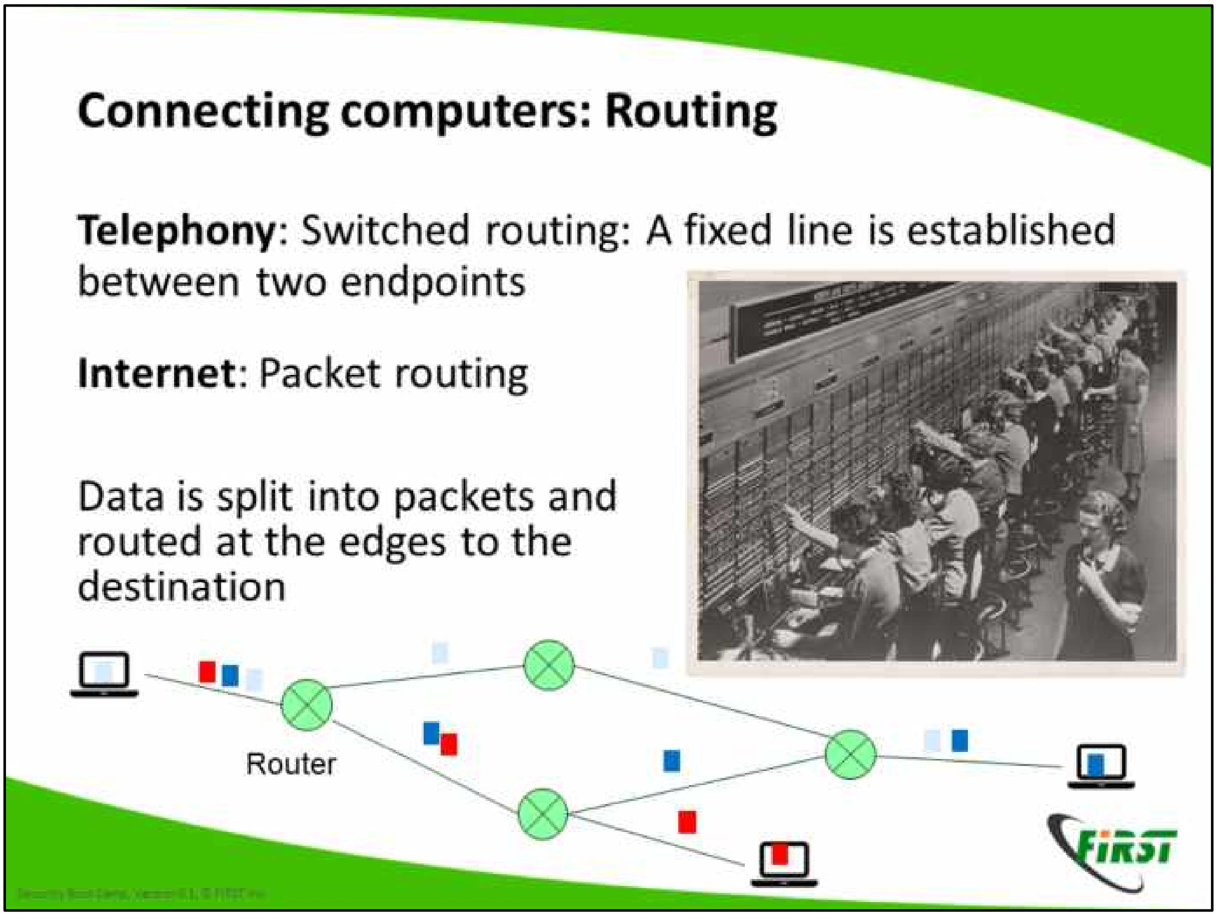
All addresses 123.4.122.*

01111011.00000100.01111010.00000000 -> Last 8 bit = 0

32-8 = 24

CIDR notation 123.4.122.0/24 = 123.4.122.0 - 123.4.122.255

We often need to to have more than just one address, namely a collection or network of addresses (e.g. all computers on this floor). For this we use the cidr notation. It’s based on binary arithmetic and thus suitable for computers to work with.



Connecting computers: Routing

Telephony: Switched routing: A fixed line is established between two endpoints

Internet: Packet routing

Data is split into packets and routed at the edges to the destination

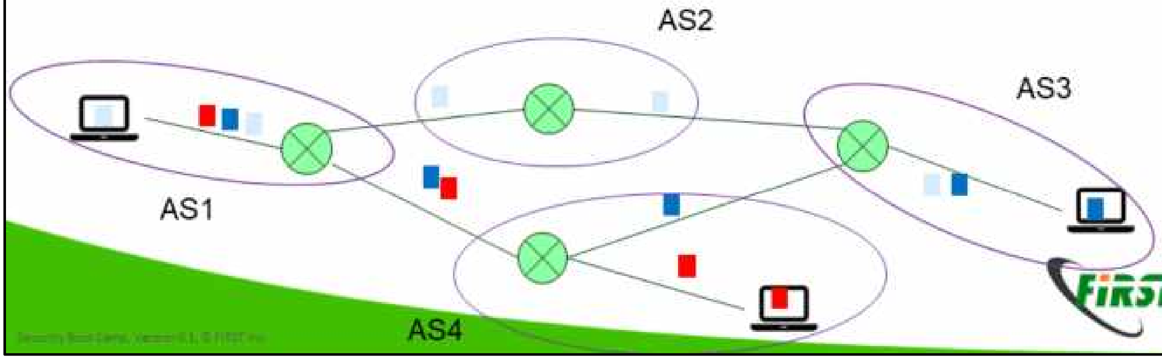
In classical telephony a standing connection is established between two endpoints. In the internet however information is separated into chunks (a few hundred bytes), called packets. These are transported to a router, a computer specialized in handling this packet. It contains huge tables for all internet addresses that tell him where to send it. Once he figures out which the next router is the packet is handed over, until it reaches its final destination. This is much more efficient then a switched network, as a connection does not tie up resources and endpoints can have many connections open at the same time. (Just send out packets to different destinations.

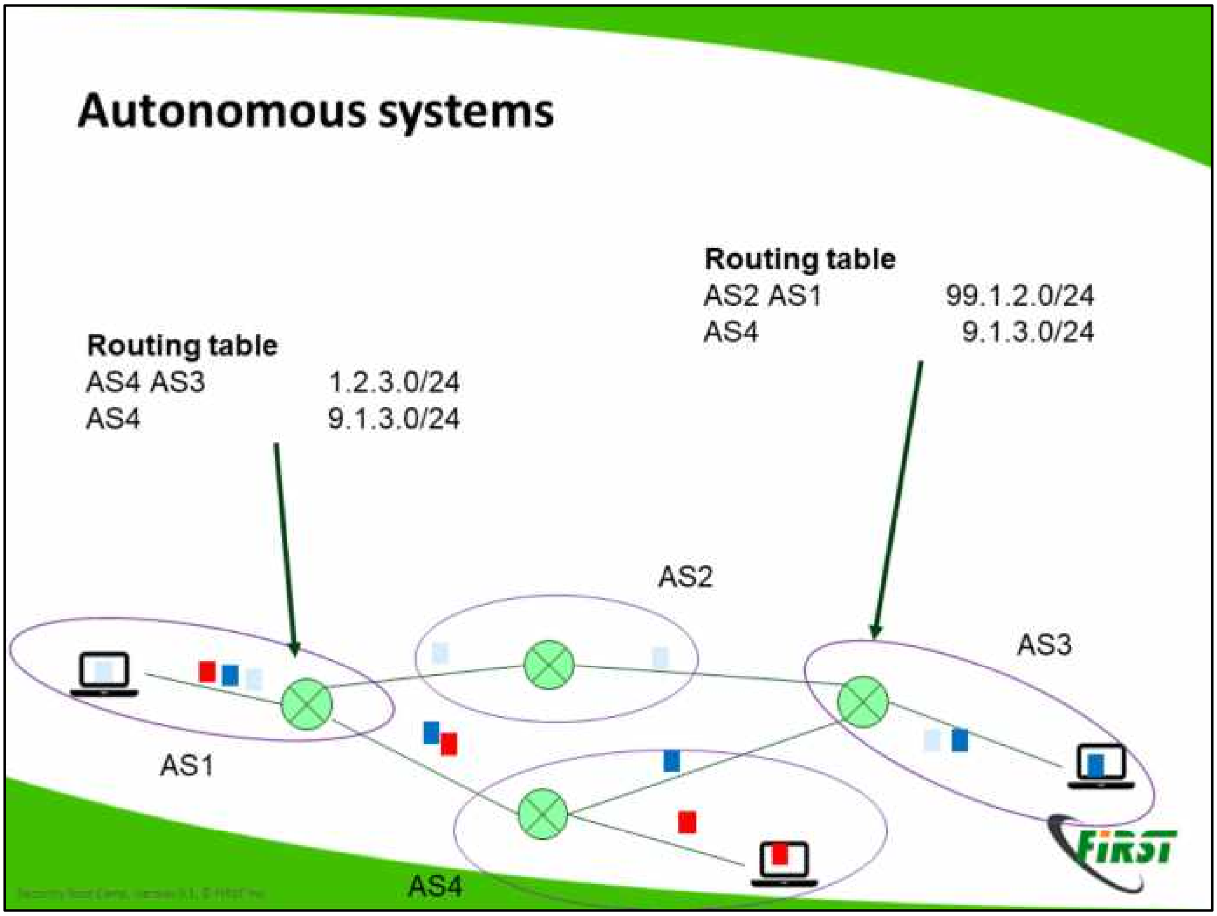
Note, that the reply does not necessarily need to travel the same way

Copyright Foto: The U.S. National Archives @ Flickr Commons

Autonomous systems

Organisations typically manage many address ranges. These are collected into so called autonomous systems (AS)





Autonomous systems

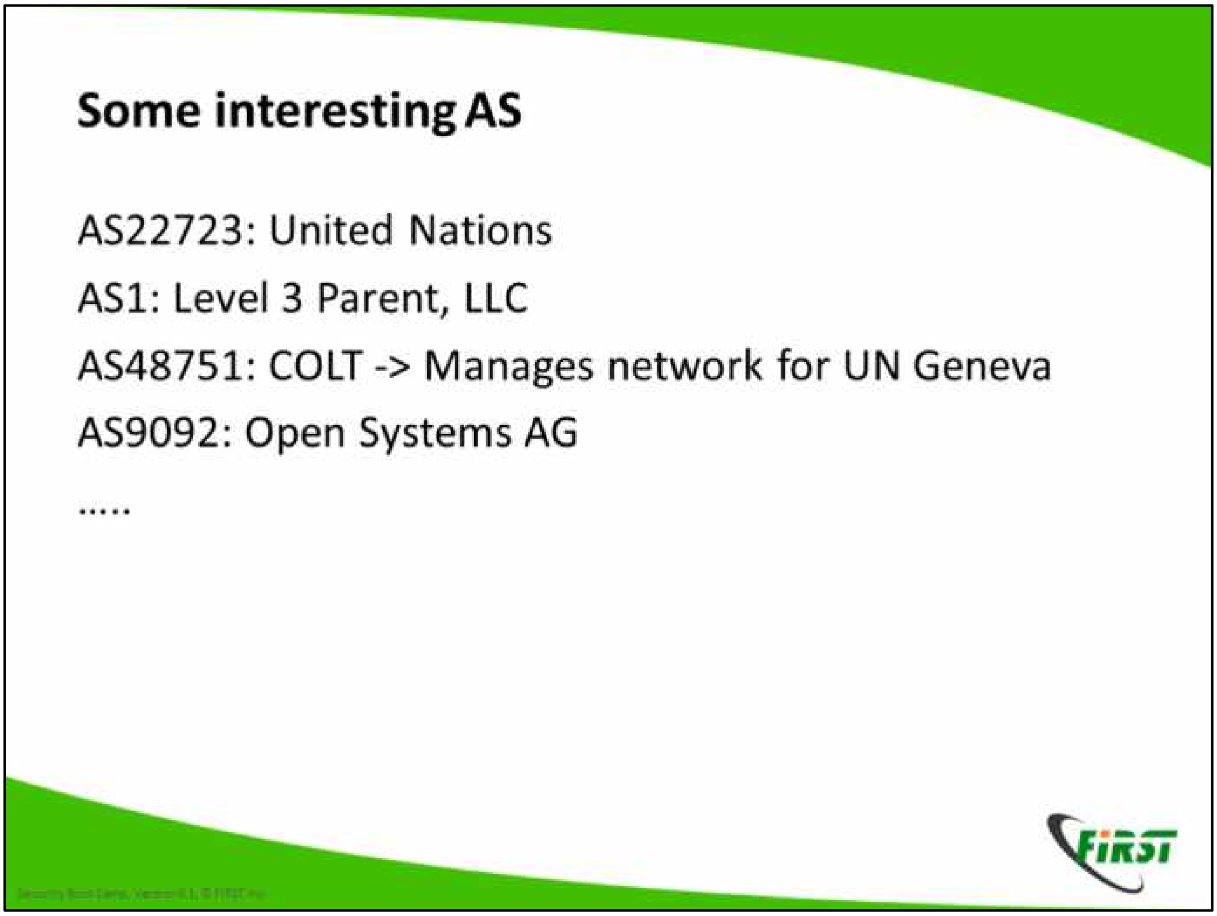
Routing table

AS4 AS3	1.2.3.0/24
AS4	9.1.3.0/24

Routing table

AS2 AS1	99.1.2.0/24
AS4	9.1.3.0/24

Routers now which network knows how to pass info on the the destination IP
Routers advertise what info they know (This is called the border gateway protocol, BGP)
Autonomous systems can be very small or very big and are not tied to national boarders, but rather to companies like ISP or organisations, like the UN



Some interesting AS

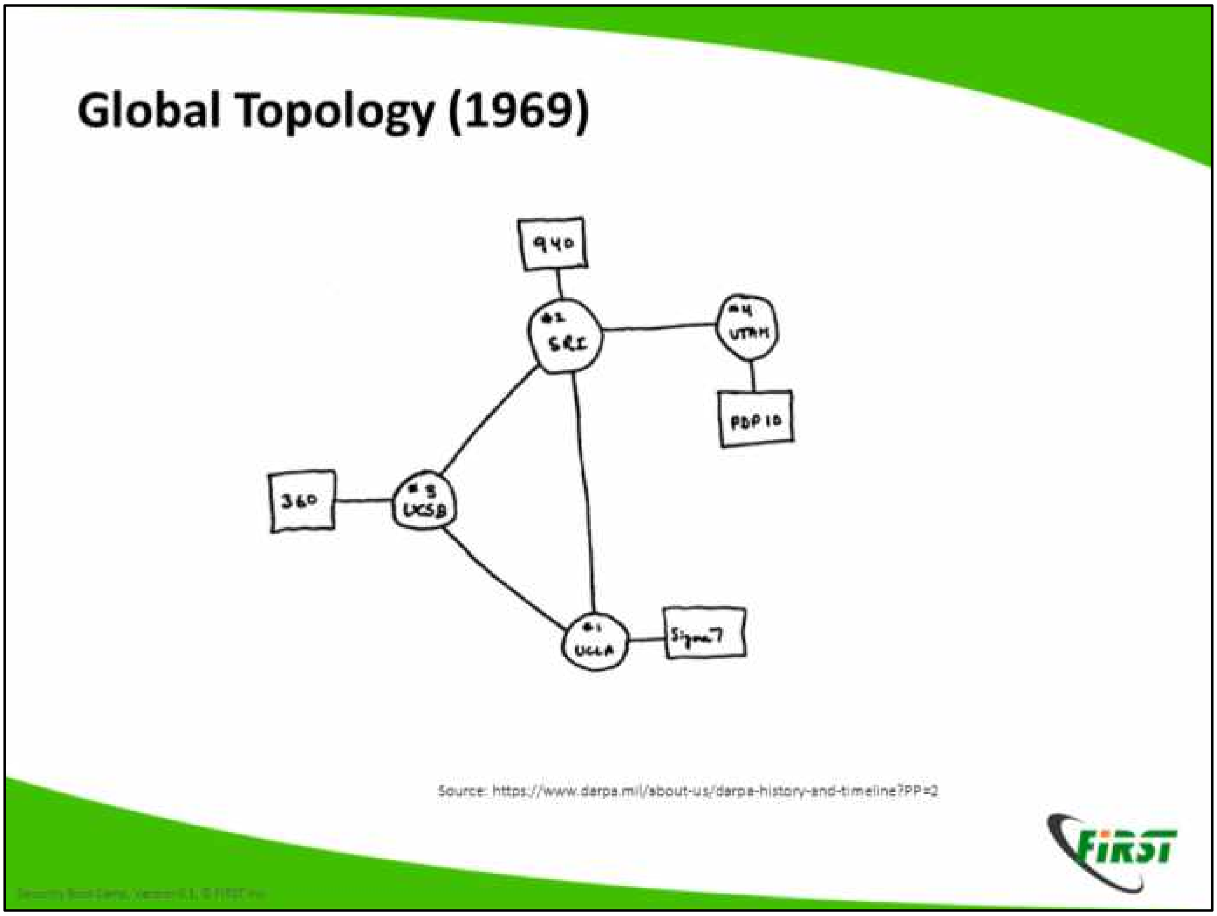
AS22723: United Nations

AS1: Level 3 Parent, LLC

AS48751: COLT -> Manages network for UN Geneva

AS9092: Open Systems AG

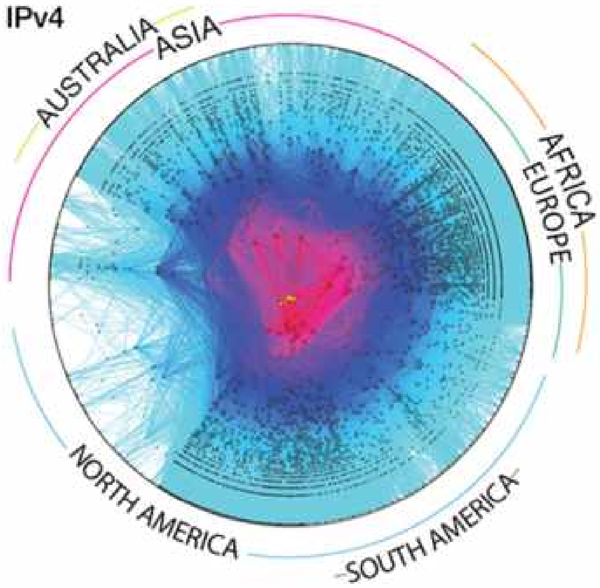
.....



Global Topology (1969)

Source: https://www.darpa.mil/about-us/darpa-history-and-timeline?PP=2

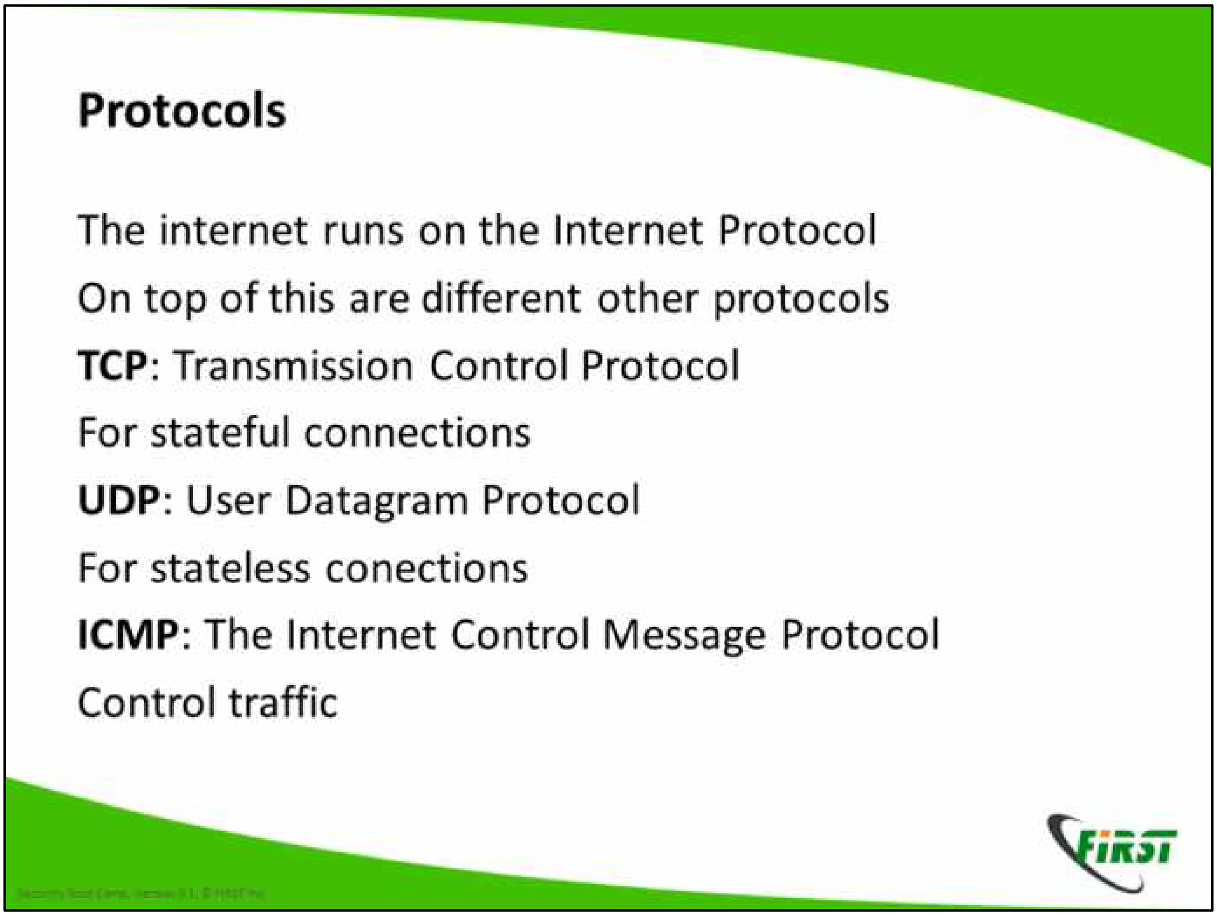
Internet Topology (2017)



Source: https://www.caida.org/research/topology/as_core_network/2015/

Think of an internet address as a street name. There might be different ways to get there and there are different places to go to.

Image: CC0 https://pxhere.com/en/photo/86816



Protocols

The internet runs on the Internet Protocol

On top of this are different other protocols

TCP: Transmission Control Protocol

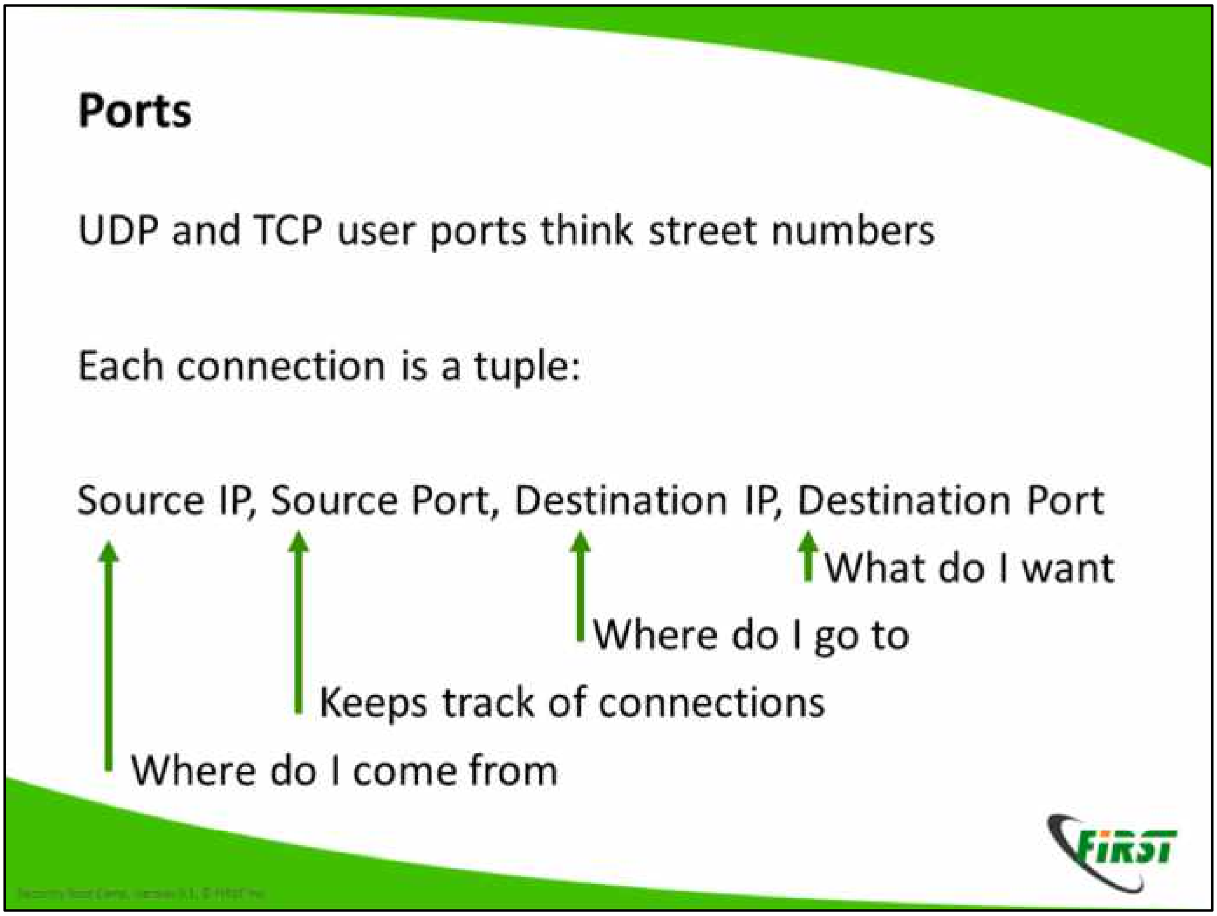
For stateful connections

UDP: User Datagram Protocol

For stateless conections

ICMP: The Internet Control Message Protocol

Control traffic



Ports

UDP and TCP user ports think street numbers

Each connection is a tuple:

Source IP, Source Port, Destination IP, Destination Port

What do I want

Where do I go to

Keeps track of connections

Where do I come from

Example https:

165.156.40.27:7550 -> 172.217.168.36:443

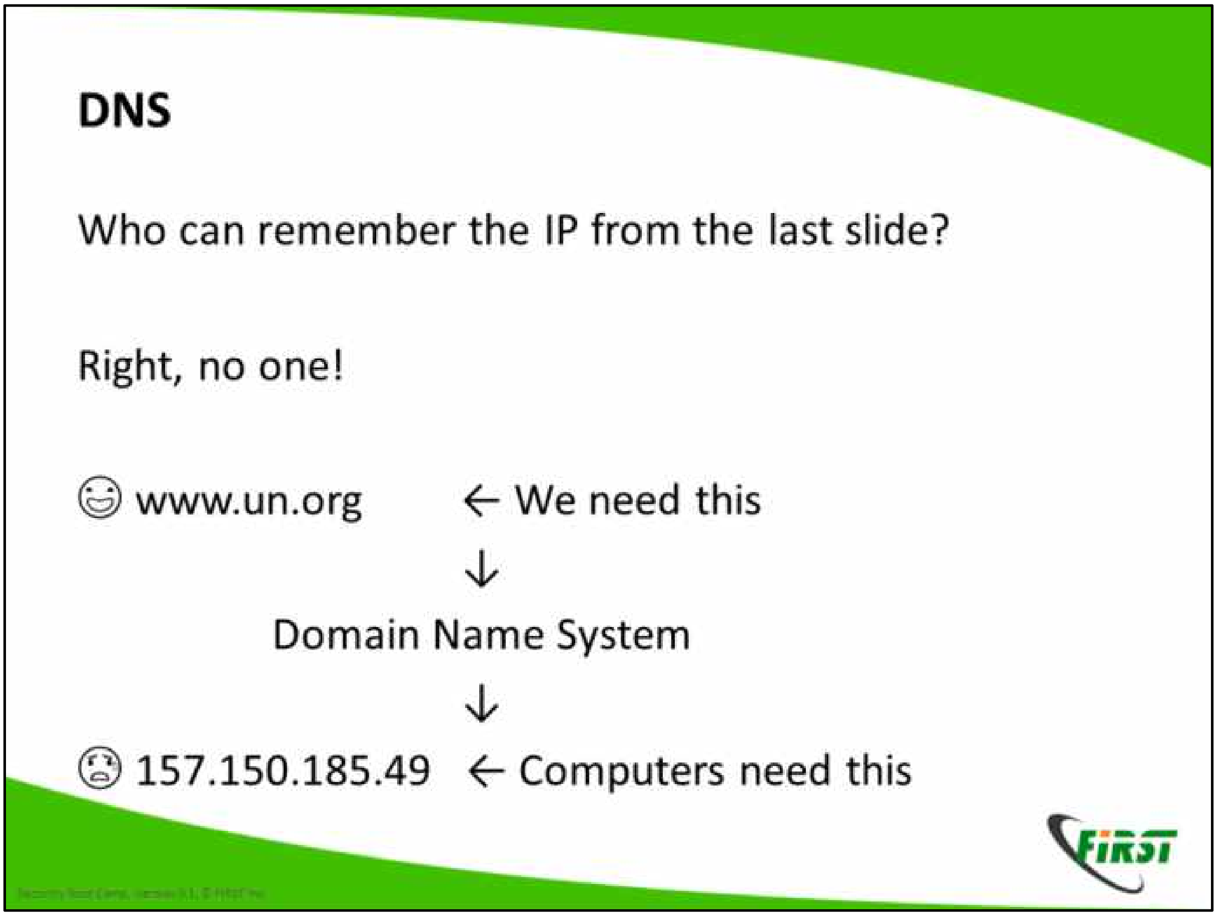
172.217.168.36: www.google.com

443: https

Others:

25: smtp →Simple mail transfer protocol

80: http (without the s for secure)



DNS

Who can remember the IP from the last slide?

Right, no one!

😃 www.un.org ← We need this

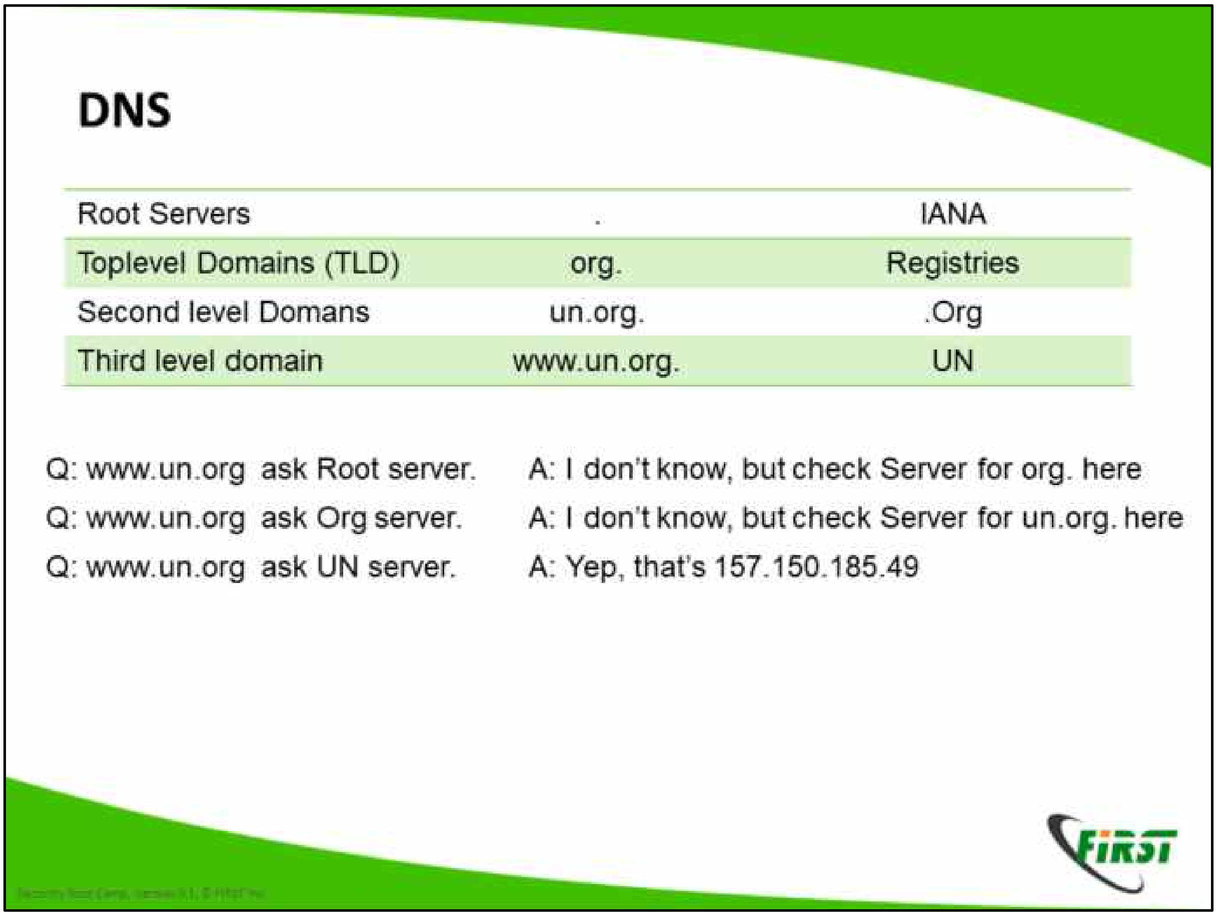
↓

Domain Name System

↓

😨 157.150.185.49 ← Computers need this

The DNS is a globa distributed hierarchical database. For each level there is a server responsible



DNS

Root Servers	.	IANA
Toplevel Domains (TLD)	org.	Registries
Second level Domans	un.org.	.Org
Third level domain	www.un.org.	UN

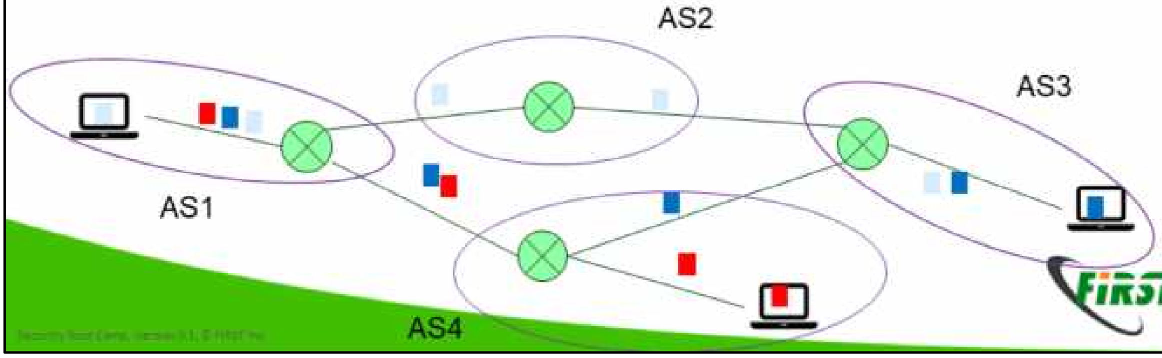
Q: www.un.org ask Root server. A: I don't know, but check Server for org. here

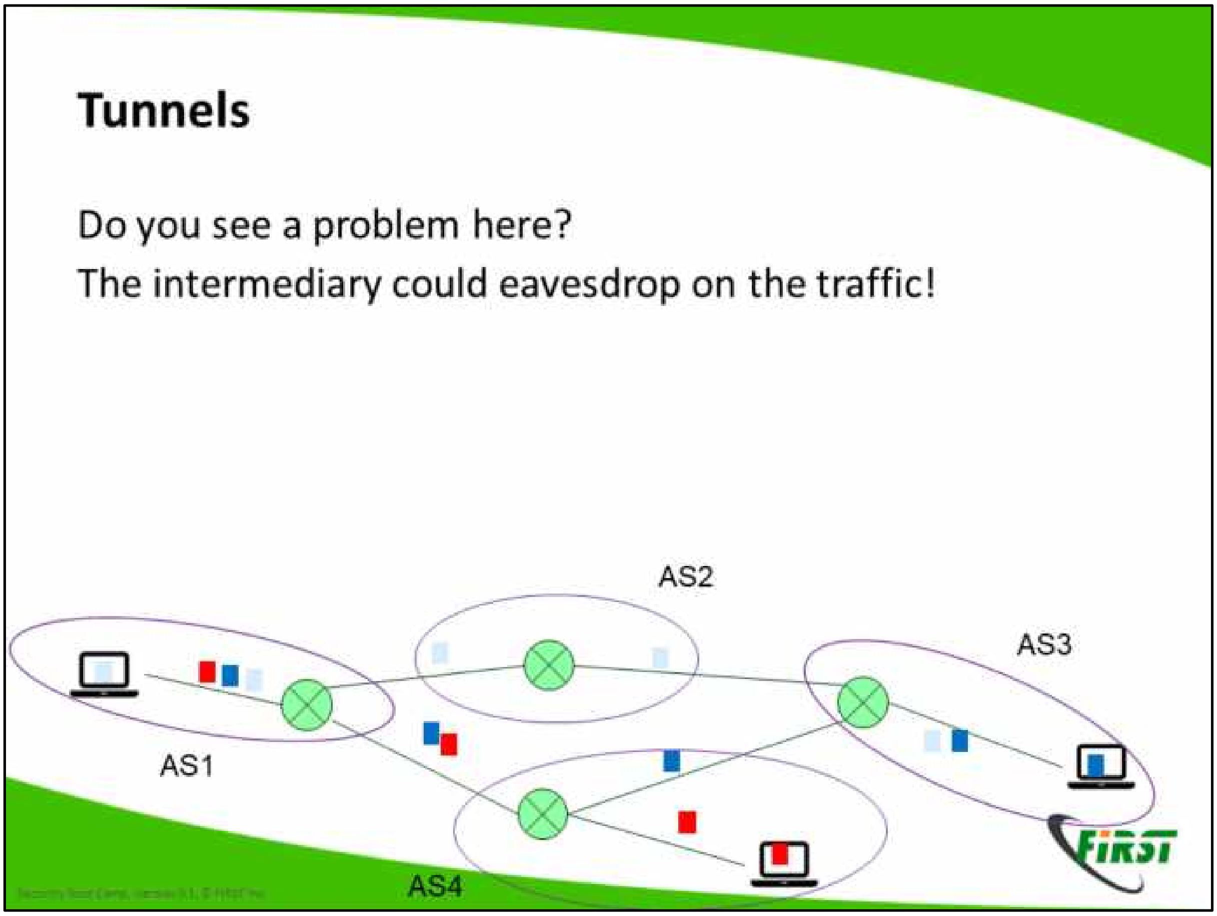
Q: www.un.org ask Org server. A: I don't know, but check Server for un.org. here

Q: www.un.org ask UN server. A: Yep, that's 157.150.185.49

Tunnels

Do you see a problem here?





Tunnels

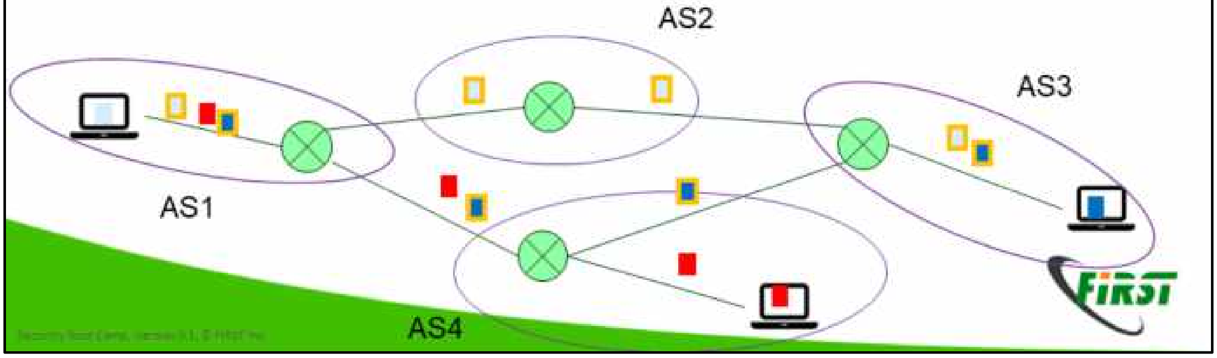
Do you see a problem here?

The intermediary could eavesdrop on the traffic!

(one) Solution: VPNs

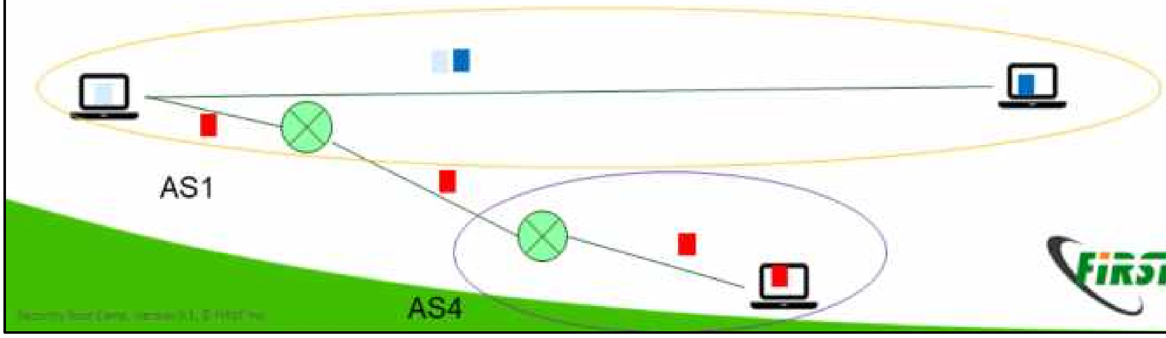
Encrypt traffic to specific destinations

→ VPN: Virtual Private Network



VPN Point of View

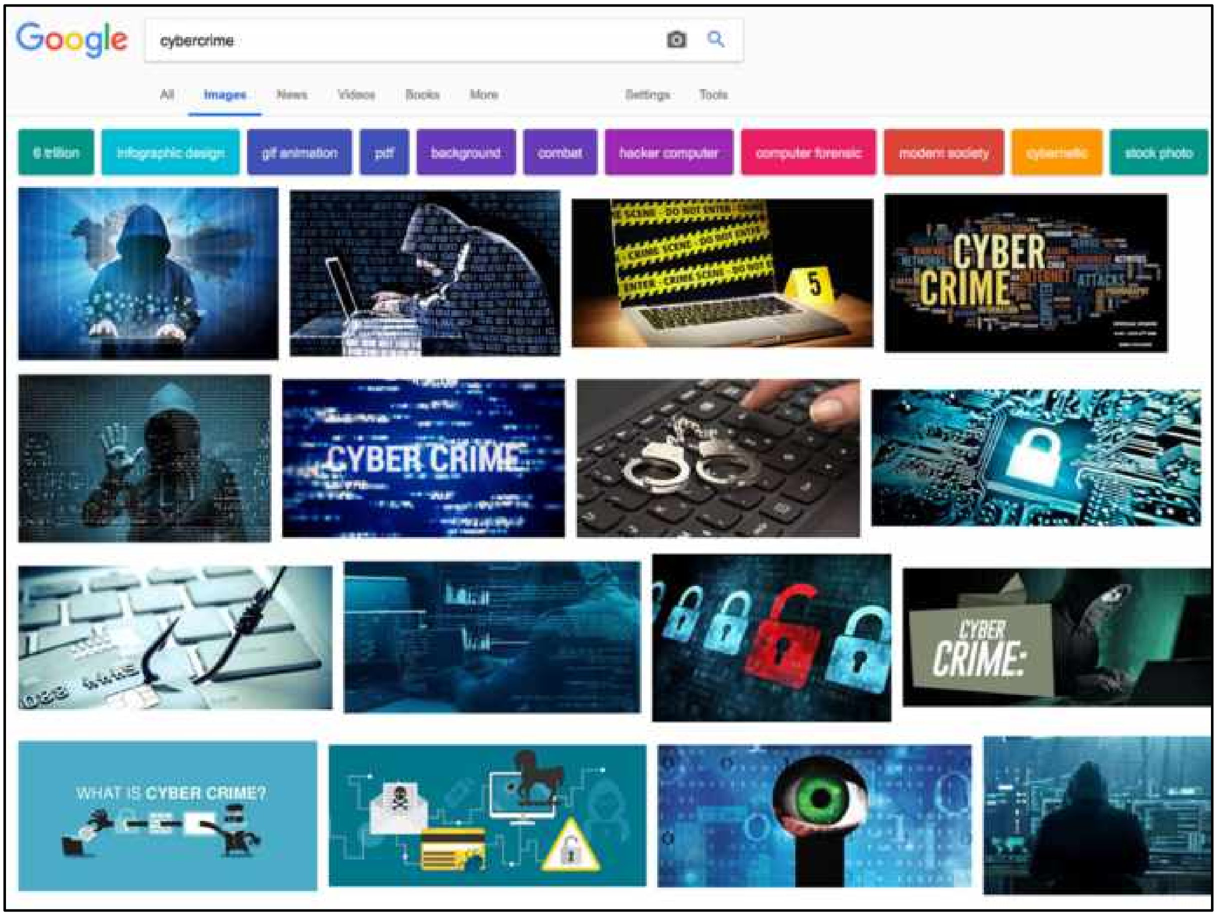
It looks as if all computers are in the same network



The dark side of the net

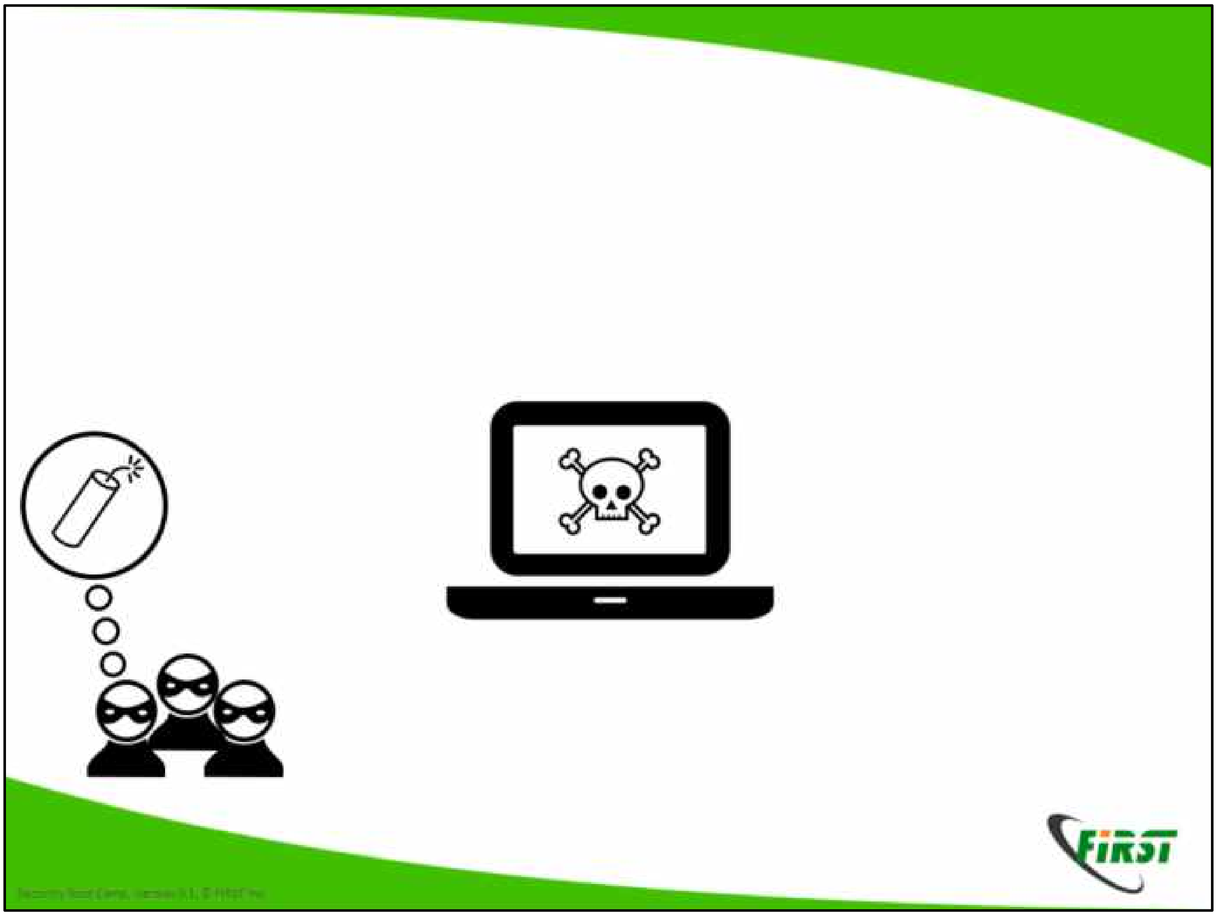
CC2.0 Diogo Rodrigues Gonçalves

Actors & Tactics

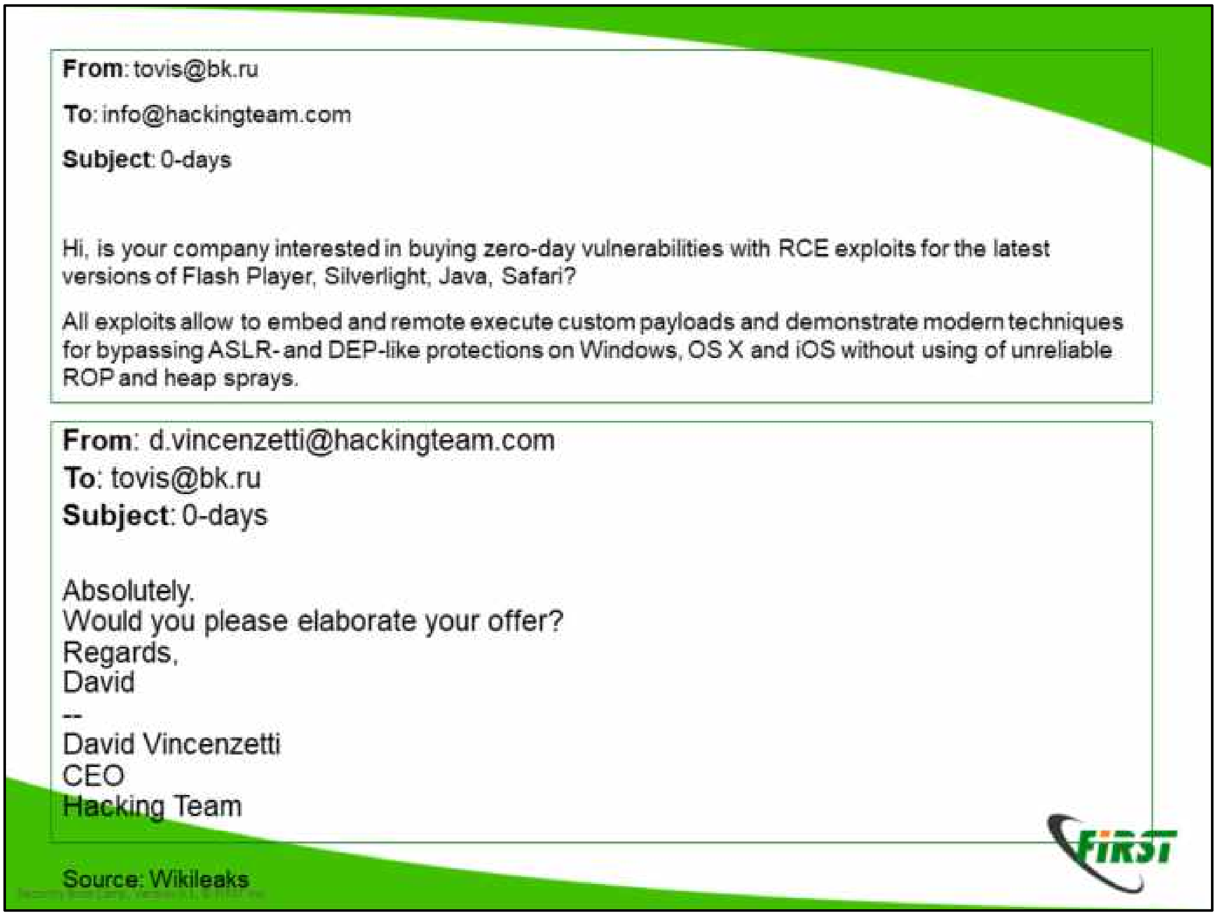


Cybercrime is a big word, Google finds a gazillion hits. But are the bad guys really waring hoodies and baklavas?
Do they steal punched credit cards? What the heck are they doing?

What are we talking about? This story begins, like so many in this game, with a hacked device. But what does it take to to hack this device? And why would you do this? Let’s explore these questions briefly!



This you do with so called injects, all available in the under ground market.



From: tovis@bk.ru

To: info@hackingteam.com

Subject: 0-days

Hi, is your company interested in buying zero-day vulnerabilities with RCE exploits for the latest versions of Flash Player, Silverlight, Java, Safari?

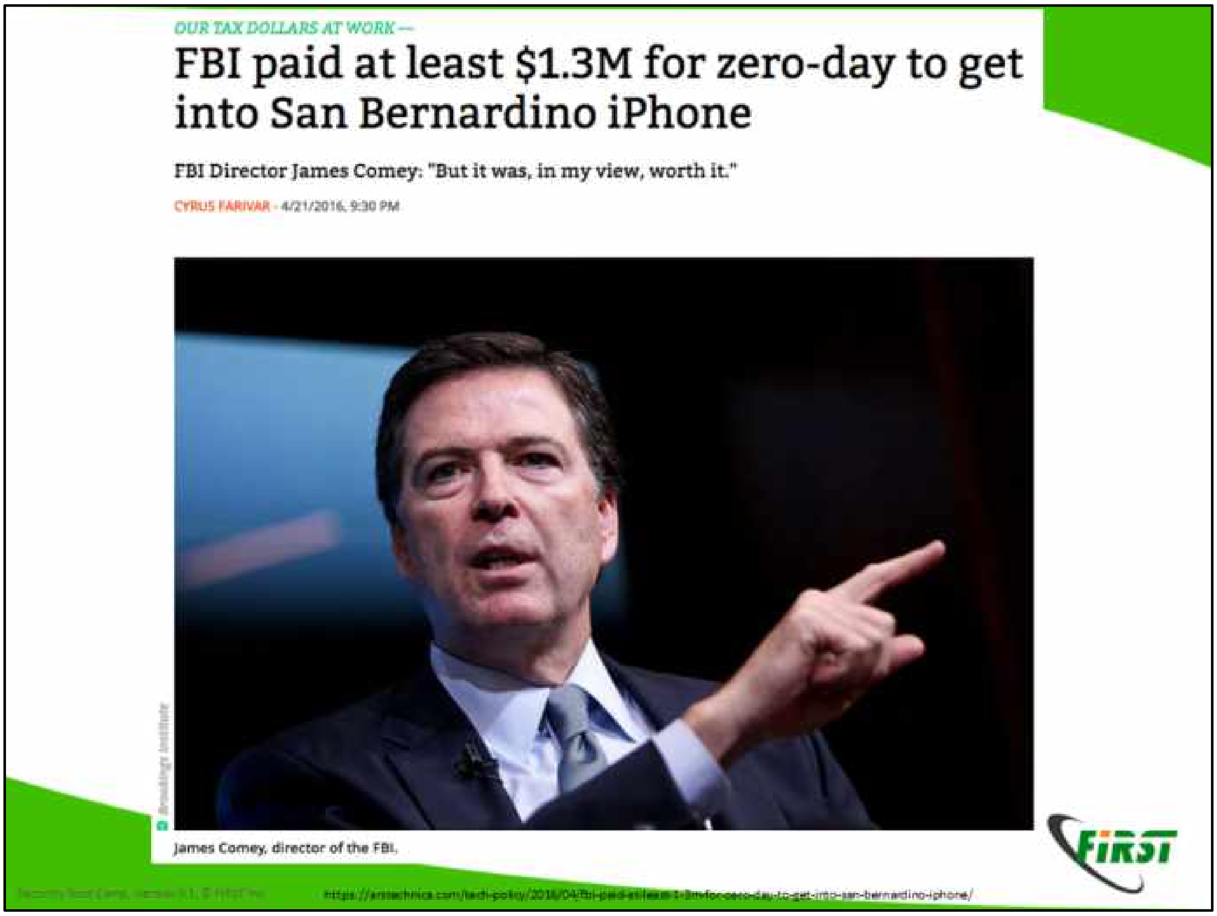
All exploits allow to embed and remote execute custom payloads and demonstrate modern techniques for bypassing ASLR- and DEP-like protections on Windows, OS X and iOS without using of unreliable ROP and heap sprays.

From: d.vincenzetti@hackingteam.com
To: tovis@bk.ru
Subject: 0-days

Absolutely.
Would you please elaborate your offer?
Regards,
David
--
David Vincenzetti
CEO
Hacking Team

Source: Wikileaks

Here is an example of how 0-days are traded. This is a shady Business with many plyers, most notably government players



OUR TAX DOLLARS AT WORK —

FBI paid at least $1.3M for zero-day to get into San Bernardino iPhone

FBI Director James Comey: "But it was, in my view, worth it."

CYRUS FARIVAR - 4/21/2016, 9:30 PM

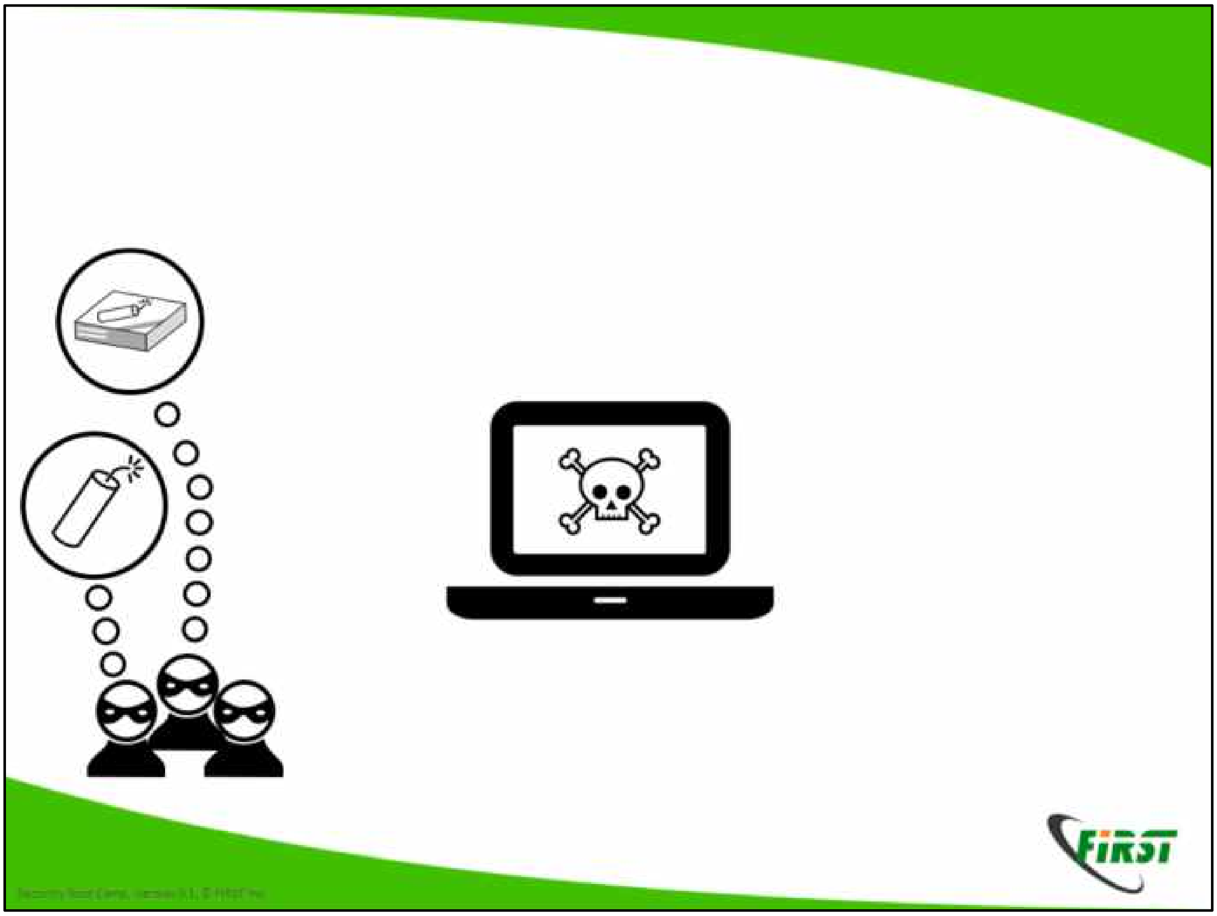
Brookings Institute

James Comey, director of the FBI.

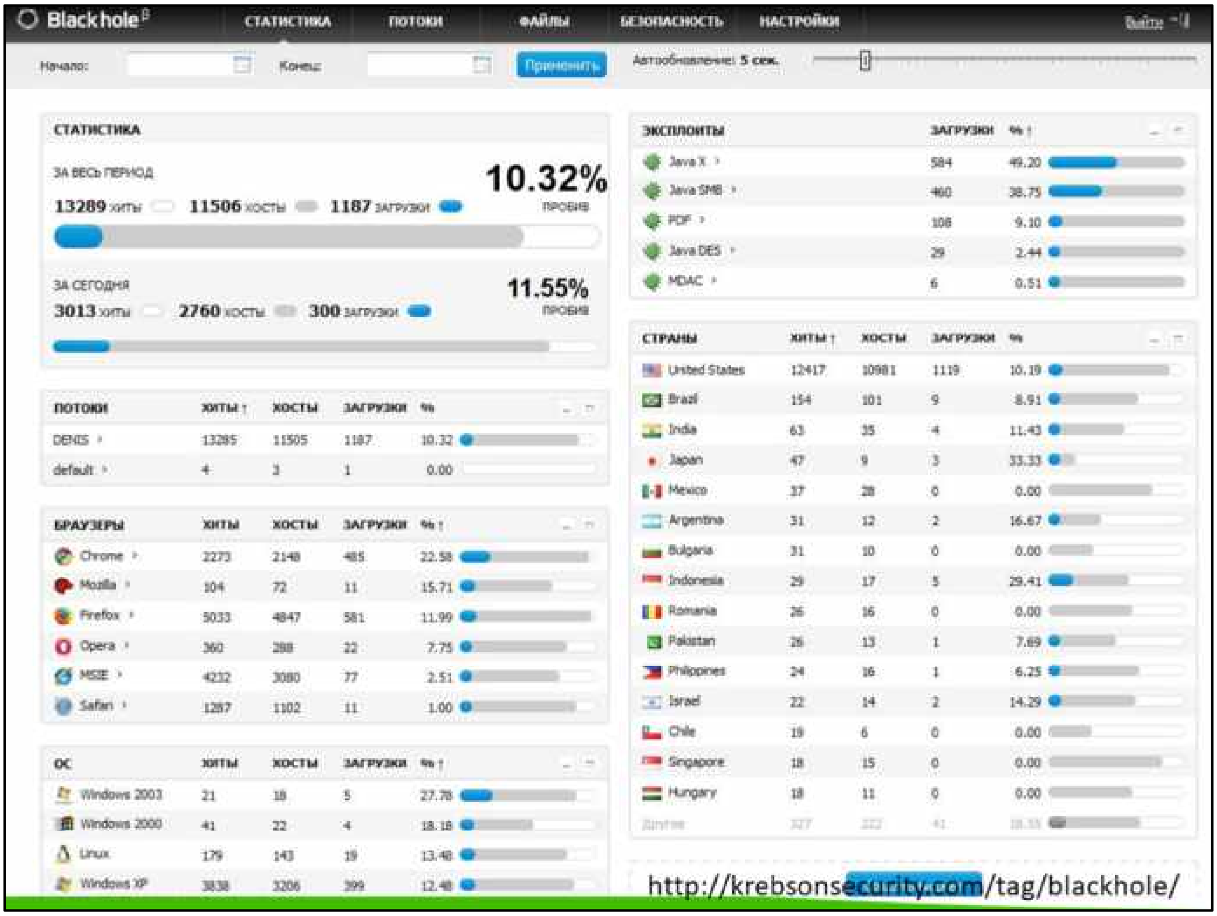
https://arstechnica.com/tech-policy/2016/04/fbi-paid-at-least-1-3m-for-zero-day-to-get-into-san-bernardino-iphone/

E.g. the FBI payed 1.3 Million dollars to read one phone. This is a fairly high price, typically the prices are around 250‘000 $

Older exploits (~ 6 mt – 1.5 years) go for a few thousend $$



So no you can exploit. You now need an infrastructure to deliver these to victim systems. This is a service, which goes under the name exploit kits.



Начало: Конец: Автообновление: **5 сек.**

СТАТИСТИКА

ЗА ВЕСЬ ПЕРИОД

13289 хиты **11506** хосты **1187** загрузки

10.32% пробив

ЗА СЕГОДНЯ

3013 хиты **2760** хосты **300** загрузки

11.55% пробив

ПОТОКИ	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
DENIS ›	13285	11505	1187	10.32
default ›	4	3	1	0.00

БРАУЗЕРЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↑
Chrome ›	2273	2148	485	22.58
Mozilla ›	104	72	11	15.71
Firefox ›	5033	4847	581	11.99
Opera ›	360	288	22	7.75
MSIE ›	4232	3080	77	2.51
Safari ›	1287	1102	11	1.00

ОС	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↑
Windows 2003	21	18	5	27.78
Windows 2000	41	22	4	18.18
Linux	179	143	19	13.48
Windows XP	3838	3206	399	12.48

ЭКСПЛОИТЫ	ЗАГРУЗКИ	% ↑
Java X ›	584	49.20
Java SMB ›	460	38.75
PDF ›	108	9.10
Java DES ›	29	2.44
MDAC ›	6	0.51

СТРАНЫ	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
United States	12417	10981	1119	10.19
Brazil	154	101	9	8.91
India	63	35	4	11.43
Japan	47	9	3	33.33
Mexico	37	28	0	0.00
Argentina	31	12	2	16.67
Bulgaria	31	10	0	0.00
Indonesia	29	17	5	29.41
Romania	26	16	0	0.00
Pakistan	26	13	1	7.69
Philippines	24	16	1	6.25
Israel	22	14	2	14.29
Chile	19	6	0	0.00
Singapore	18	15	0	0.00
Hungary	18	11	0	0.00
Другие	327	222	41	18.55

http://krebsonsecurity.com/tag/blackhole/

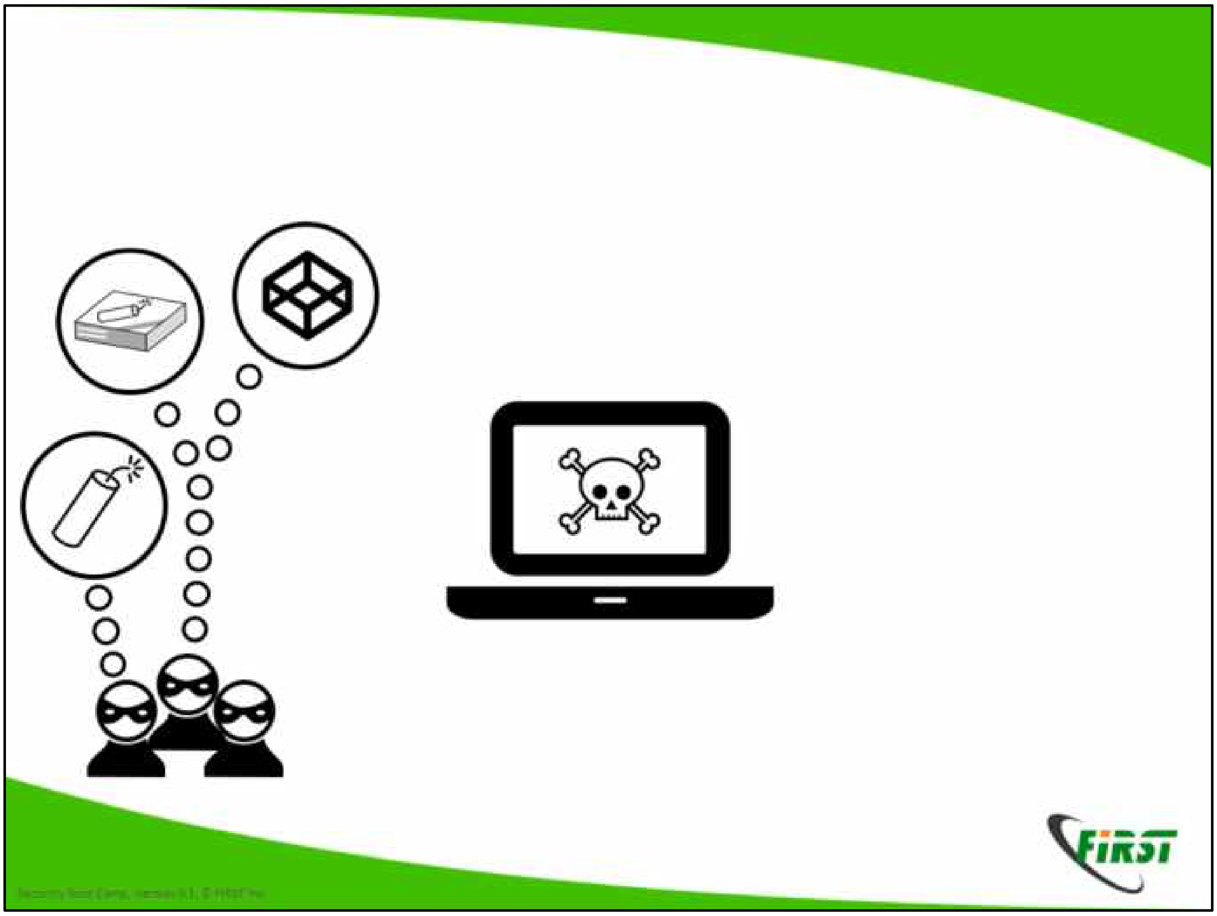
Here an example: It comes with a GUI. You see where computers are hacked, which OS they run etc. Dending on the country you will deliver different malware (or rather you sell the hacked systems to some one else)

Prices: US$ 500 – 700/Monat
Customers: > 1‘000

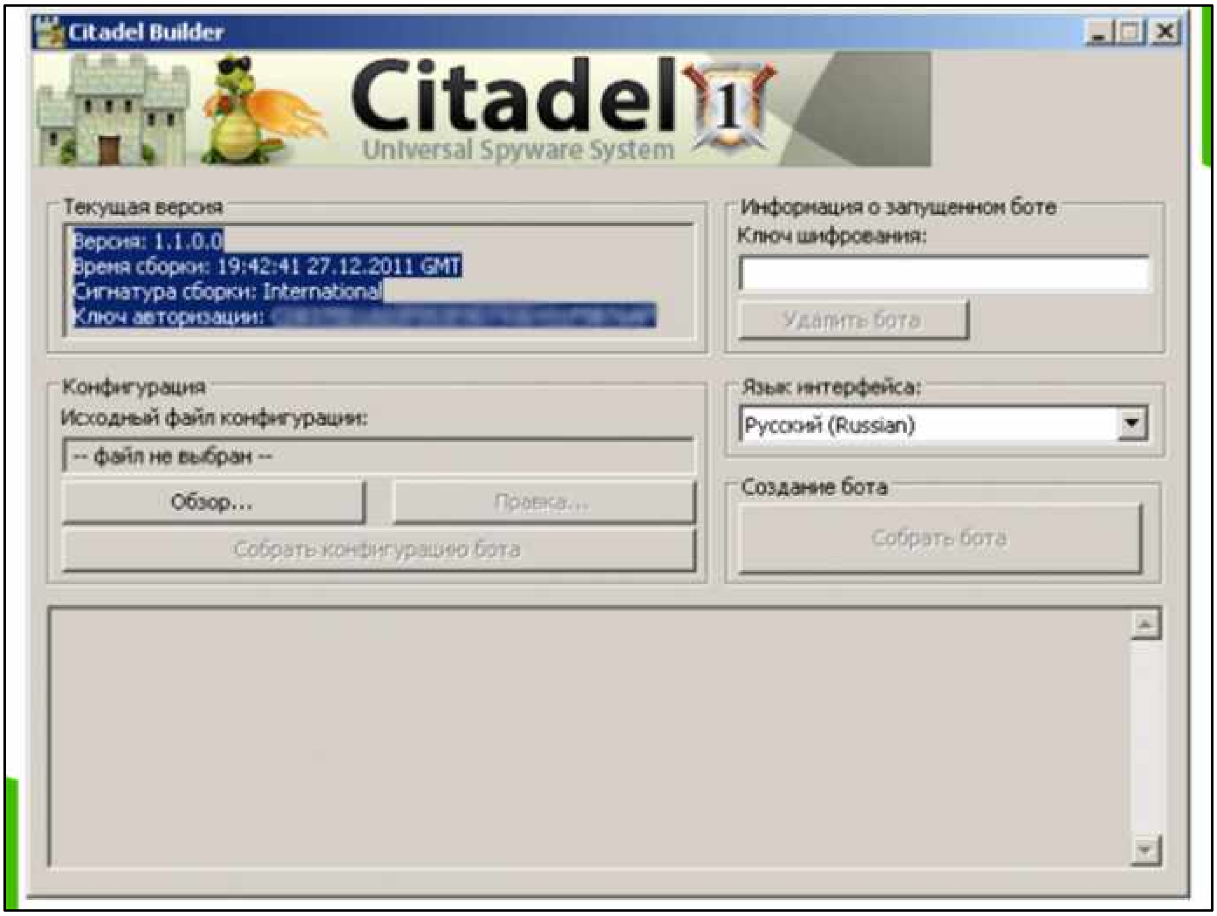
Dimitry Fedotov aka Paunch
Arrested: December 2013

Dimitri‘s Porsche

This is the author of the Blackhole kit.



Now you can start installing malware, that is “viruses” Today they are frameworks that allow you to control the entries system



Текущая версия

Версия: 1.1.0.0
Время сборки: 19:42:41 27.12.2011 GMT
Сигнатура сборки: International
Ключ авторизации: [redacted]

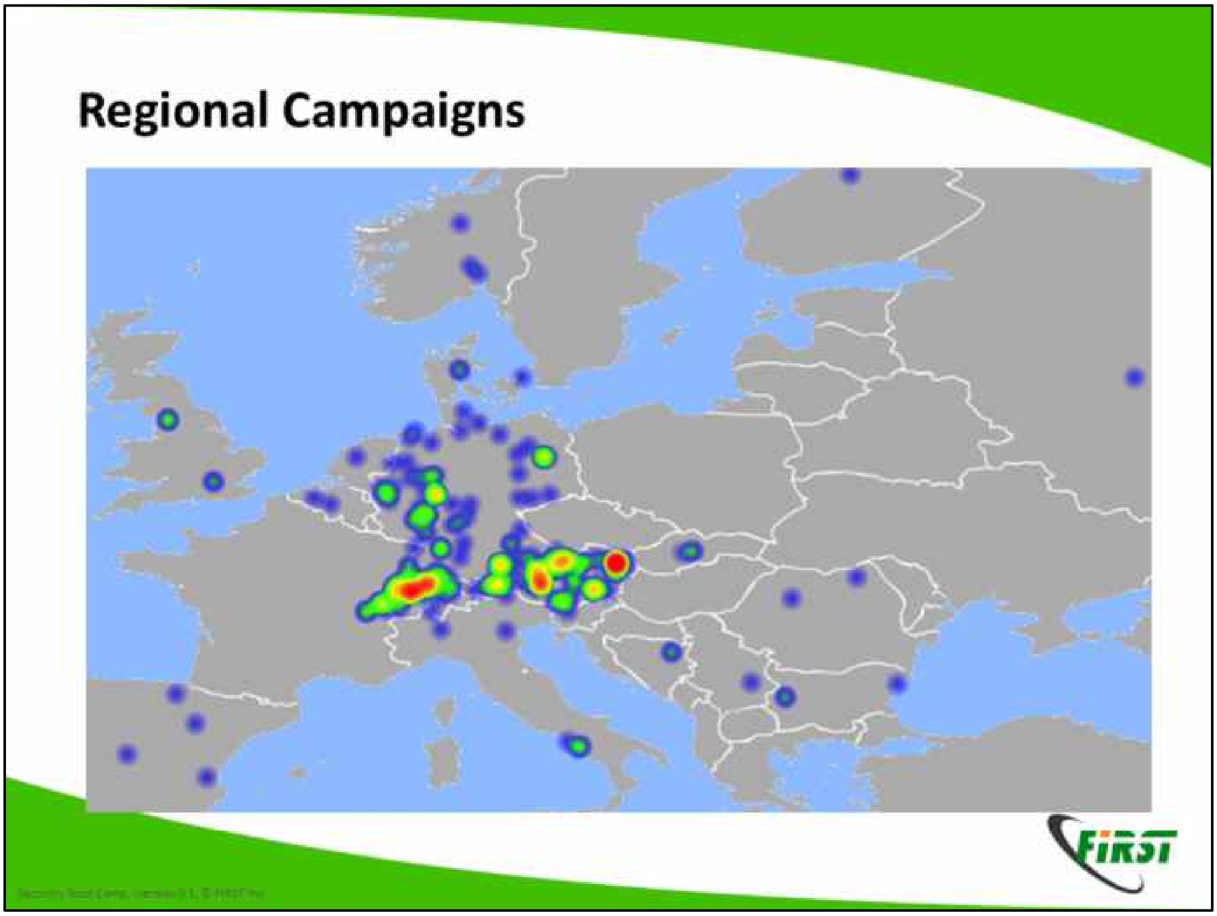
Ключ шифрования:

Конфигурация

Исходный файл конфигурации: -- файл не выбран --

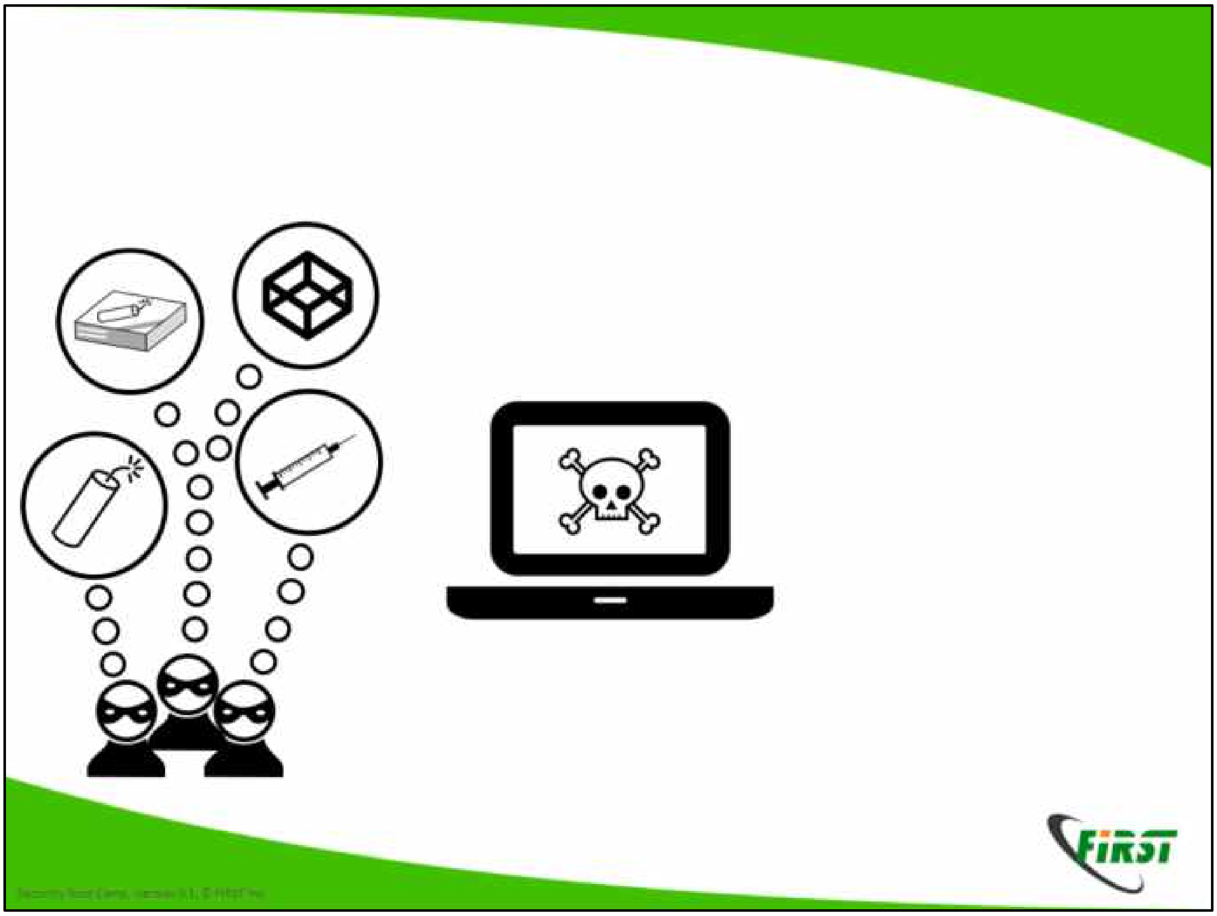
Язык интерфейса: Русский (Russian)

You configure these with GUIs too. These you can buy

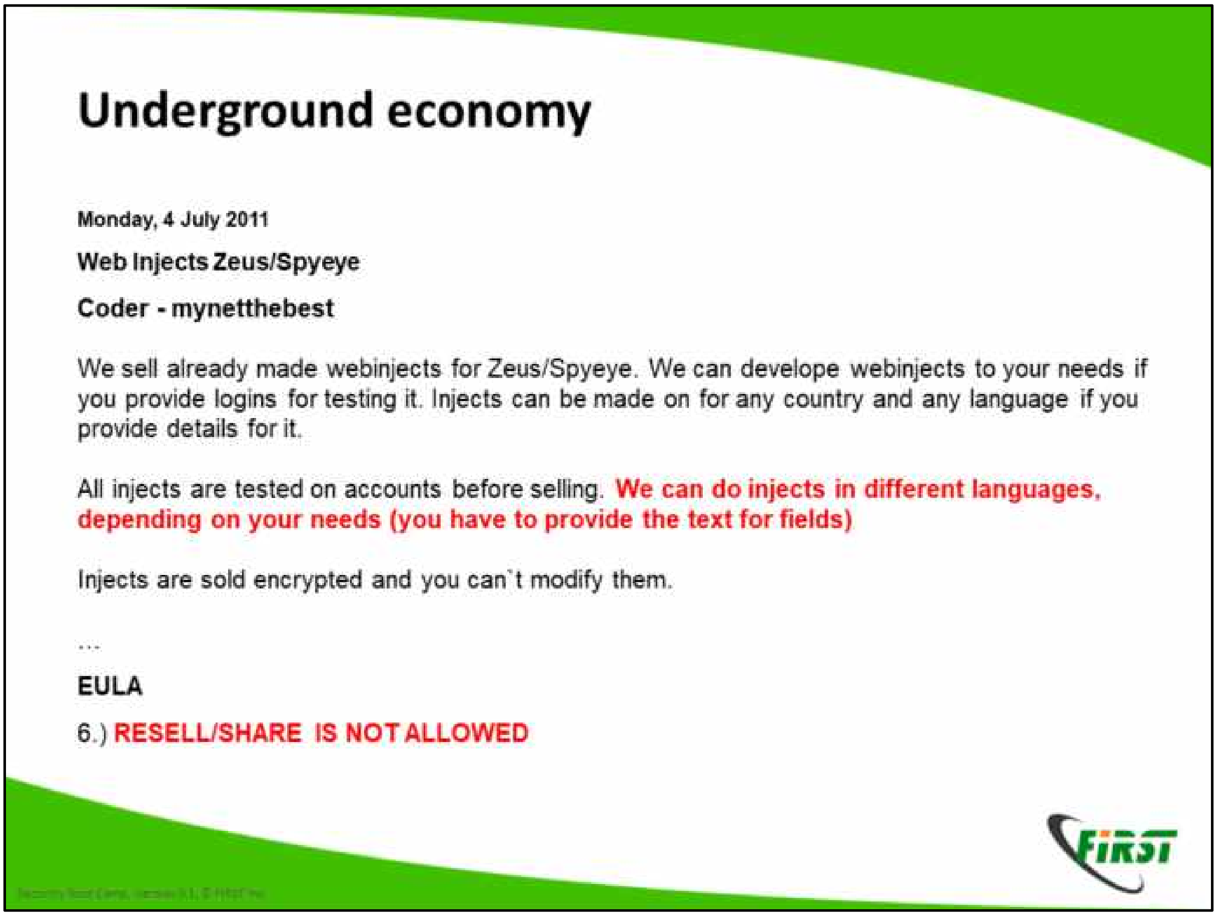


Regional Campaigns

Old times: Author controled all, and had all security researchers at his neck
Today they sell/rent and many different groups operate these.
This is an example of Retefee, a banking trojan, which is mostly active in AT and CH



Finally you need to have software for your exact goal, kind of like an App. These are called injects



Underground economy

Monday, 4 July 2011

Web Injects Zeus/Spyeye

Coder - mynetthebest

We sell already made webinjects for Zeus/Spyeye. We can develope webinjects to your needs if you provide logins for testing it. Injects can be made on for any country and any language if you provide details for it.

All injects are tested on accounts before selling. **We can do injects in different languages, depending on your needs (you have to provide the text for fields)**

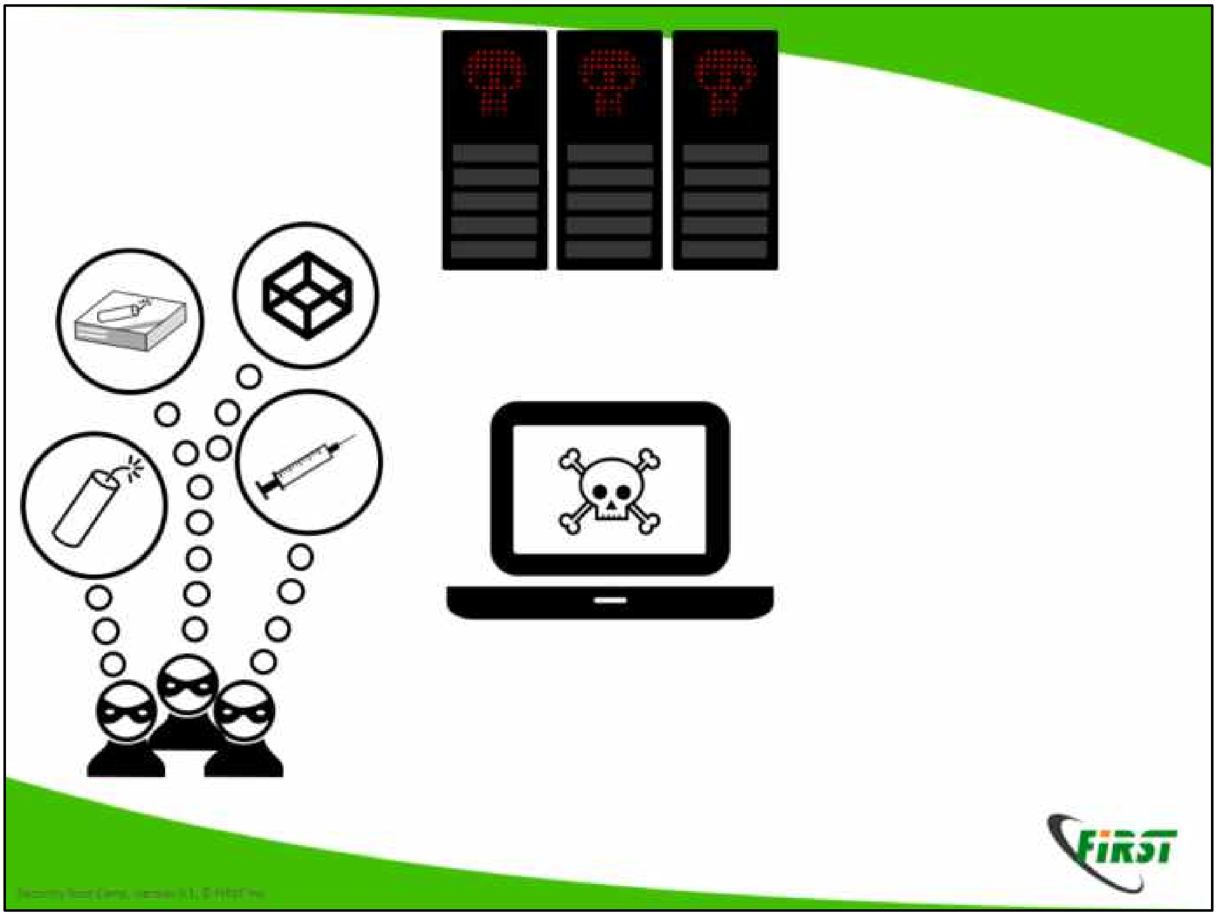
Injects are sold encrypted and you can`t modify them.

...

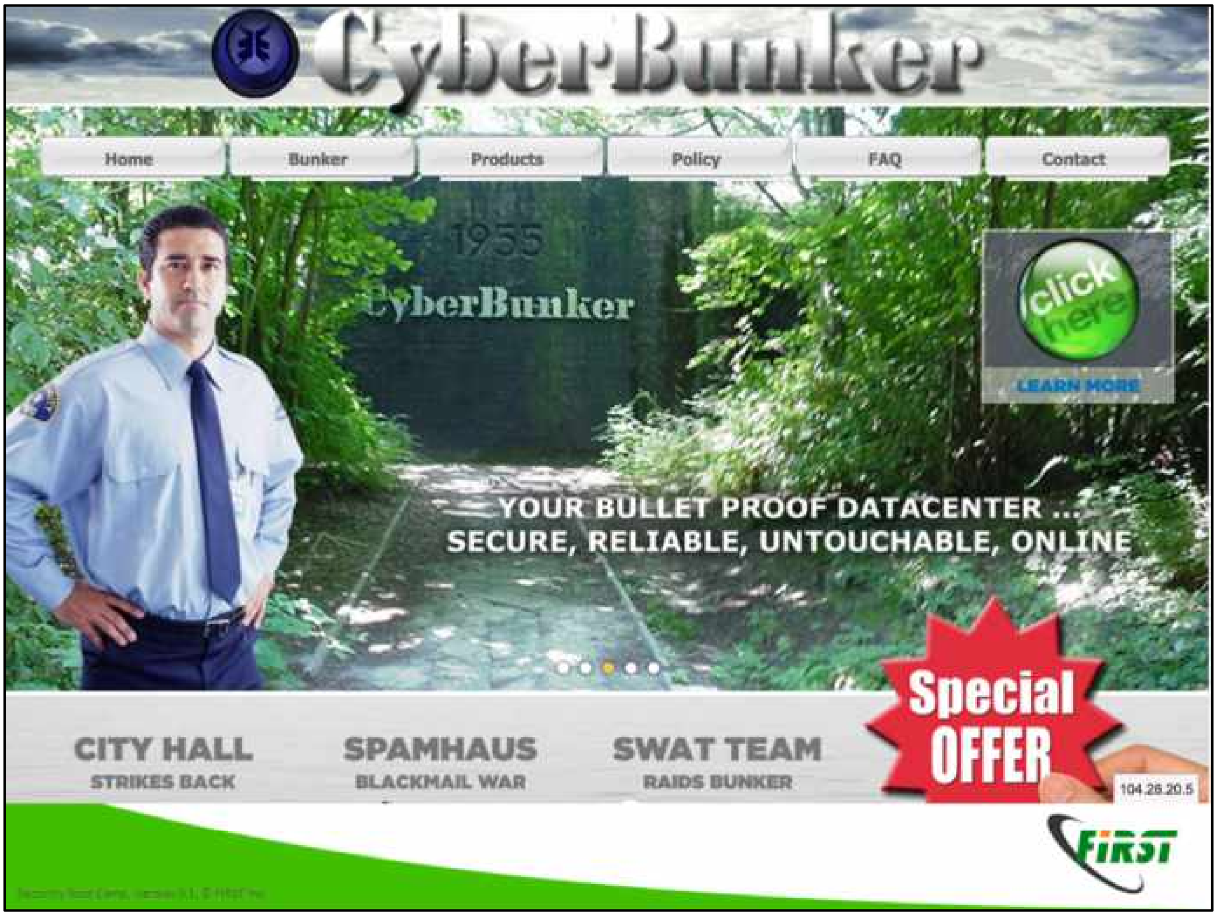
EULA

6.) **RESELL/SHARE IS NOT ALLOWED**

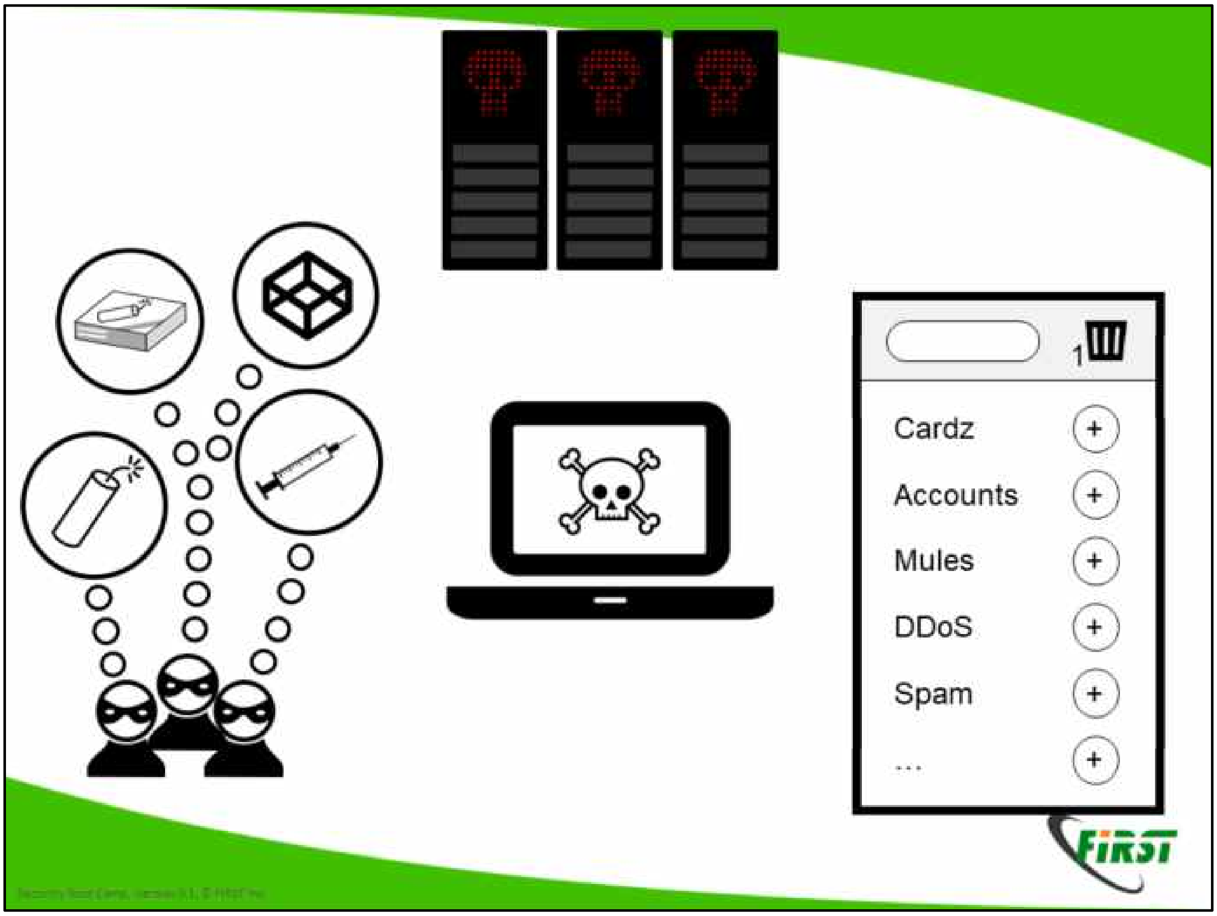
They come with an EULA
Question: How do you enforce this?
Answer: If violation is detected Code is submited to Virus totla -> Next day AV cleans this out.



Now you need hosting infra. -> Bullet proof hosting

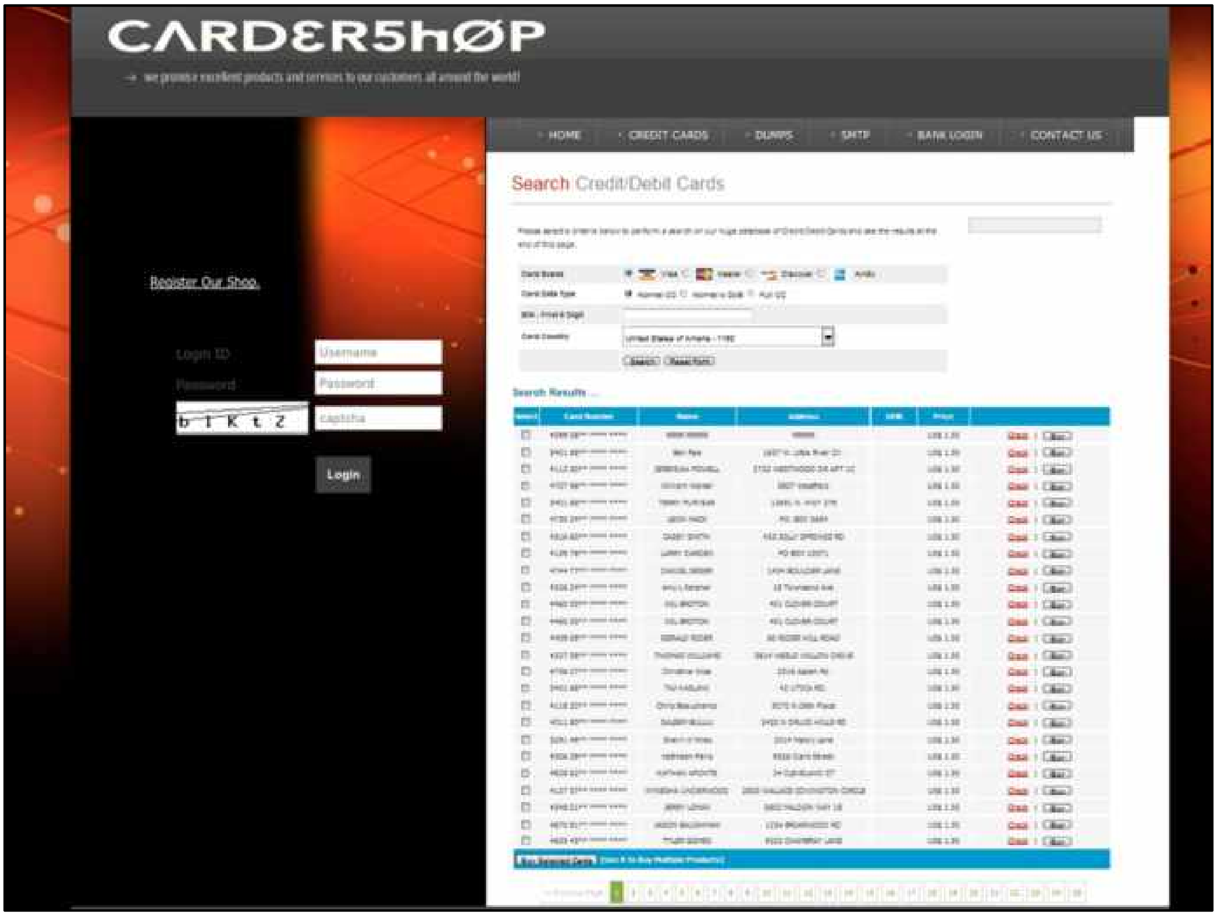


Bullet proof hosting.



Now all is in place and you can start doing bussines:

- Top Credit cards -> How much, do you think, does a fully working CC cost? Answer: USD 7, but 21 for CH CC Those are typically sold in batches of 100 or so on special undergorund markets (think amazon).
- Accounts, such as gmail, etc. Would you like more twitter folowwers? You can get them.



CARDER5hØP

→ we promise excellent products and services to our customers all around the world!

Search Credit/Debit Cards

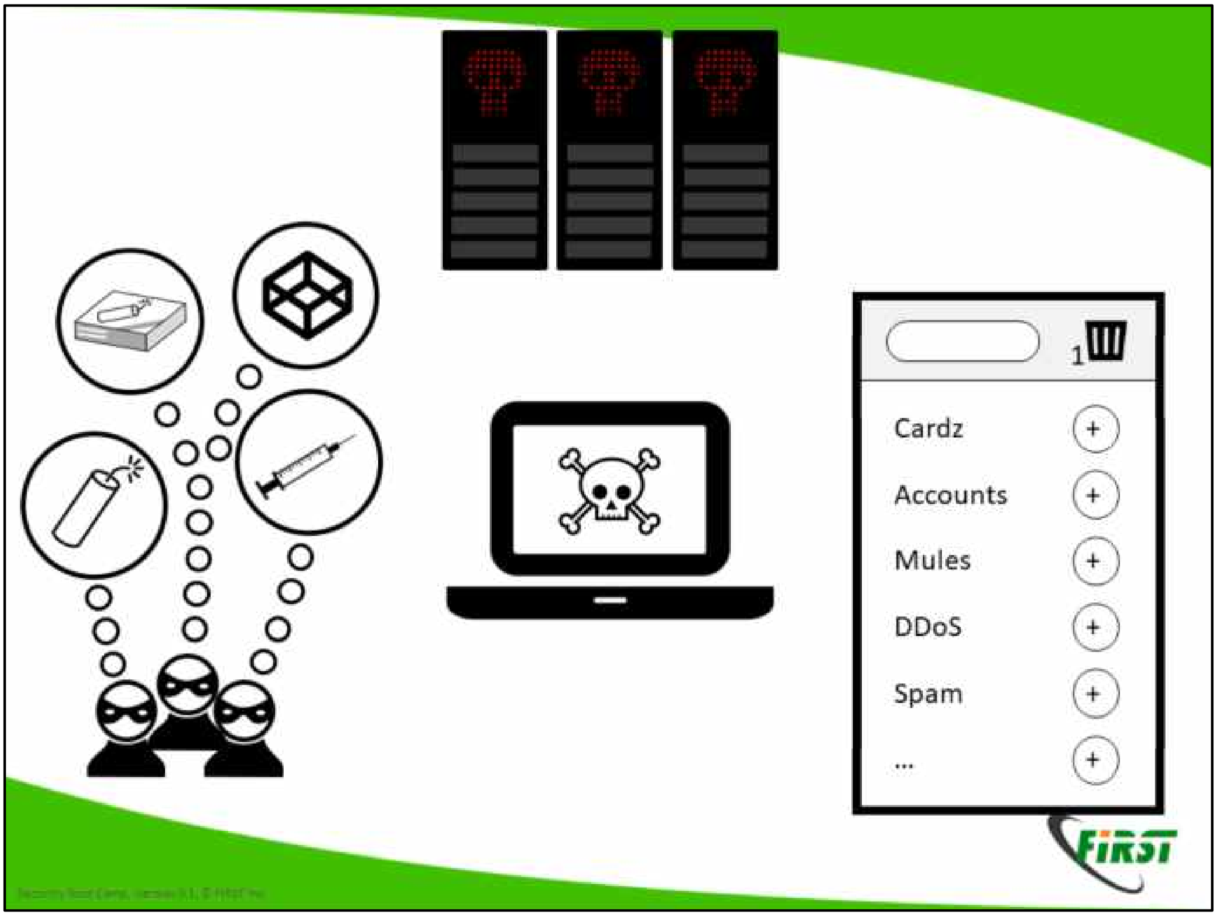
Please select a criteria below to perform a search on our huge database of Credit/Debit Cards and see the results at the end of this page.

Card Brand	● Visa ○ Master ○ Discover ○ Amex
Card Data Type	● Normal CC ○ Normal + SSN ○ Full CC
BIN - First 6 Digit	
Card Country	United States of America
	Search Reset Form

Search Results ...

Select	Card Number	Name	Address	SSN	Price	
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy
□	[illegible]	[illegible]	[illegible]		[illegible]	Check | Buy

Buy Selected Cards (Use it to Buy Multiple Products)



Now, if you buy these CCs you want to make them to money: Buy goods and sell them again. Don’t do this yourself, use a mule.

Gwapoo

DDoS as a Service for $5

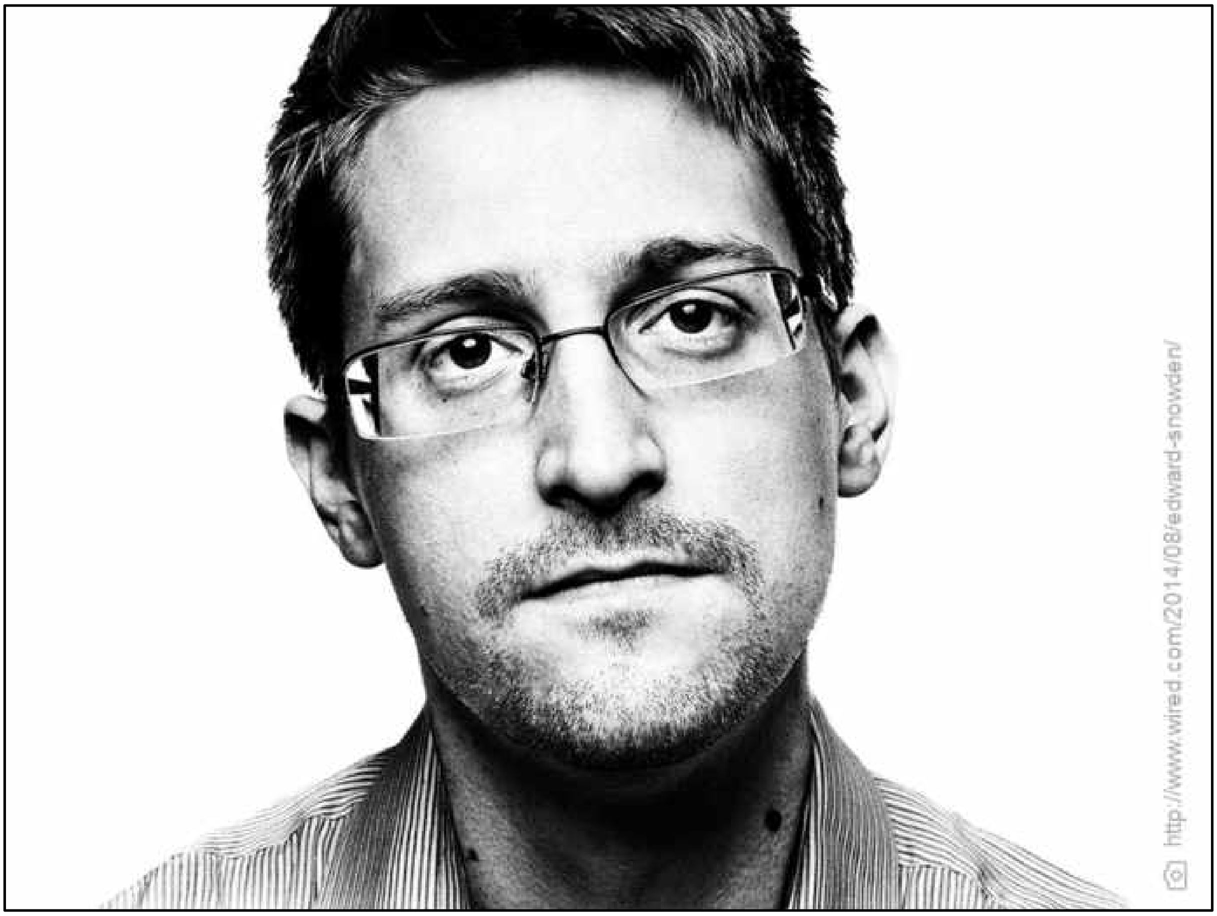
In NL students purchase this to avoid online exams (oder to your lap top -> WiFi congested, Exam off)

The internet underground is service oriented market economy!

Take home message

So these are criminals, but there is more.

ZeuS and SpyEye: Hamza Bendelladj, 100 Milion Betrug 2013, Happy hacker
GameOver ZeuS: Eugeniy Bogachev, Kopfgeld 3 Millionen, -> Dyer
Black Hole Exploit Kit, Paunch aka Dmitry E. Fedotov



http://www.wired.com/2014/08/edward-snowden/

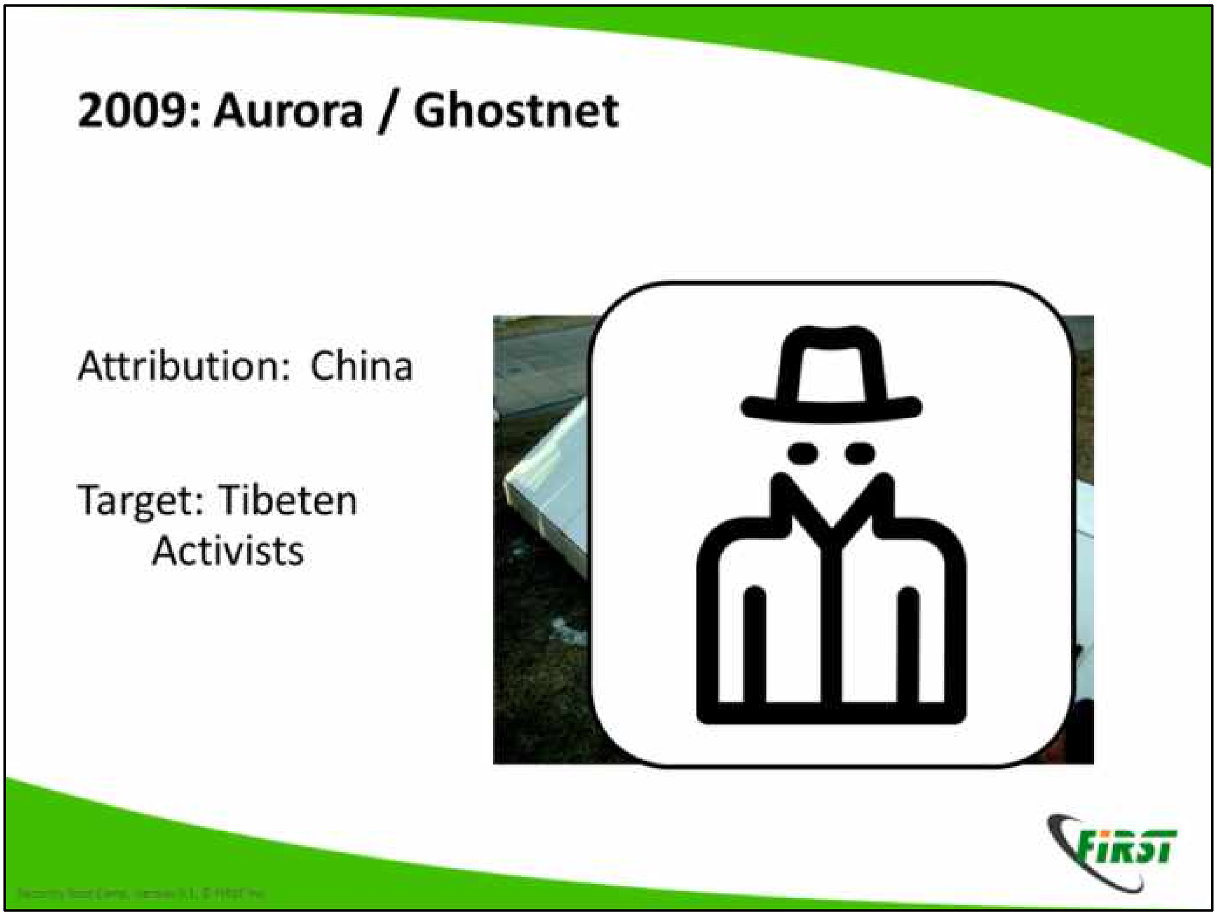
Since Snowde it shold be cleare to everybody that also governments have realized that the internet exists.

2003: Titan Rain

Attribution: China

Target: US / Defense Contractors

First known: Classic hacking: Titan rain, CN group steals software from US Army

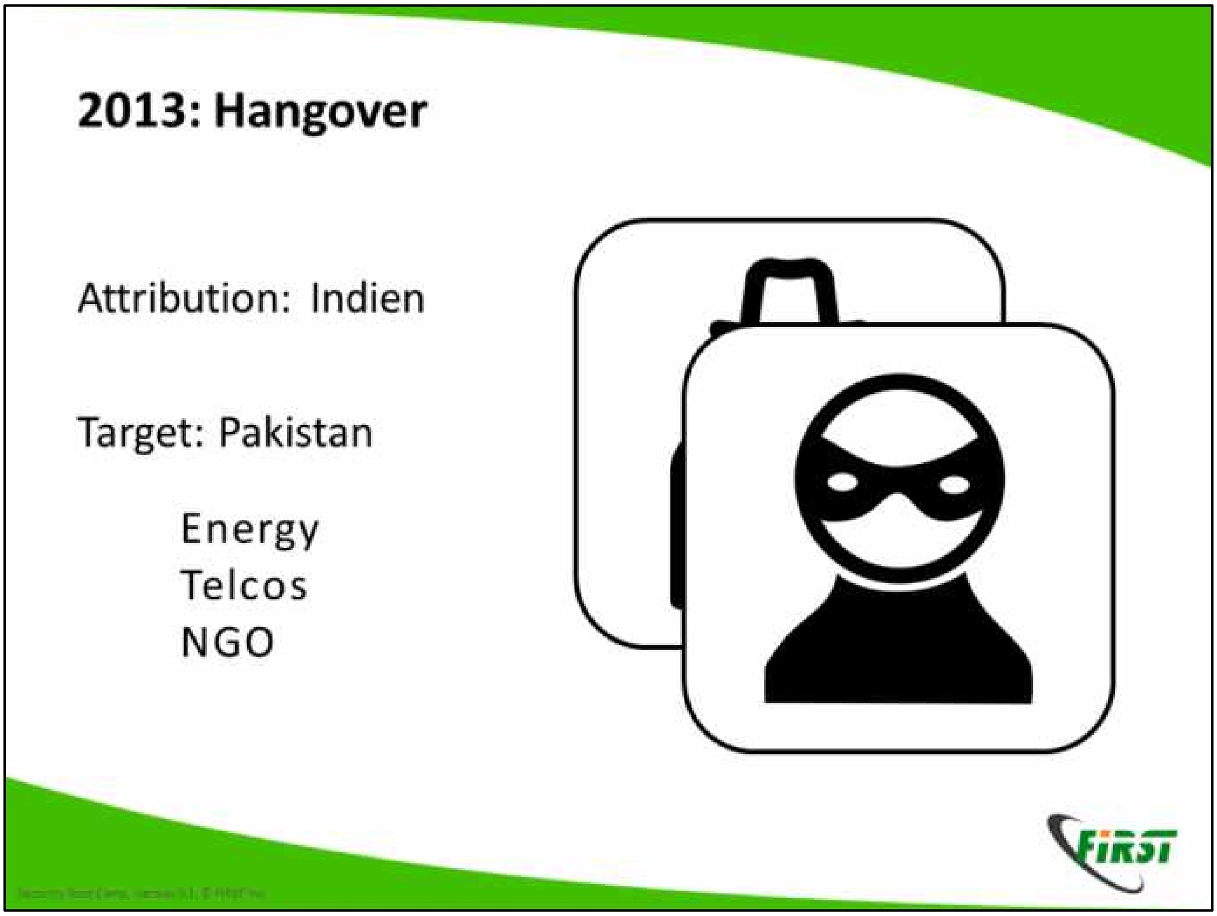


2009: Aurora / Ghostnet

Attribution: China

Target: Tibeten Activists

Aurora: Angriff auf Google mit dem Ziel e-Mail Konten von Dissidenten zu hacken
Ghostnet: Entdeckung bei den Leuten des Dalei Lamas aber nicht darauf beschränkt.



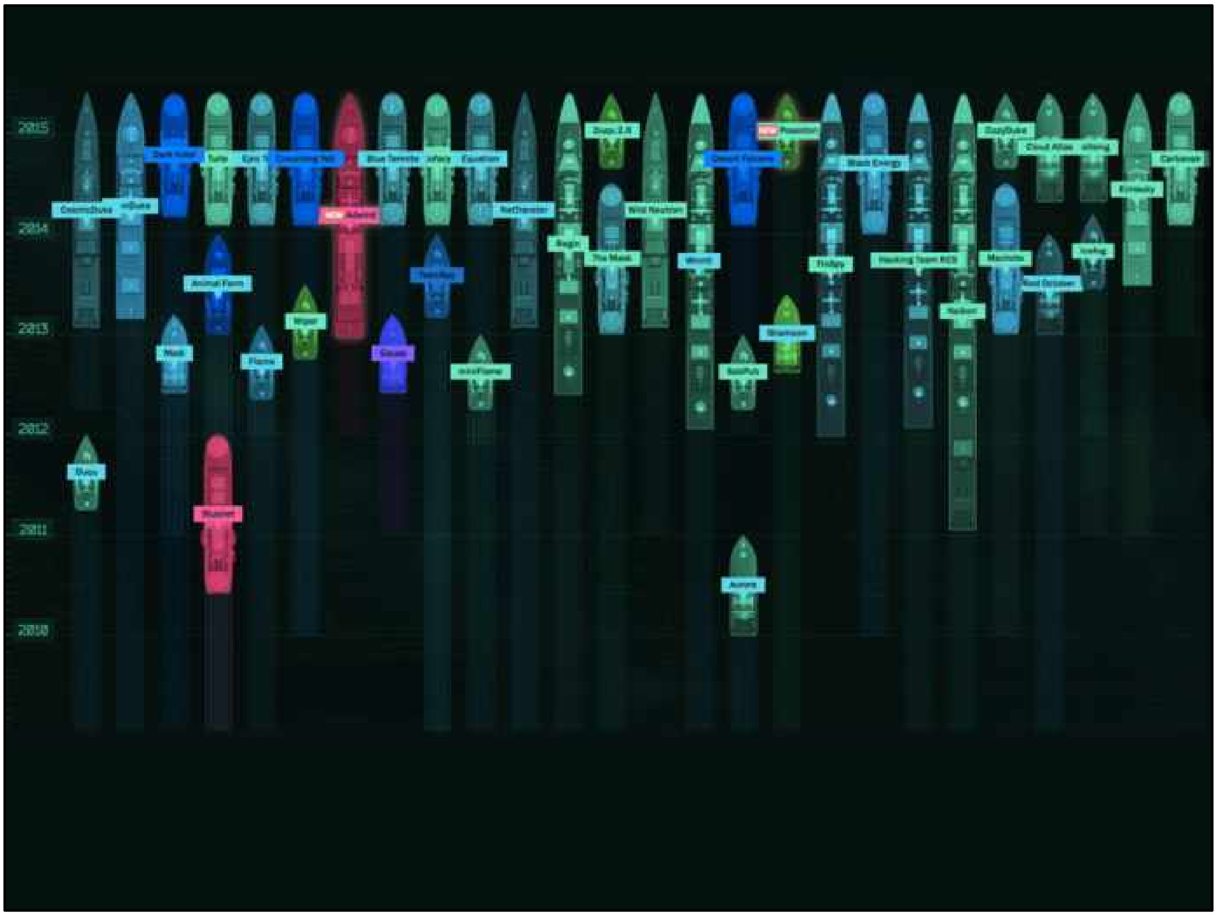
2013: Hangover

Attribution: Indien

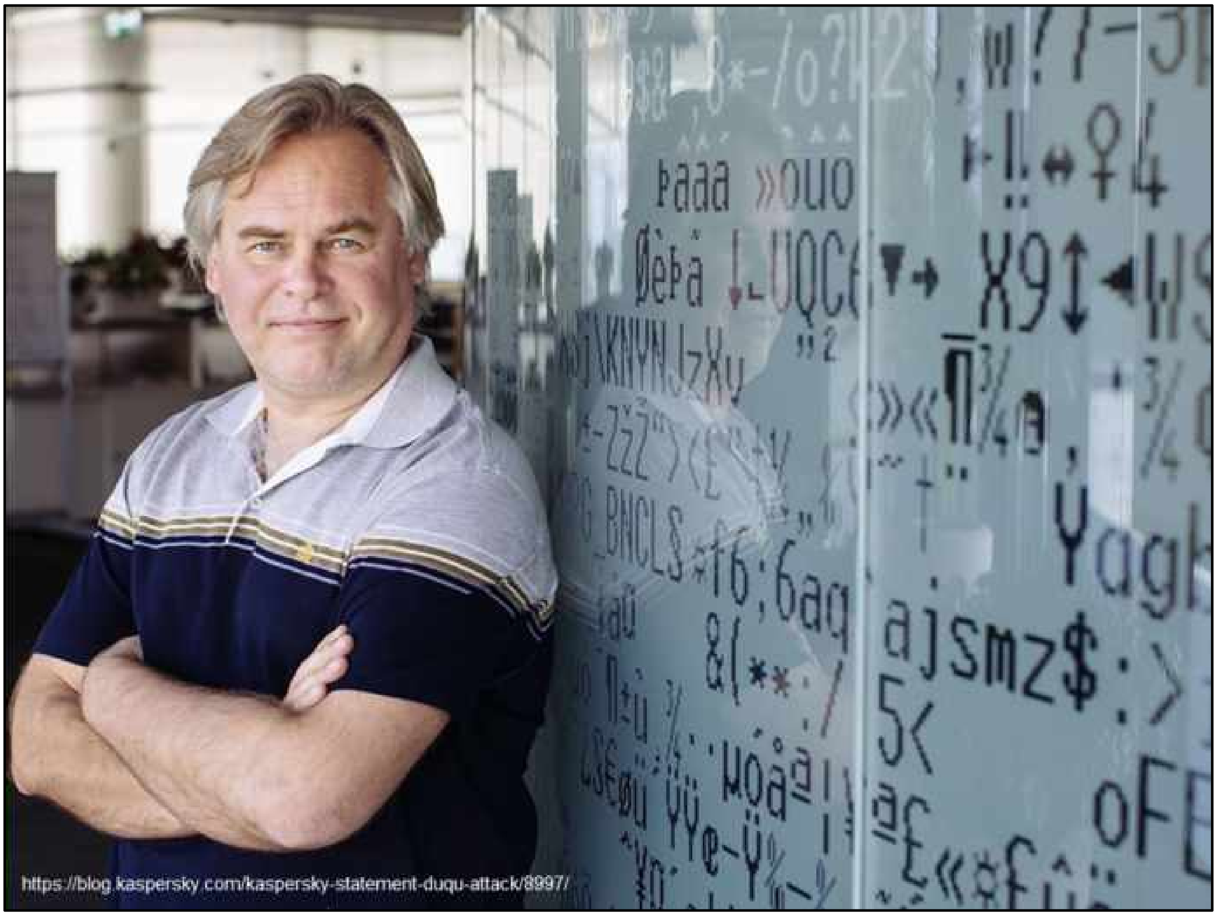
Target: Pakistan

- Energy
- Telcos
- NGO

Why NGOs? This can be sold to interested paries.

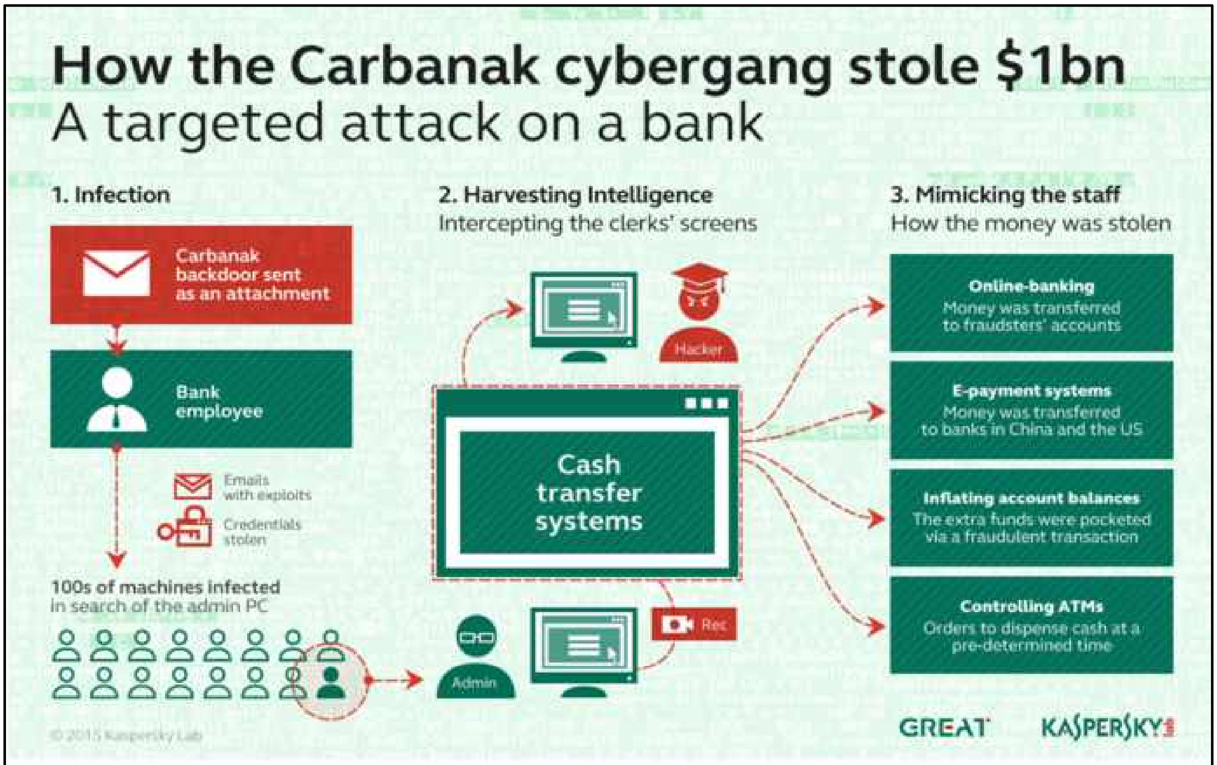


APTs werden normalerweise Staaten zugeschrieben



https://blog.kaspersky.com/kaspersky-statement-duqu-attack/8997/

But Kaspersky was affected, and admitted it (Hats of for that). -> Hacked for 6 month by Duqu 2, the same Malware used to spy on the US-Iran negotioations in Lausanne



How the Carbanak cybergang stole $1bn

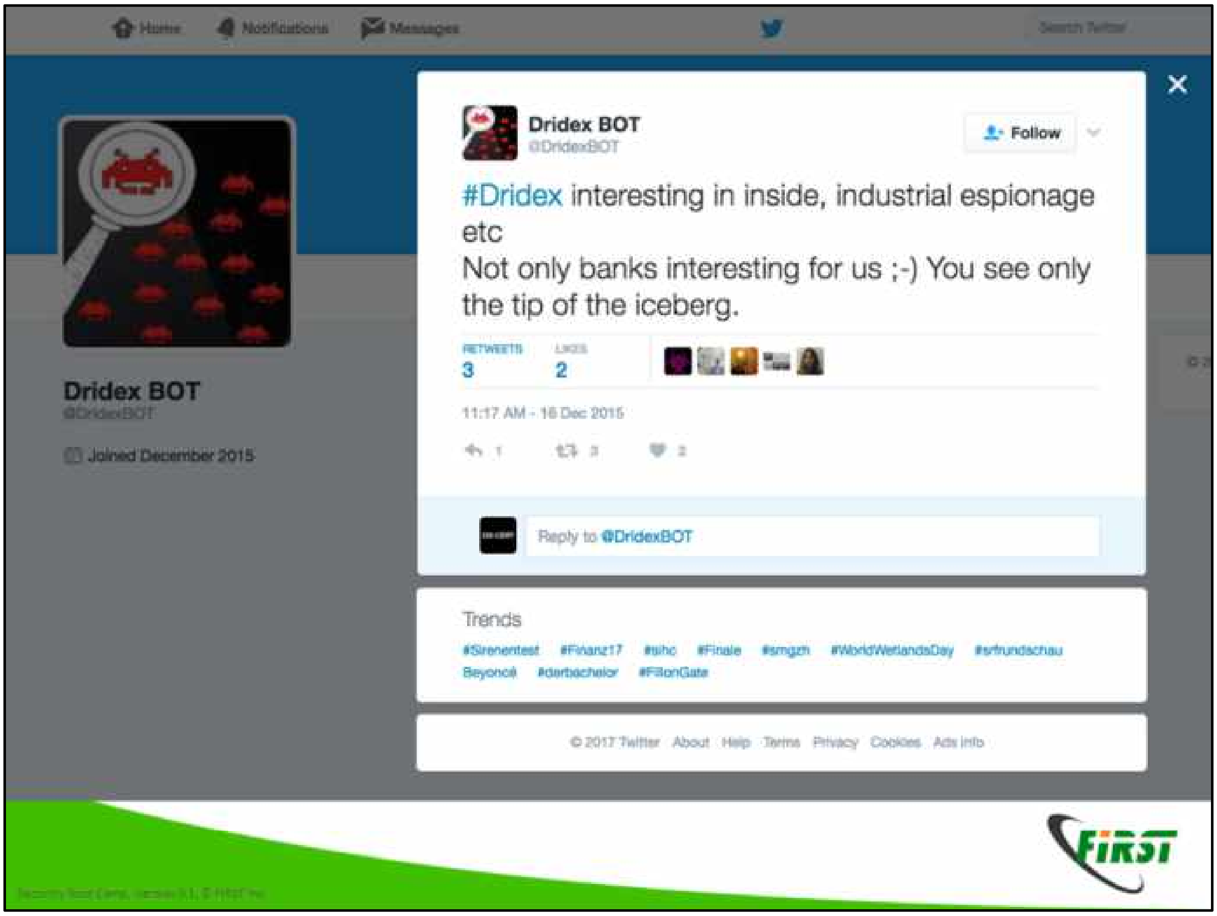
A targeted attack on a bank

1. Infection
Carbanak backdoor sent as an attachment
Bank employee
Emails with exploits
Credentials stolen
100s of machines infected
in search of the admin PC
2. Harvesting Intelligence
Intercepting the clerks' screens
Hacker
Cash transfer systems
Admin
Rec
3. Mimicking the staff
How the money was stolen
Online-banking
Money was transferred to fraudsters' accounts
E-payment systems
Money was transferred to banks in China and the US
Inflating account balances
The extra funds were pocketed via a fraudulent transaction
Controlling ATMs
Orders to dispense cash at a pre-determined time
GREAT
KASPERSKY

© 2015 Kaspersky Lab

APT normally attributed to Staats.
Wh has heard of Carbanack?
No one, keeps surprising me every time.

Attackes took 2 (!) years to infltrate Ukrainien and Russion banks. On day X they stole 1-2 billion (!) USD) by getting money out of ATMs, moving it around accounts, opening closing accounts.



Dridex BOT
@DridexBOT
Joined December 2015

Dridex BOT
@DridexBOT

#Dridex interesting in inside, industrial espionage etc
Not only banks interesting for us ;-) You see only the tip of the iceberg.

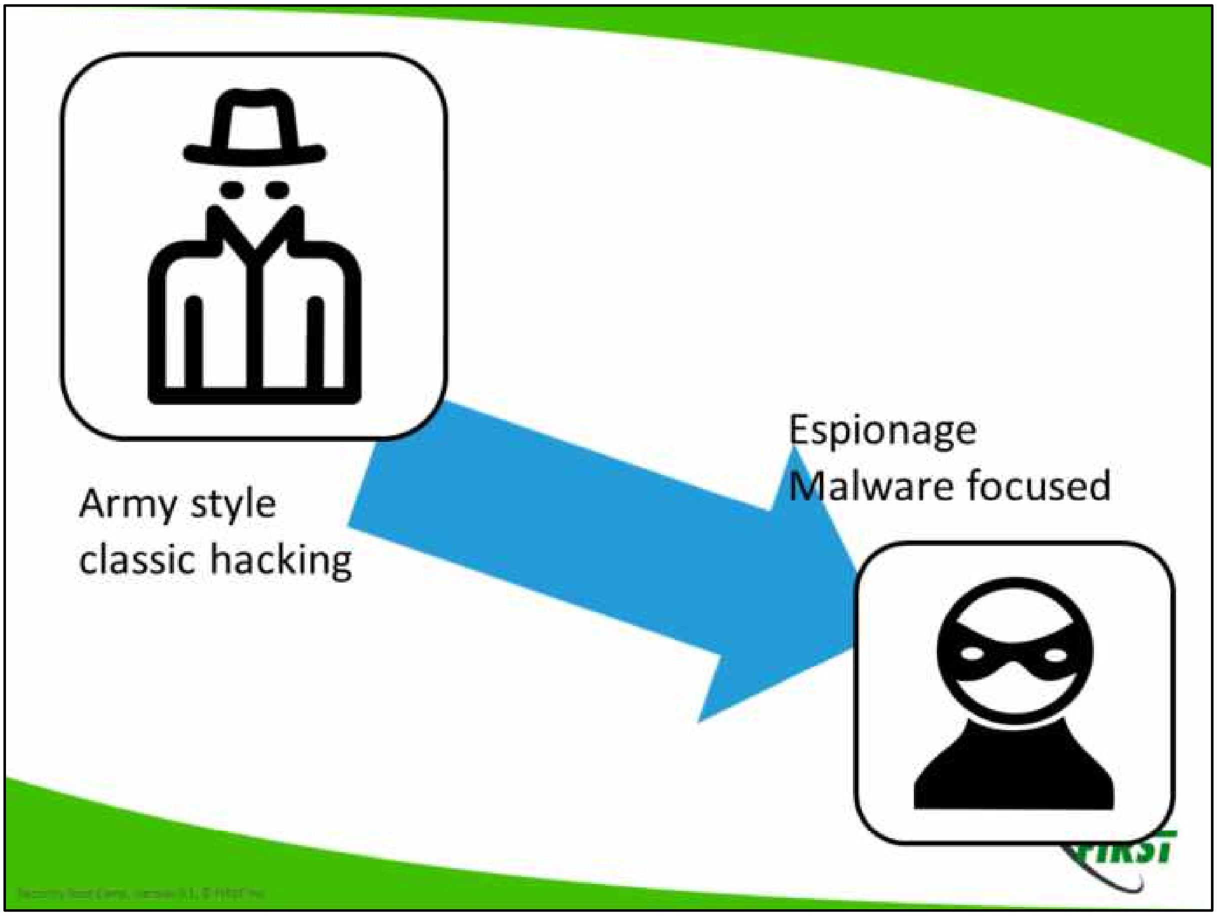
RETWEETS 3 LIKES 2

11:17 AM - 16 Dec 2015

Reply to @DridexBOT

#Sirenentest #Finanz17 #sihc #Finale #smgzh #WorldWetlandsDay #srfrundschau Beyoncé #derbachelor #FillonGate

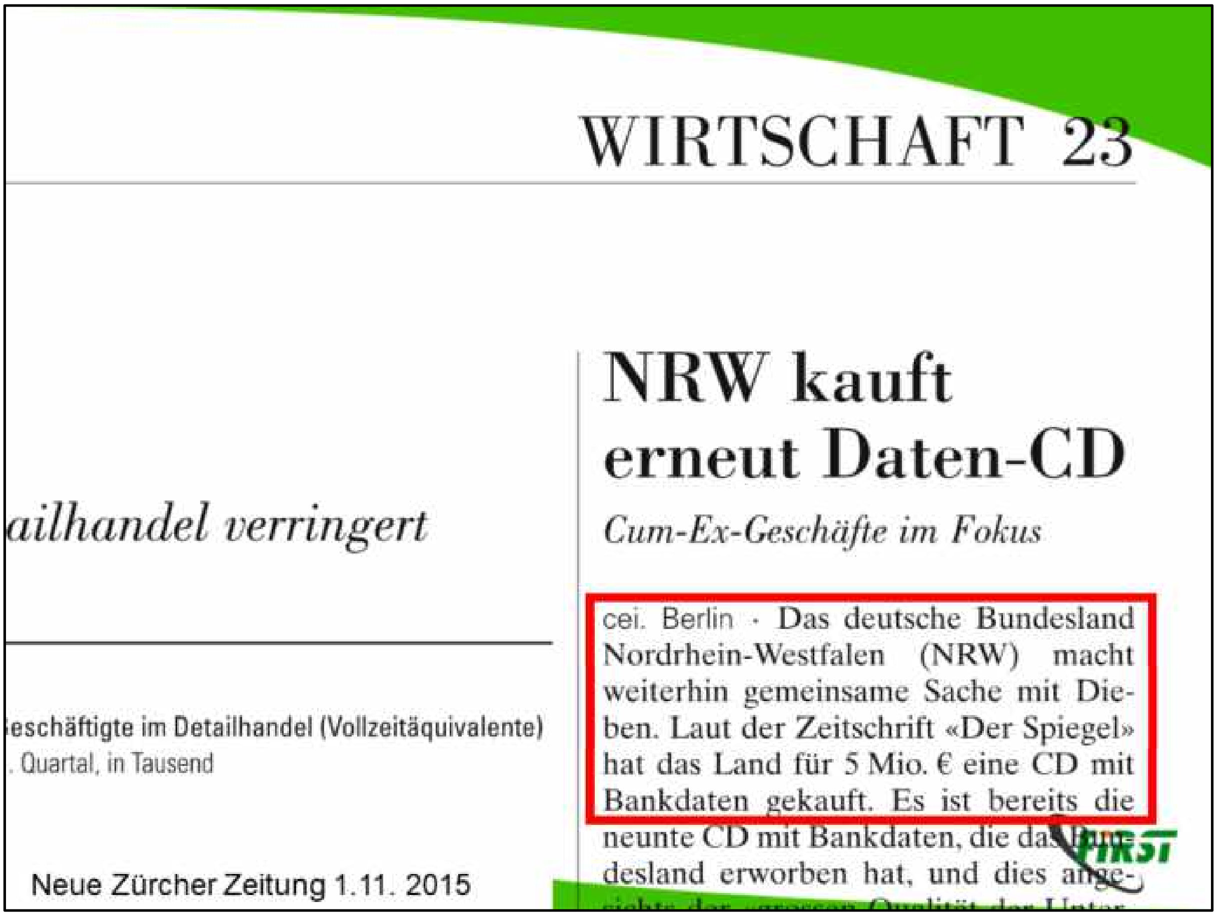
In late August 2015, a 30-year-old Moldovan individual by the name Andrey Ghinkul was arested in Cyprus, Spams dropped. But Tote leben länger … Dridex ist immer noch aktiv and tweeting.



Army style classic hacking

Espionage Malware focused

Trend „State sponsored / classical hacking -> Industrial espionage / Malware based) -> Professionalisation



WIRTSCHAFT 23

ailhandel verringert

eschäftigte im Detailhandel (Vollzeitäquivalente)
. Quartal, in Tausend

Neue Zürcher Zeitung 1.11. 2015

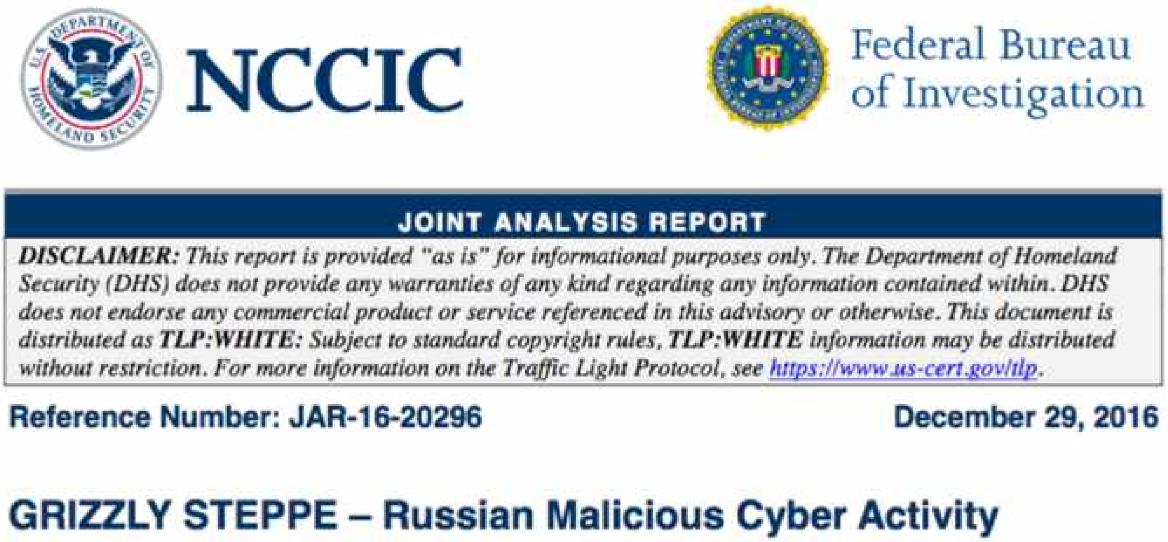
NRW kauft erneut Daten-CD

Cum-Ex-Geschäfte im Fokus

cei. Berlin · Das deutsche Bundesland Nordrhein-Westfalen (NRW) macht weiterhin gemeinsame Sache mit Dieben. Laut der Zeitschrift «Der Spiegel» hat das Land für 5 Mio. € eine CD mit Bankdaten gekauft. Es ist bereits die neunte CD mit Bankdaten, die das Bundesland erworben hat, und dies angesichts der grossen Qualität der Unter-

BTW: Staaten mischen hier mit. Not ok.

Grizzly Steppe



NCCIC

Federal Bureau of Investigation

JOINT ANALYSIS REPORT

DISCLAIMER: *This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as* ***TLP:WHITE:*** *Subject to standard copyright rules,* ***TLP:WHITE*** *information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.us-cert.gov/tlp.*

Reference Number: JAR-16-20296

December 29, 2016

GRIZZLY STEPPE – Russian Malicious Cyber Activity

And recently ….

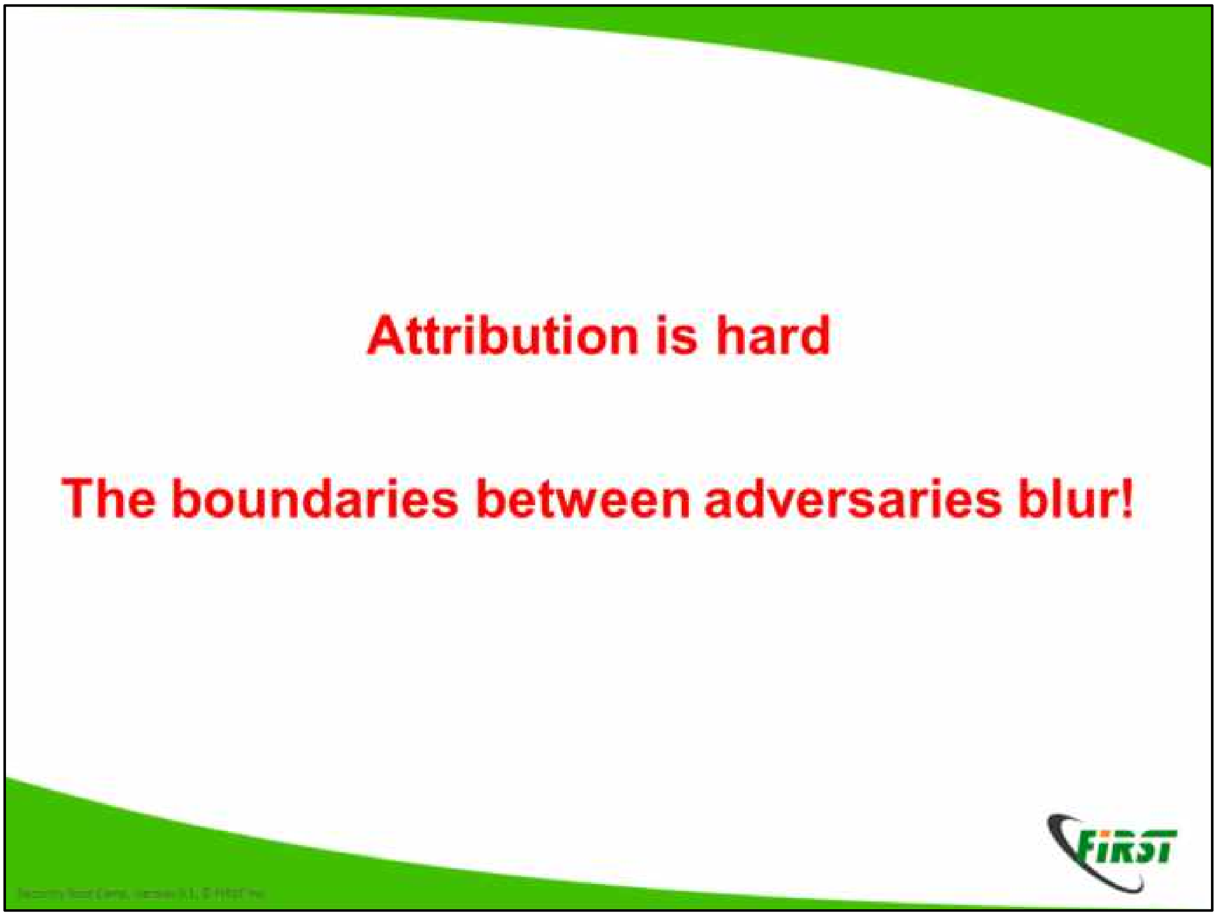
مجتمع فولاد نطنز
۱۵ کیلومتر
نطنز
۲۵ کیلومتر
Natanz Steel Group
15 km
Natanz
25 km

Crimea on 23. December 2015 Crimea: Russia shuts down Ukrainien powerplants.

TIONAL CYBERSECURITY CONGRESS
ОДНЫЙ КОНГРЕСС ПО КИБЕРБЕЗОПАСНОСТИ
CC4 http://www.en.kremlin.ru

Putin 1.6.2017, St Petersburg Economic Forum: Russia would never do something like this. But we cannot exclude that patriotic hackers would.

https://www.ft.com/content/f607ac6c-46e6-11e7-8519-9f94ee97d996



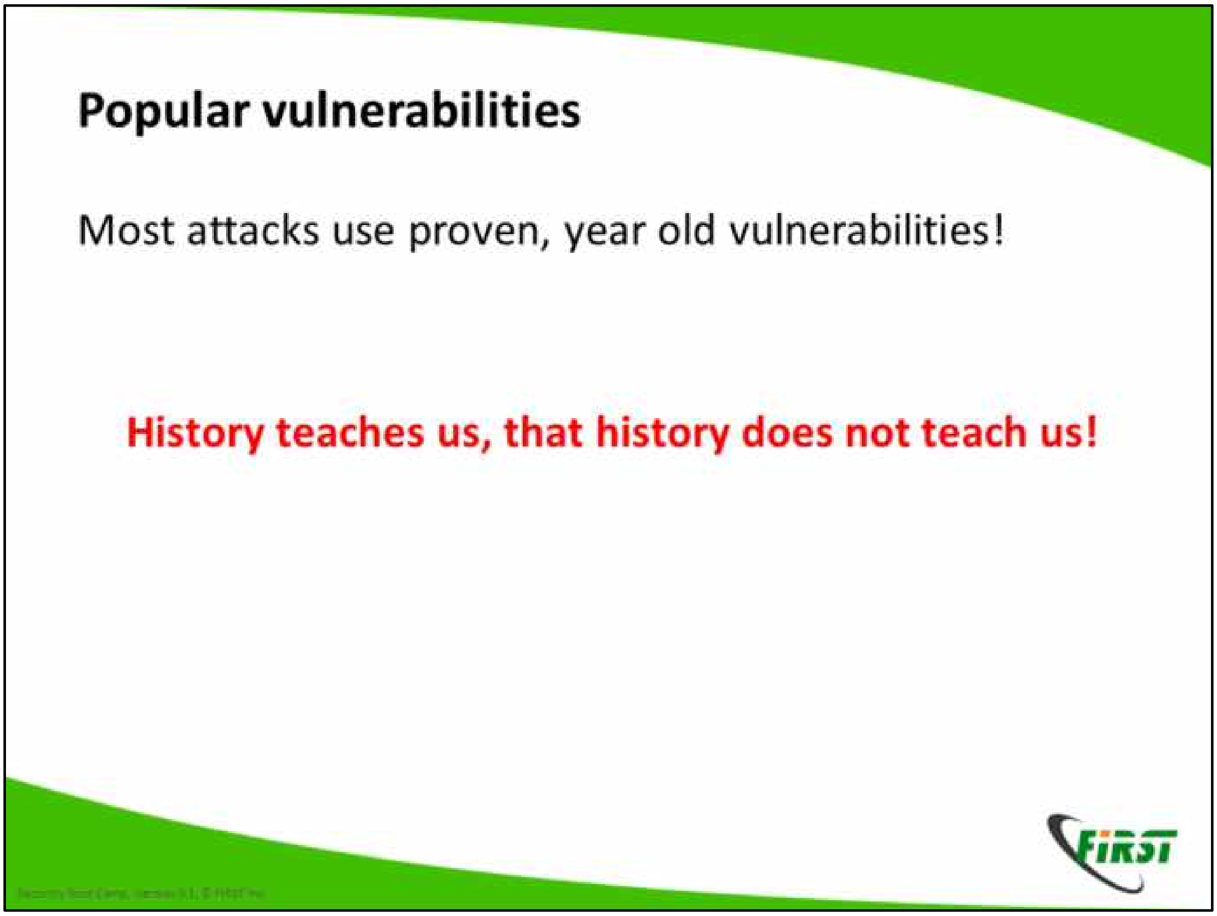
Attribution is hard

The boundaries between adversaries blur!

Tools and Methods

Image: CC0 https://www.publicdomainpictures.net/en/view-image.php?image=2680&picture=swiss-knife

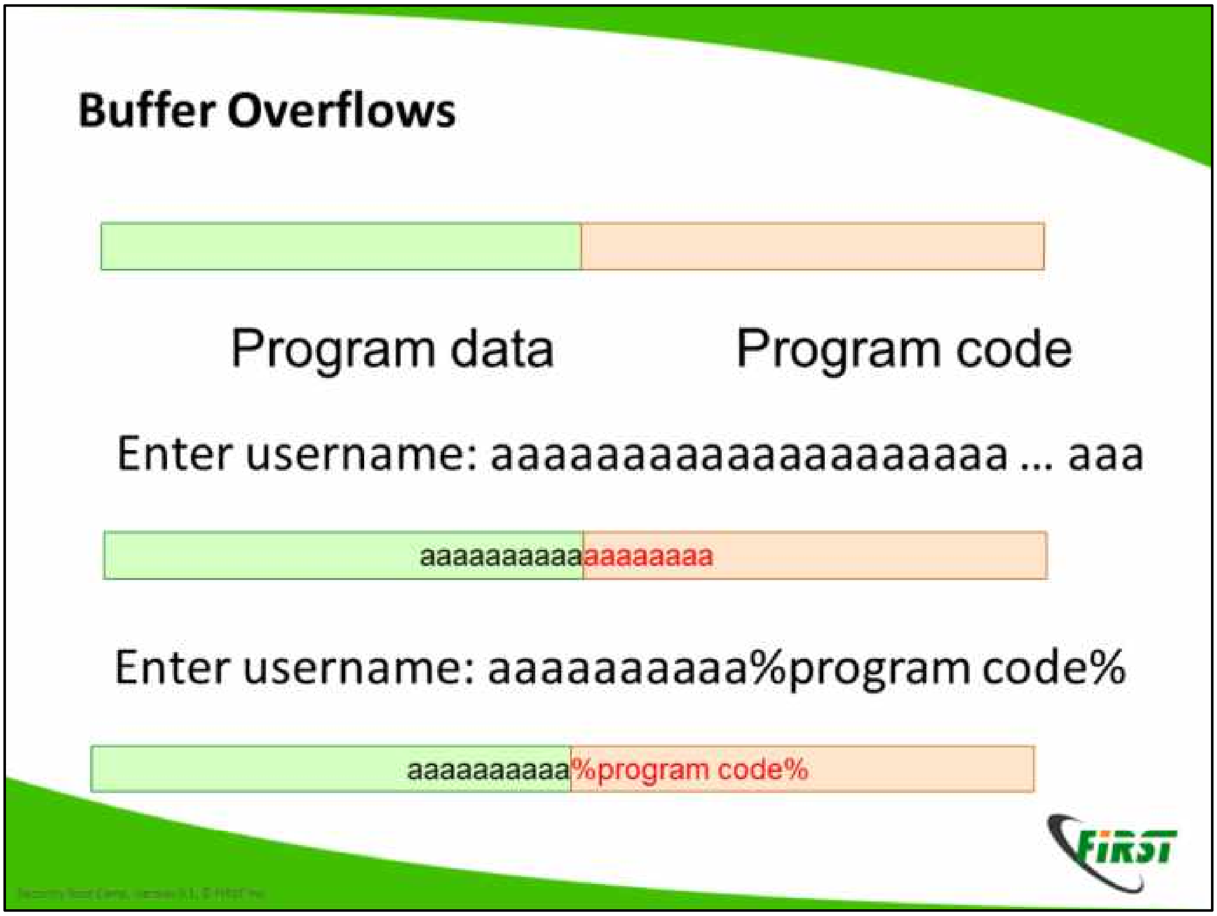
What are we talking about? This story begins, like so many in this game, with a hacked device. But what does it take to to hack this device? And why would you do this? Let’s explore these questions briefly!



Popular vulnerabilities

Most attacks use proven, year old vulnerabilities!

History teaches us, that history does not teach us!



Buffer Overflows

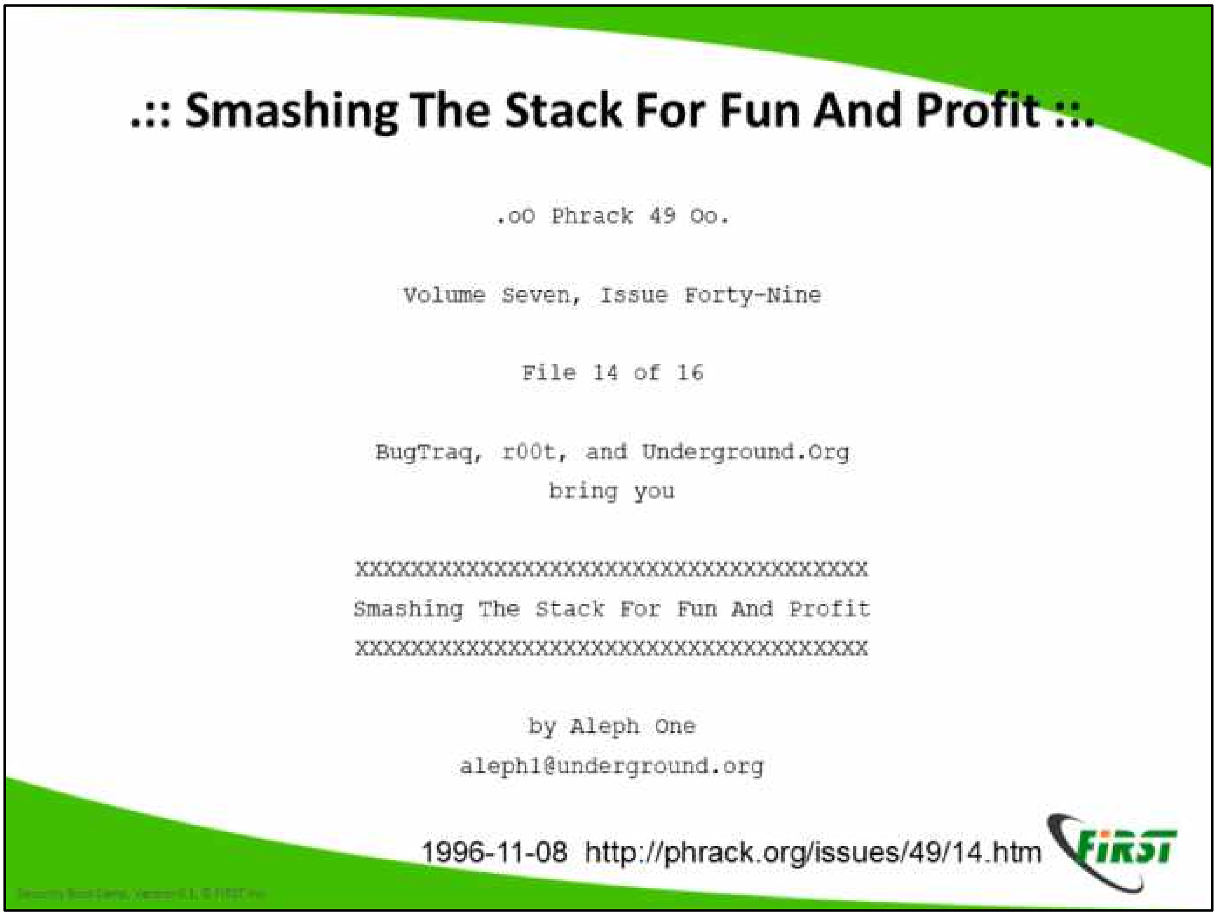
Program data   Program code

Enter username: aaaaaaaaaaaaaaaaaaaaa … aaa

aaaaaaaaaaaaaaaaaaa

Enter username: aaaaaaaaaa%program code%

aaaaaaaaaa%program code%

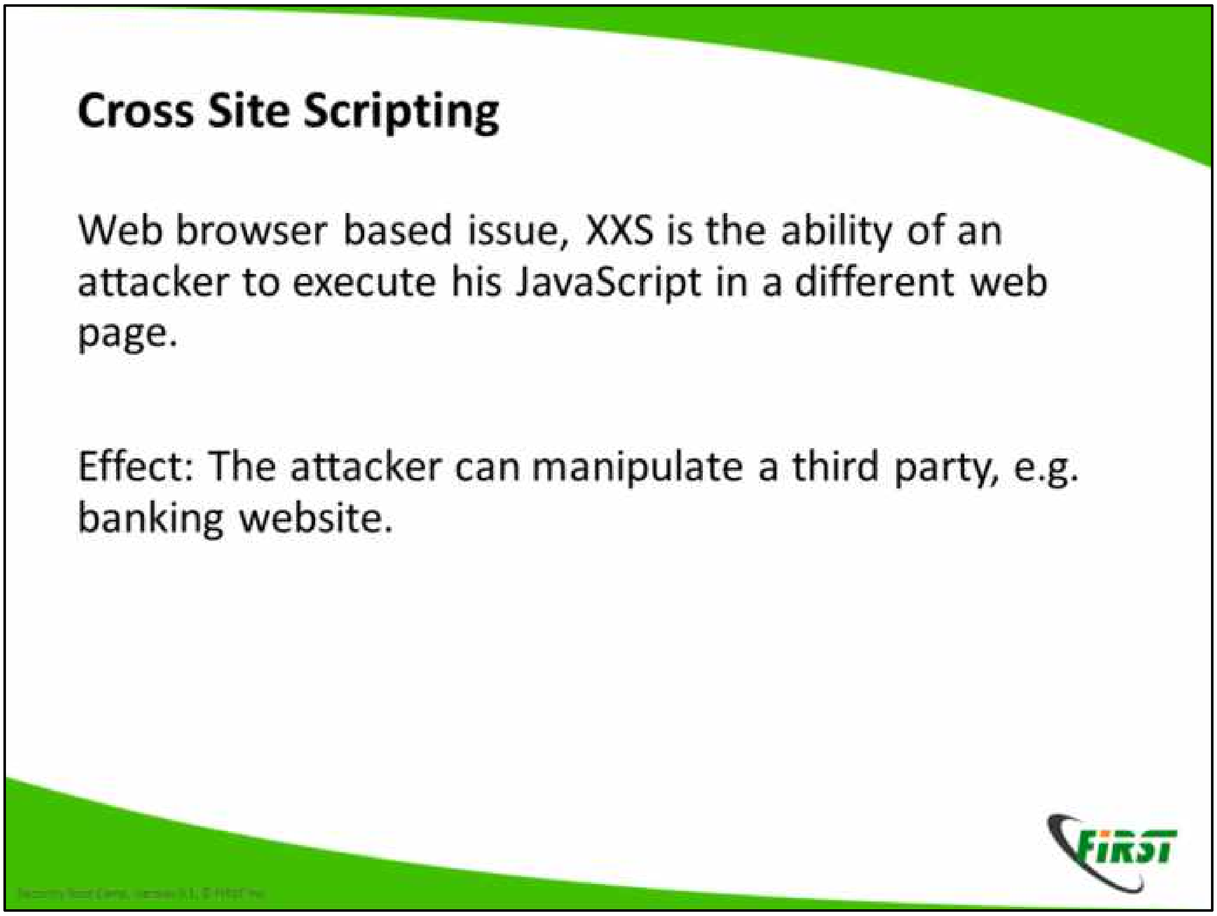


.:: Smashing The Stack For Fun And Profit ::.

```
                .oO Phrack 49 Oo.

          Volume Seven, Issue Forty-Nine

                   File 14 of 16

          BugTraq, r00t, and Underground.Org
                     bring you

        XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
        Smashing The Stack For Fun And Profit
        XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

                  by Aleph One
              aleph1@underground.org
```

1996-11-08 http://phrack.org/issues/49/14.htm

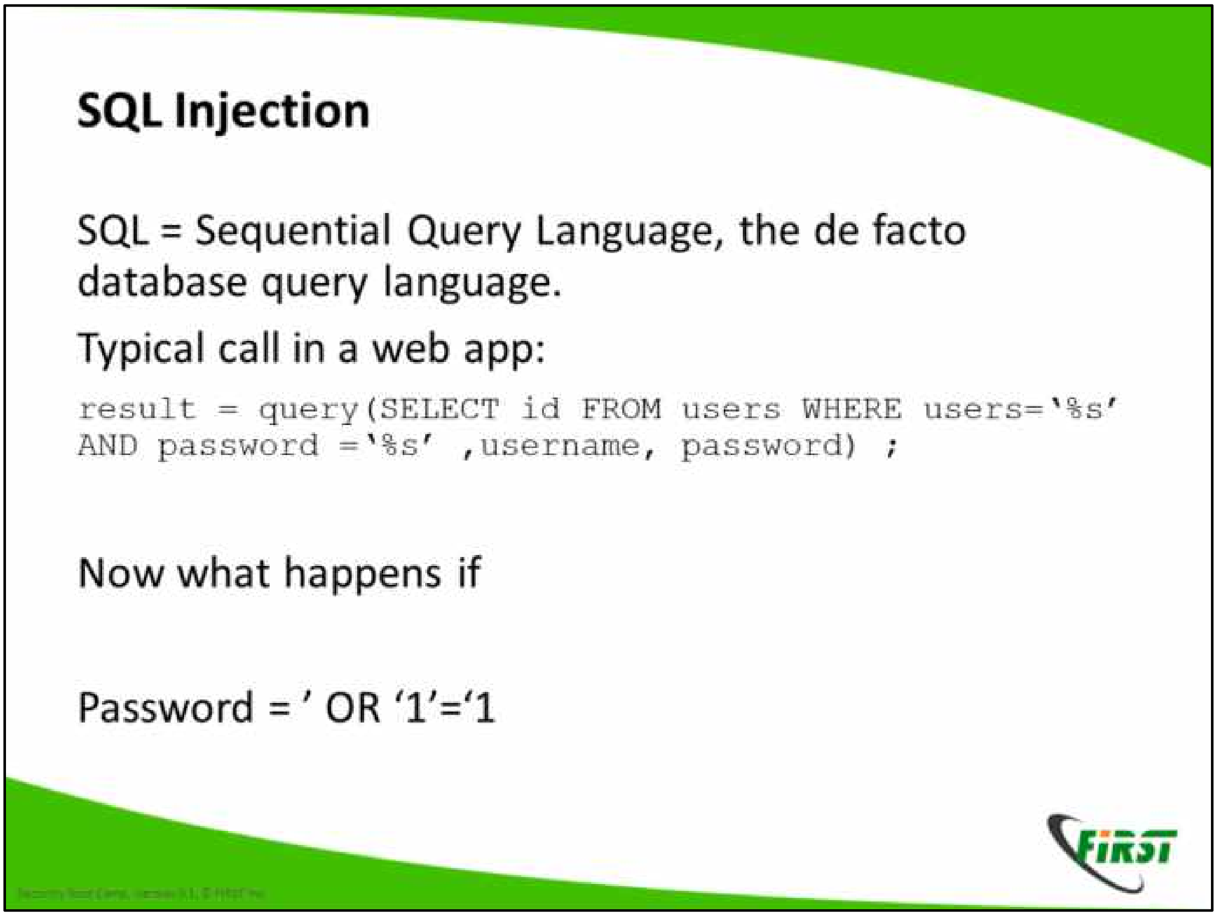
Elias Levy alias aleph1, founder and operate of the bugtraq mailinglist publishd in 1996 a step by step guide on buffer overflows.



Cross Site Scripting

Web browser based issue, XXS is the ability of an attacker to execute his JavaScript in a different web page.

Effect: The attacker can manipulate a third party, e.g. banking website.



SQL Injection

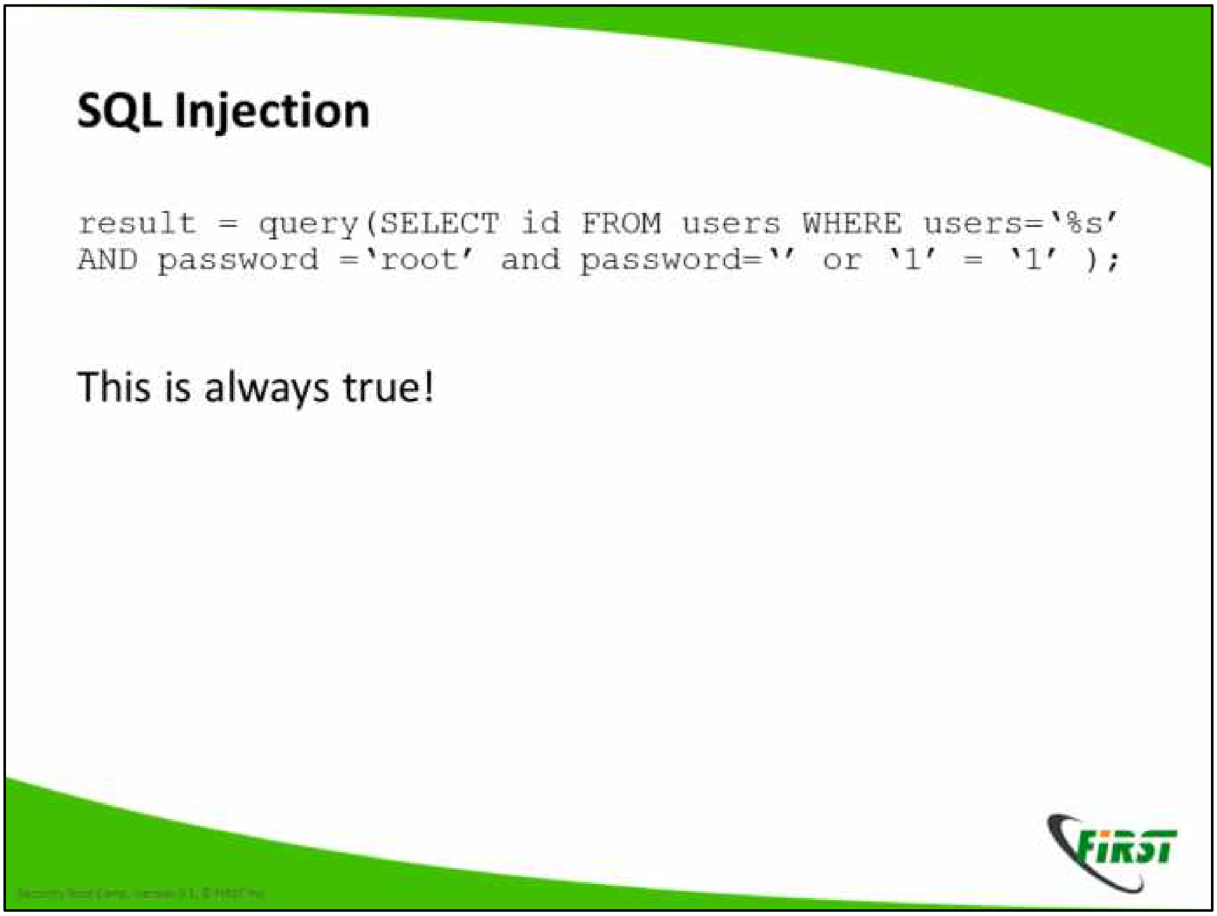
SQL = Sequential Query Language, the de facto database query language.

Typical call in a web app:

```
result = query(SELECT id FROM users WHERE users=‘%s’
AND password =‘%s’ ,username, password) ;
```

Now what happens if

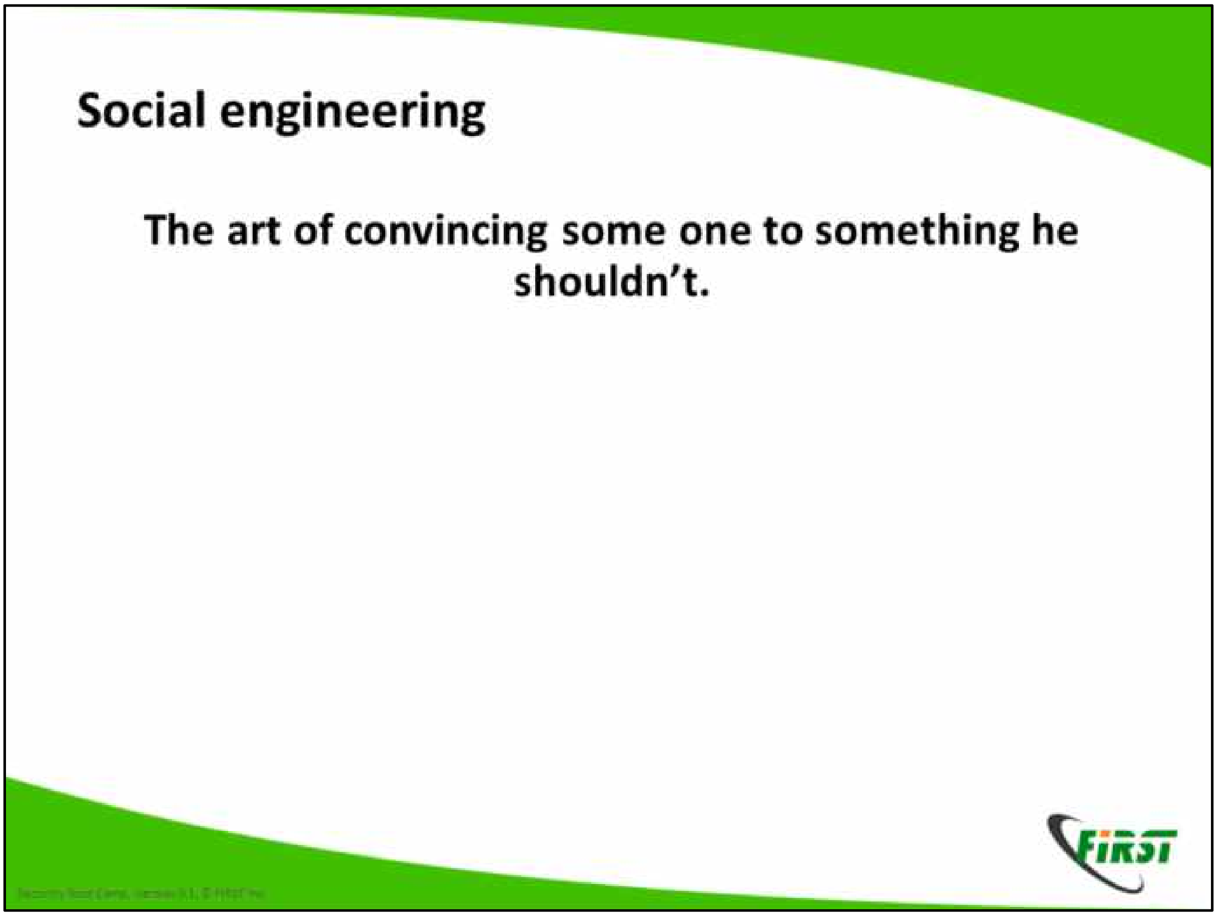
Password = ’ OR ‘1’=‘1



SQL Injection

```
result = query(SELECT id FROM users WHERE users=‘%s’
AND password =‘root’ and password=‘’ or ‘1’ = ‘1’ );
```

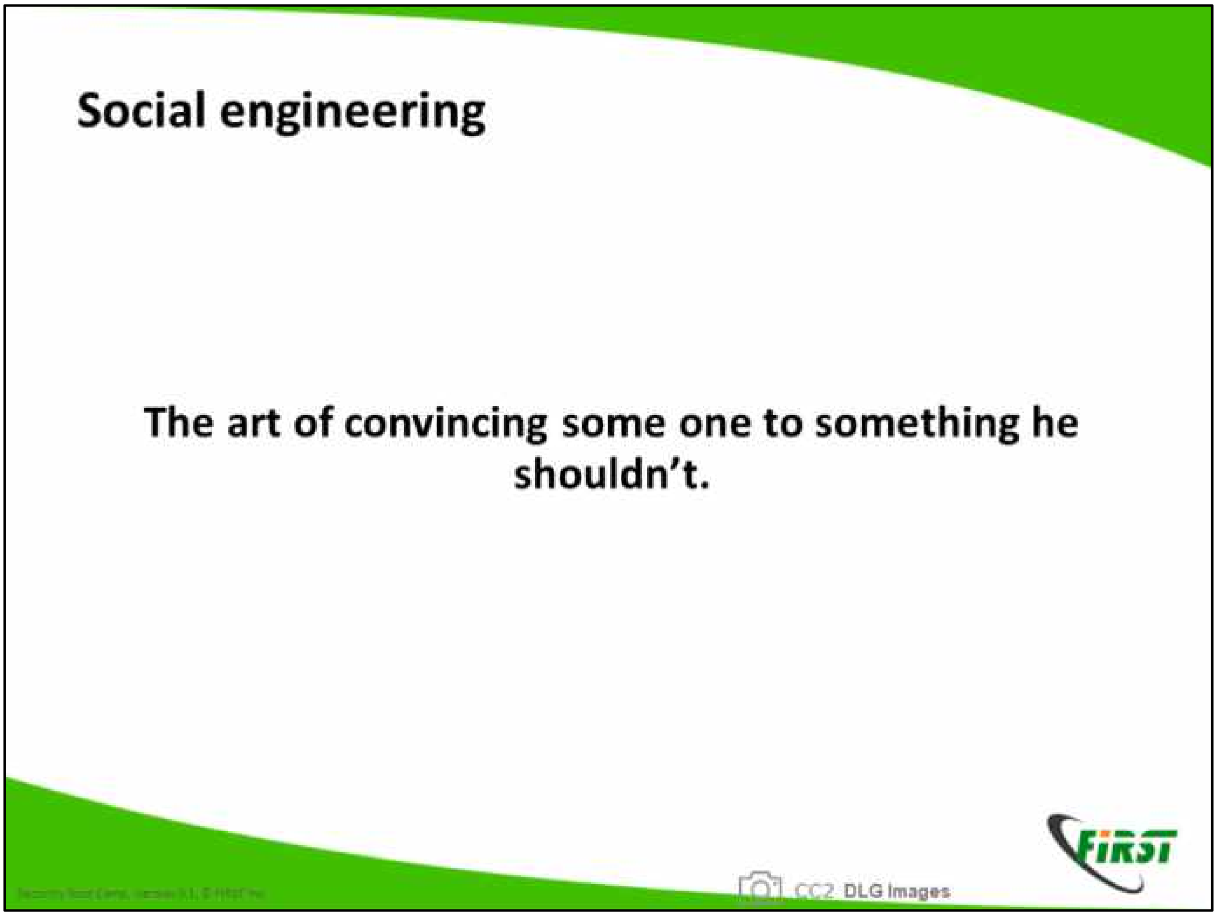
This is always true!



Social engineering

The art of convincing some one to something he shouldn't.

Hacking computers becomes inquiringly more difficult as operating systems become more and more secure. Hacking humans on the other hand is still the same.



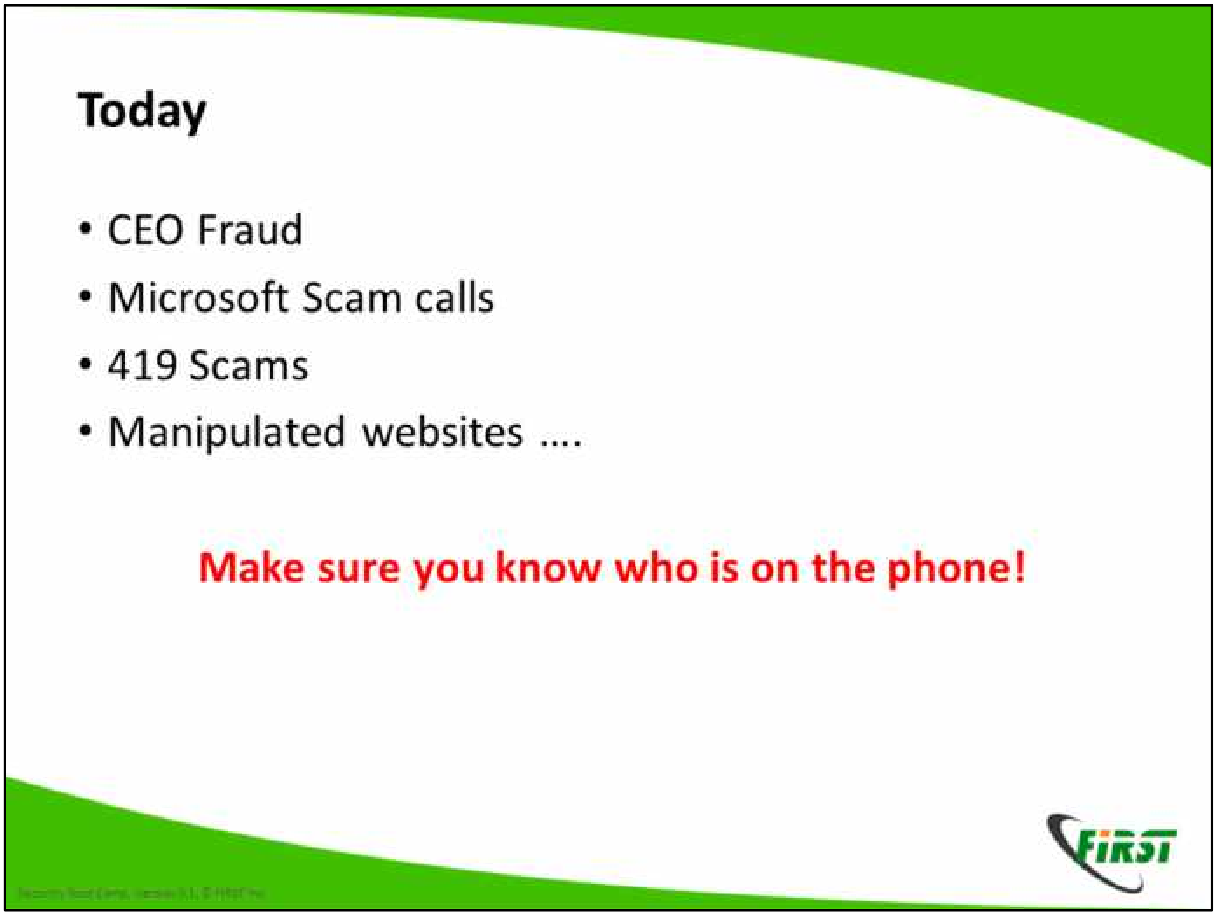
Social engineering

The art of convincing some one to something he shouldn’t.

CC2 DLG Images

Security Boot Camp, Version 3.1, © FIRST Inc

Hacking computers becomes inquiringly more difficult as operating systems become more and more secure. Hacking humans on the other hand is still the same. It’s been around since ever, (Joke alert: The snake taked Eve into eating the apple, creating the mess we have today).

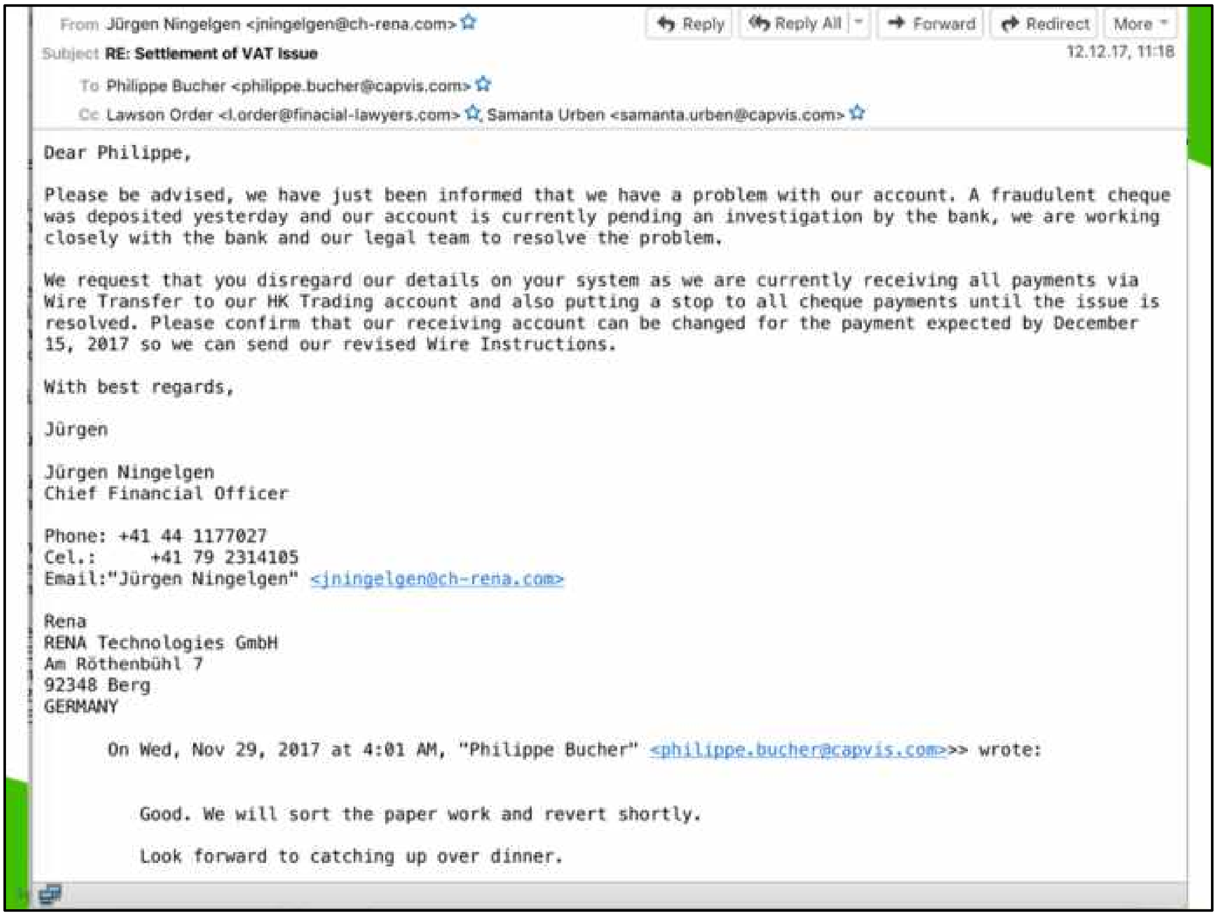


Today

- CEO Fraud
- Microsoft Scam calls
- 419 Scams
- Manipulated websites ….

Make sure you know who is on the phone!

https://web.archive.org/web/20110927122343/http://forum.419eater.com/forum/viewtopic.php?t=184886#1545310



From Jürgen Ningelgen <jningelgen@ch-rena.com>
Subject **RE: Settlement of VAT Issue**
12.12.17, 11:18
To Philippe Bucher <philippe.bucher@capvis.com>
Cc Lawson Order <l.order@finacial-lawyers.com>, Samanta Urben <samanta.urben@capvis.com>

Dear Philippe,

Please be advised, we have just been informed that we have a problem with our account. A fraudulent cheque was deposited yesterday and our account is currently pending an investigation by the bank, we are working closely with the bank and our legal team to resolve the problem.

We request that you disregard our details on your system as we are currently receiving all payments via Wire Transfer to our HK Trading account and also putting a stop to all cheque payments until the issue is resolved. Please confirm that our receiving account can be changed for the payment expected by December 15, 2017 so we can send our revised Wire Instructions.

With best regards,

Jürgen

Jürgen Ningelgen
Chief Financial Officer

Phone: +41 44 1177027
Cel.: +41 79 2314105
Email:"Jürgen Ningelgen" <jningelgen@ch-rena.com>

Rena
RENA Technologies GmbH
Am Röthenbühl 7
92348 Berg
GERMANY

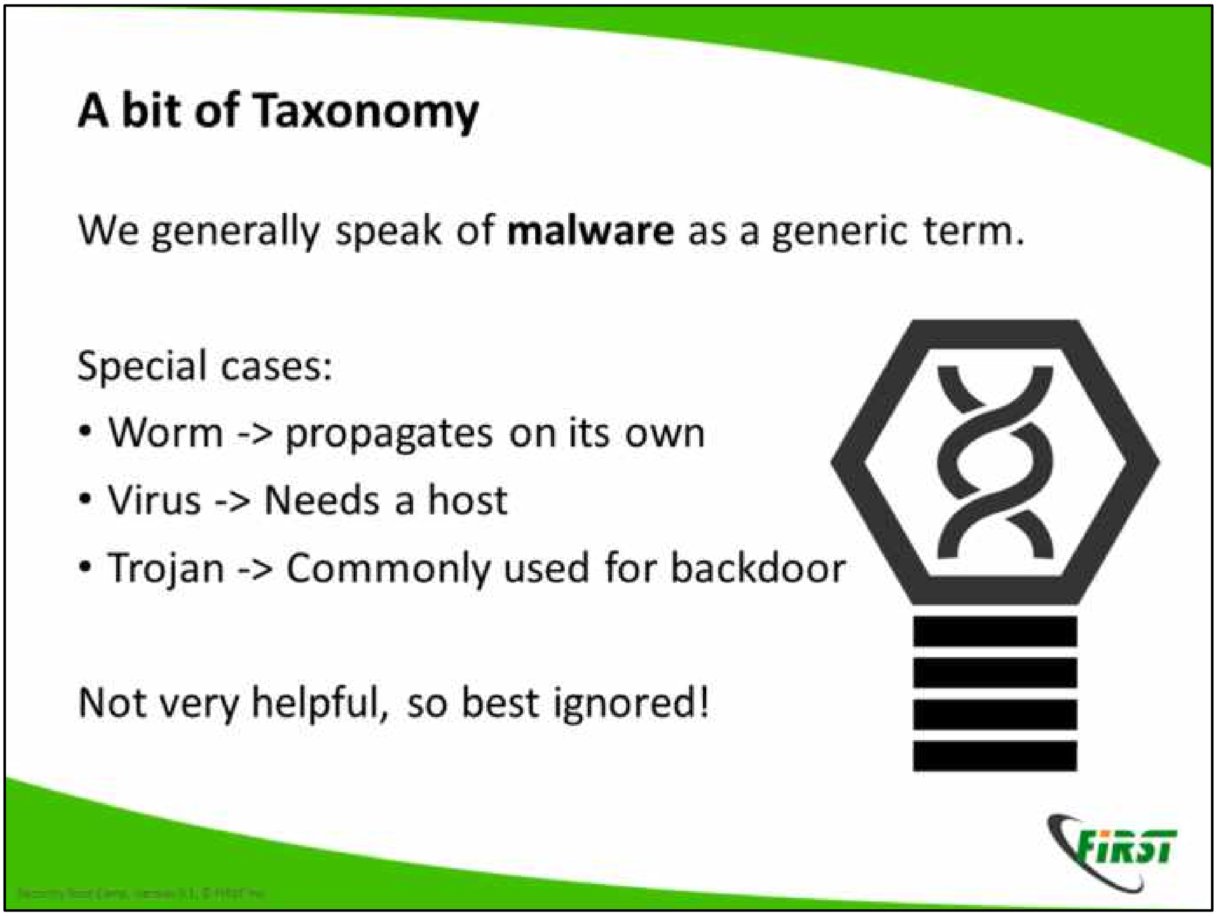
> On Wed, Nov 29, 2017 at 4:01 AM, "Philippe Bucher" <philippe.bucher@capvis.com>> wrote:
>
> Good. We will sort the paper work and revert shortly.
>
> Look forward to catching up over dinner.

Story:

- Long negotiations
- A lot of people in the e-mail thread
- After clousure of the deal: One more mail, from a slightly different domain rena.com -> ch-rena.com
- Please pay to another account.
- Bumm 1.2 millions USD gone.
- Above domain is from an example, nt the real one.

Malware distribution

Malware is distributed through about half half through e-mail or the web, the later is called drive by. Hang on, we’ll explain how this works.



A bit of Taxonomy

We generally speak of **malware** as a generic term.

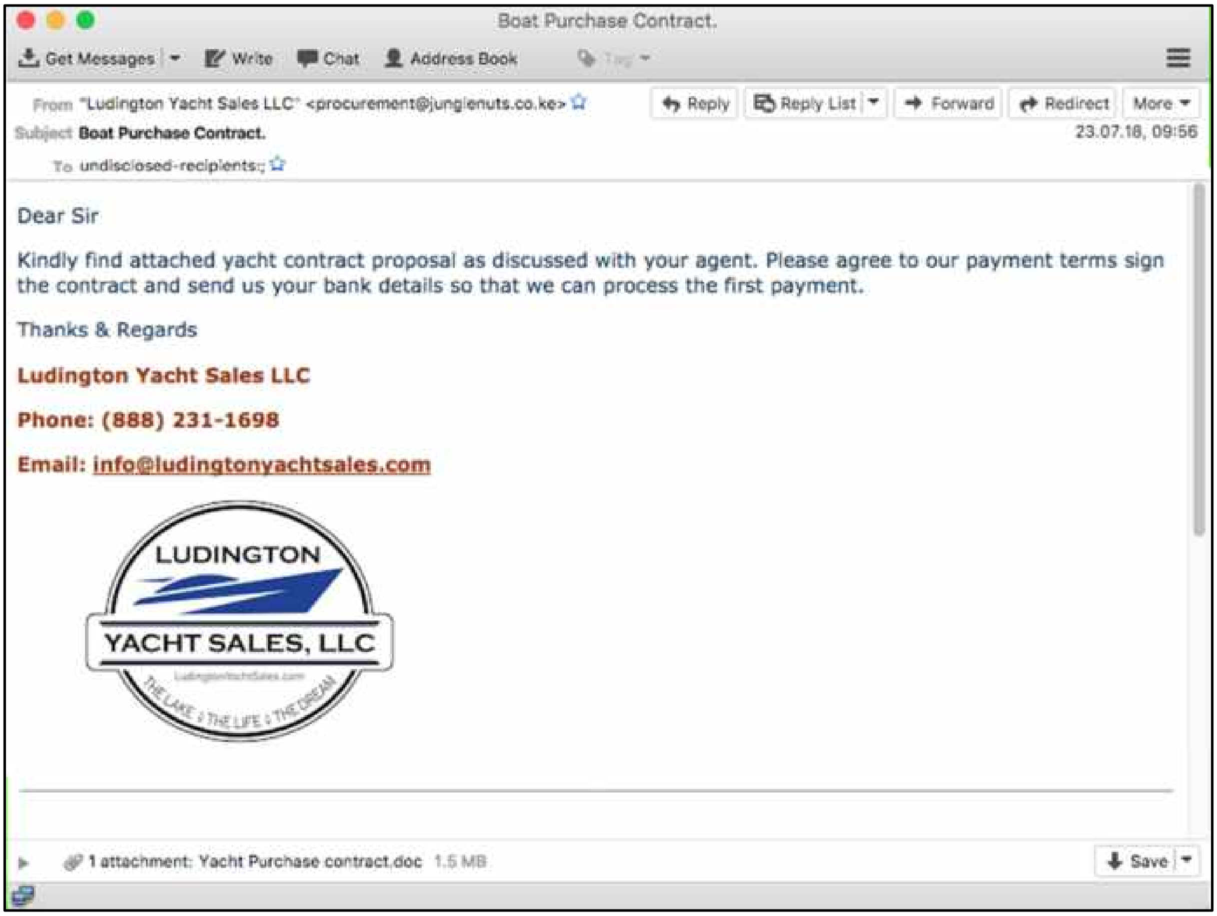
Special cases:

- Worm -> propagates on its own
- Virus -> Needs a host
- Trojan -> Commonly used for backdoor

Not very helpful, so best ignored!

Malware distribution

Malware is distributed through about half half through e-mail or the web, the later is called drive by. Hang on, we’ll explain how this works.



From "Ludington Yacht Sales LLC" <procurement@junglenuts.co.ke>
Subject Boat Purchase Contract.
To undisclosed-recipients:;
23.07.18, 09:56

Dear Sir

Kindly find attached yacht contract proposal as discussed with your agent. Please agree to our payment terms sign the contract and send us your bank details so that we can process the first payment.

Thanks & Regards

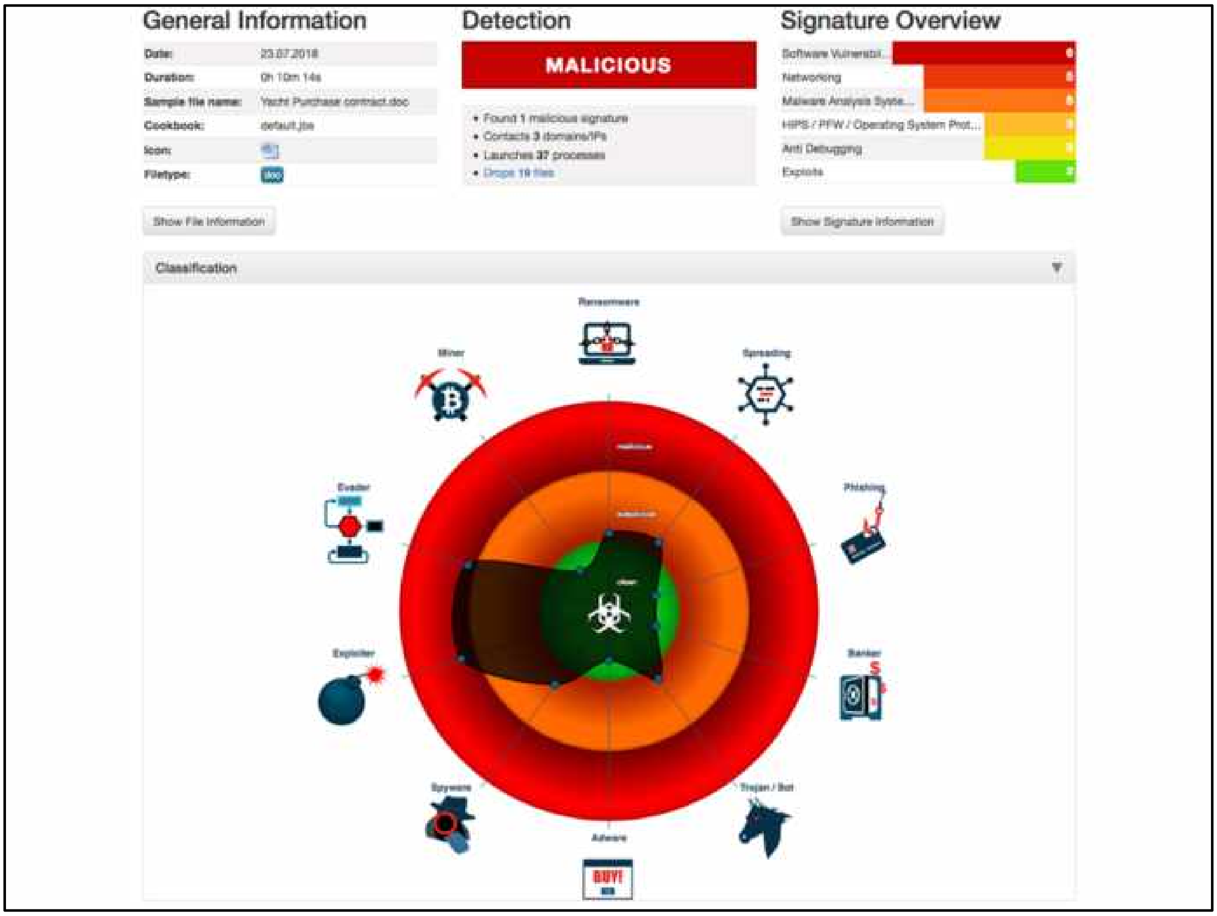
Ludington Yacht Sales LLC

Phone: (888) 231-1698

Email: info@ludingtonyachtsales.com

1 attachment: Yacht Purchase contract.doc 1.5 MB

Take this e-mail, there are a gazillion examples. It contains a word file.
So who thinks open a word file, or a PDF is an issue?



General Information

Date:	23.07.2018
Duration:	0h 10m 14s
Sample file name:	Yacht Purchase contract.doc
Cookbook:	default.jbs
Icon:	
Filetype:	doc

Detection

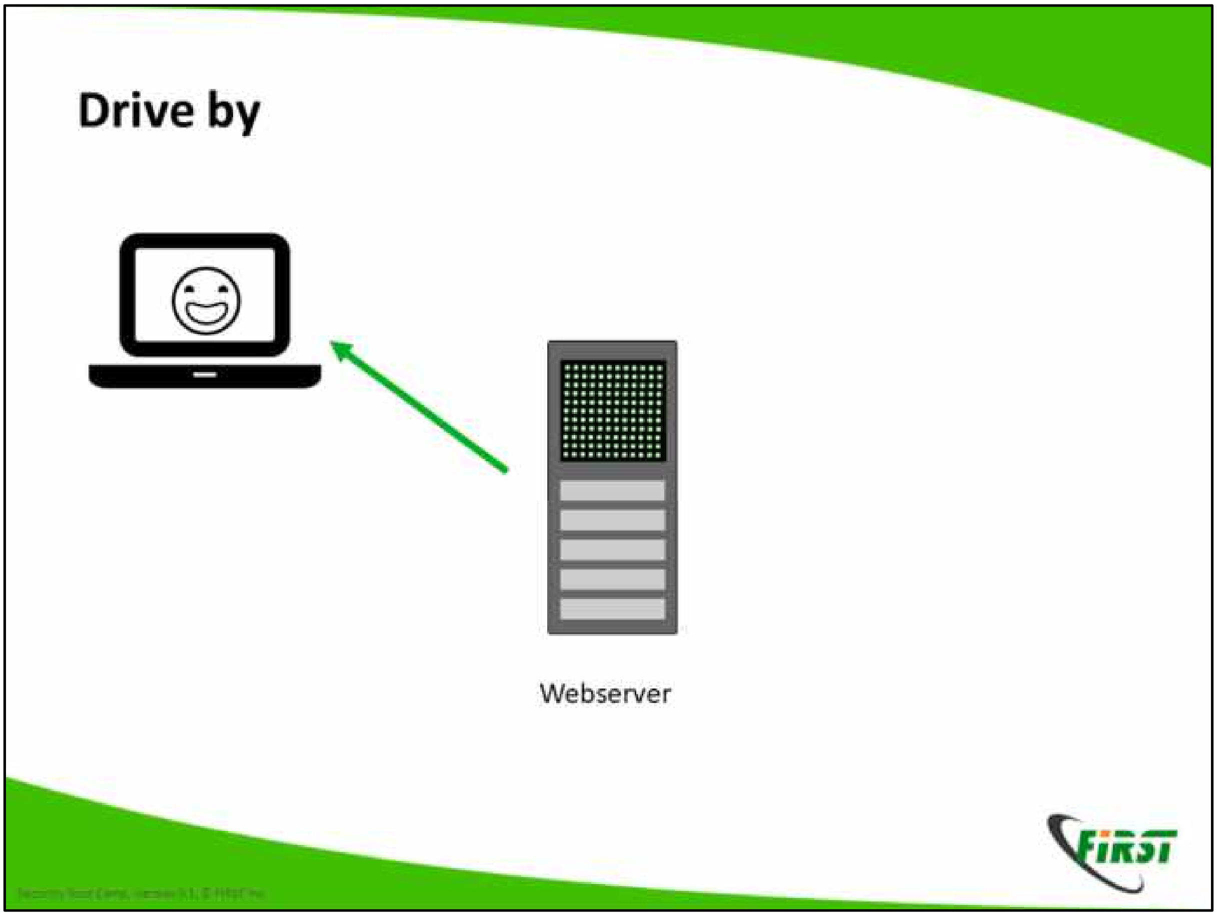
MALICIOUS

- Found 1 malicious signature
- Contacts 3 domains/IPs
- Launches 37 processes
- Drops 19 files

Signature Overview

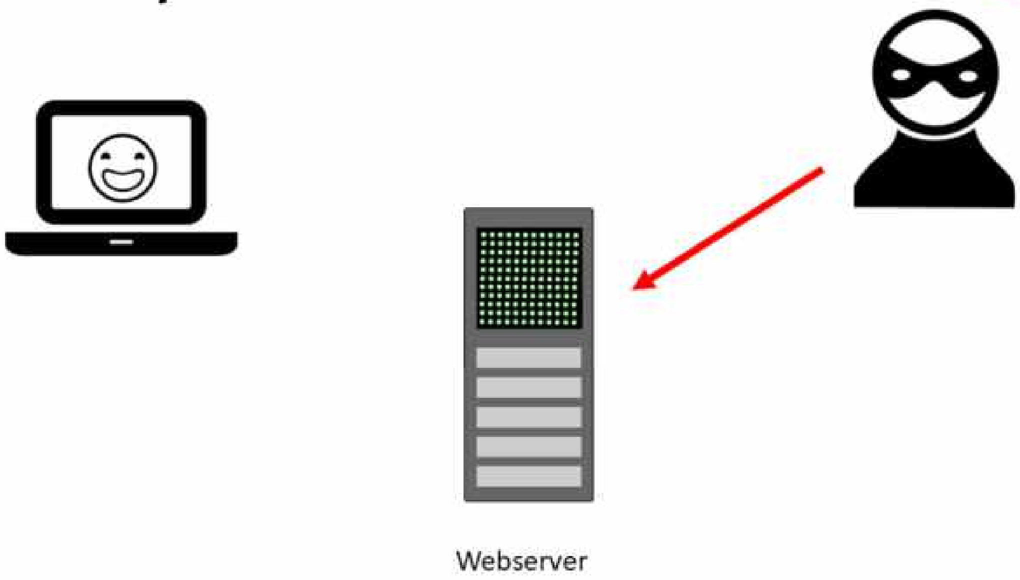
- Software Vulnerabil...
- Networking
- Malware Analysis Syste...
- HIPS / PFW / Operating System Prot...
- Anti Debugging
- Exploits

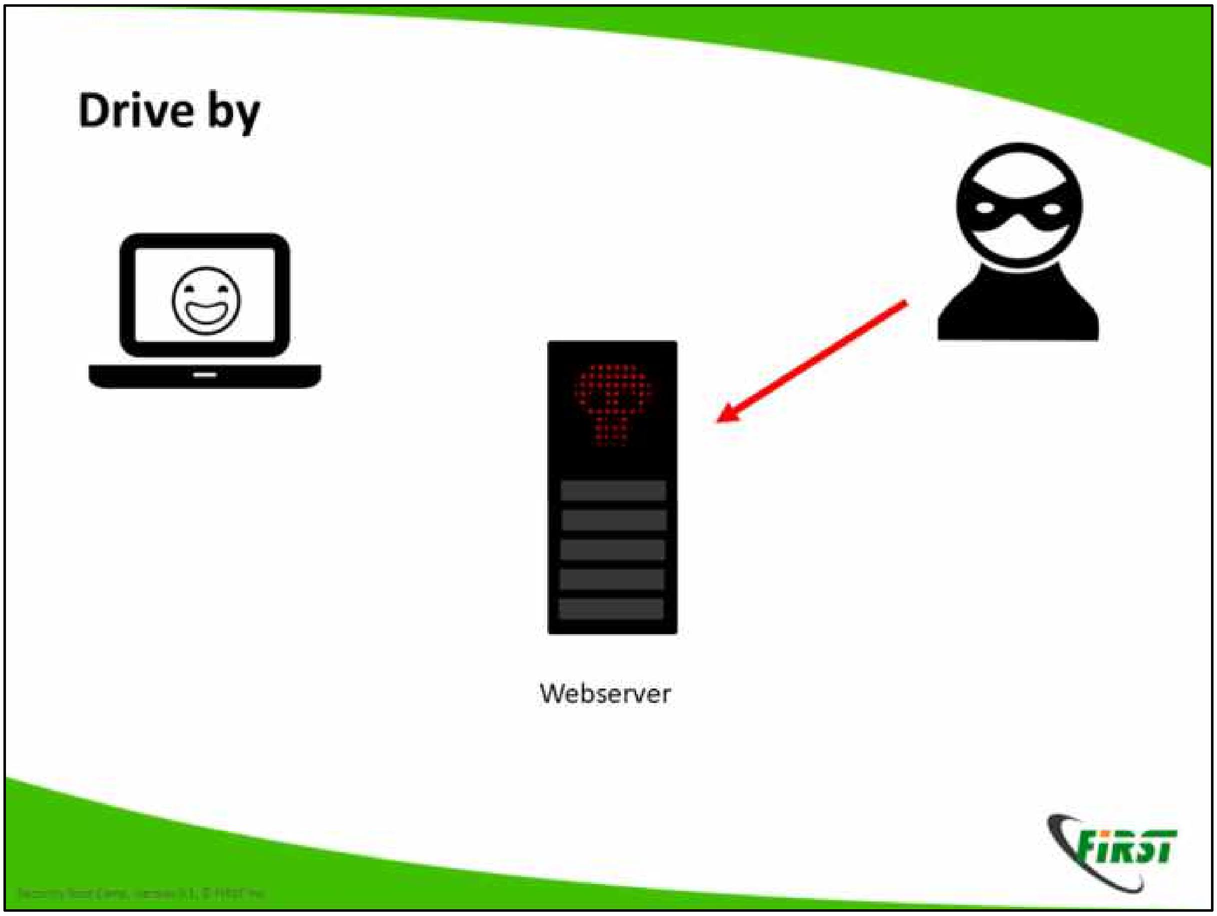
Well, it is. This particular word file executes a macro which exploits a security vulnerability to escape the Word processor and downloads further malware.



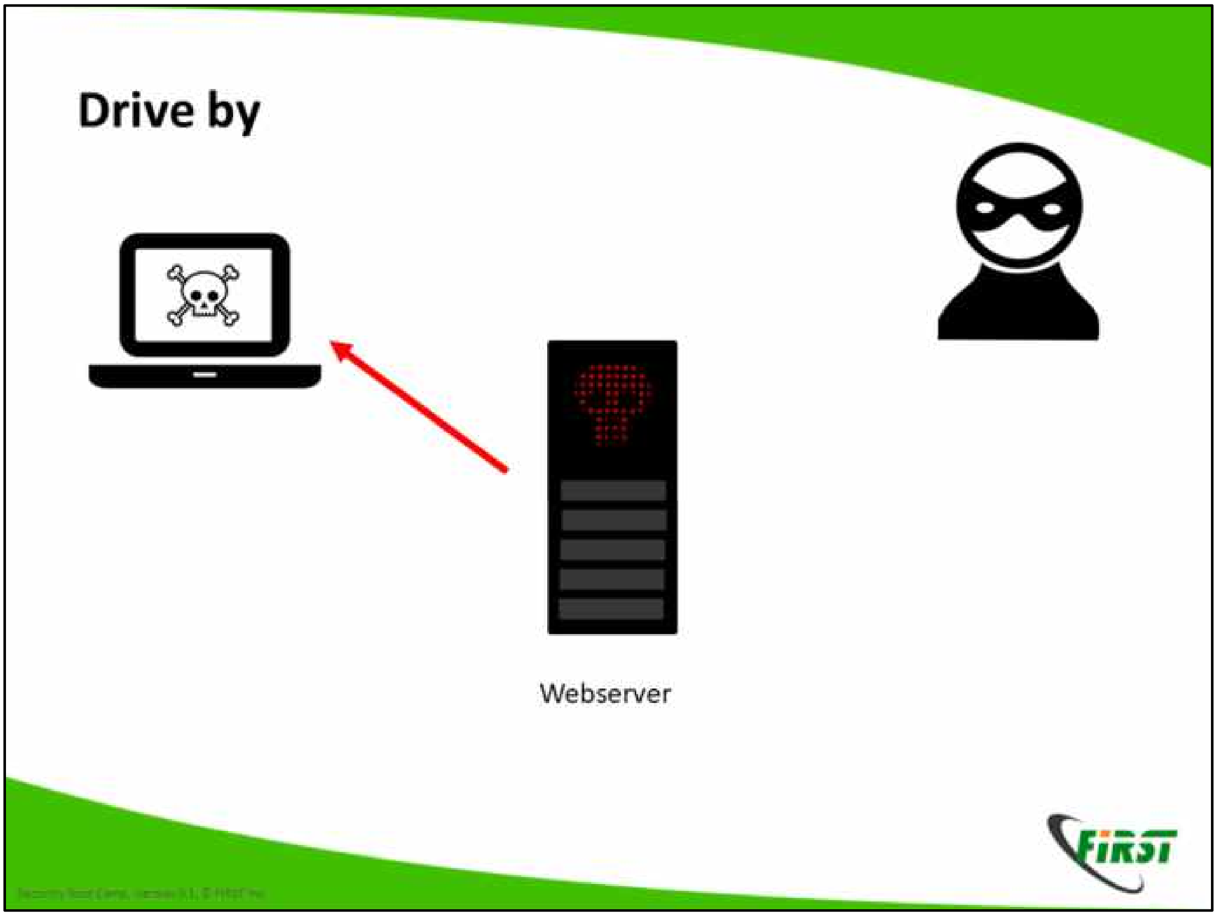
Drive by

Drive by



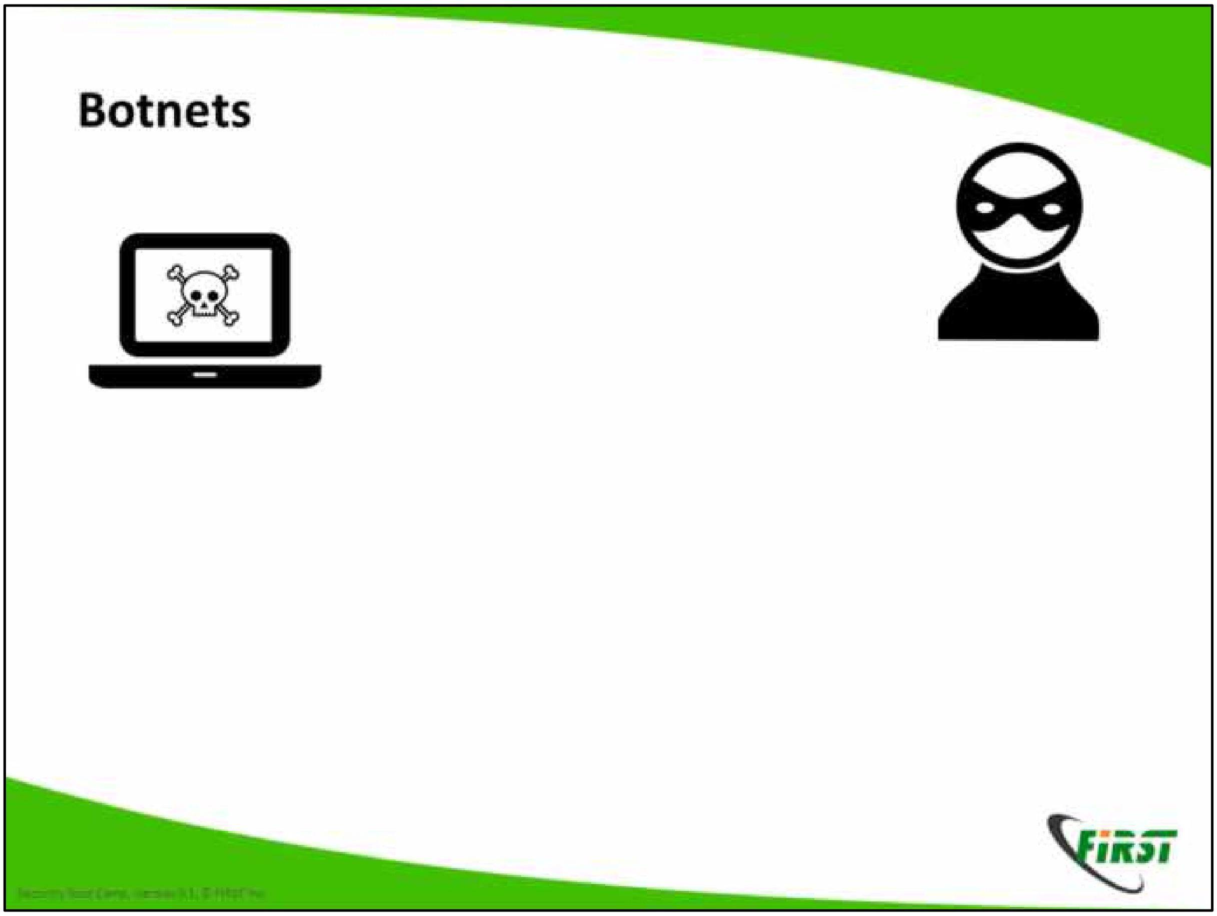


Drive by



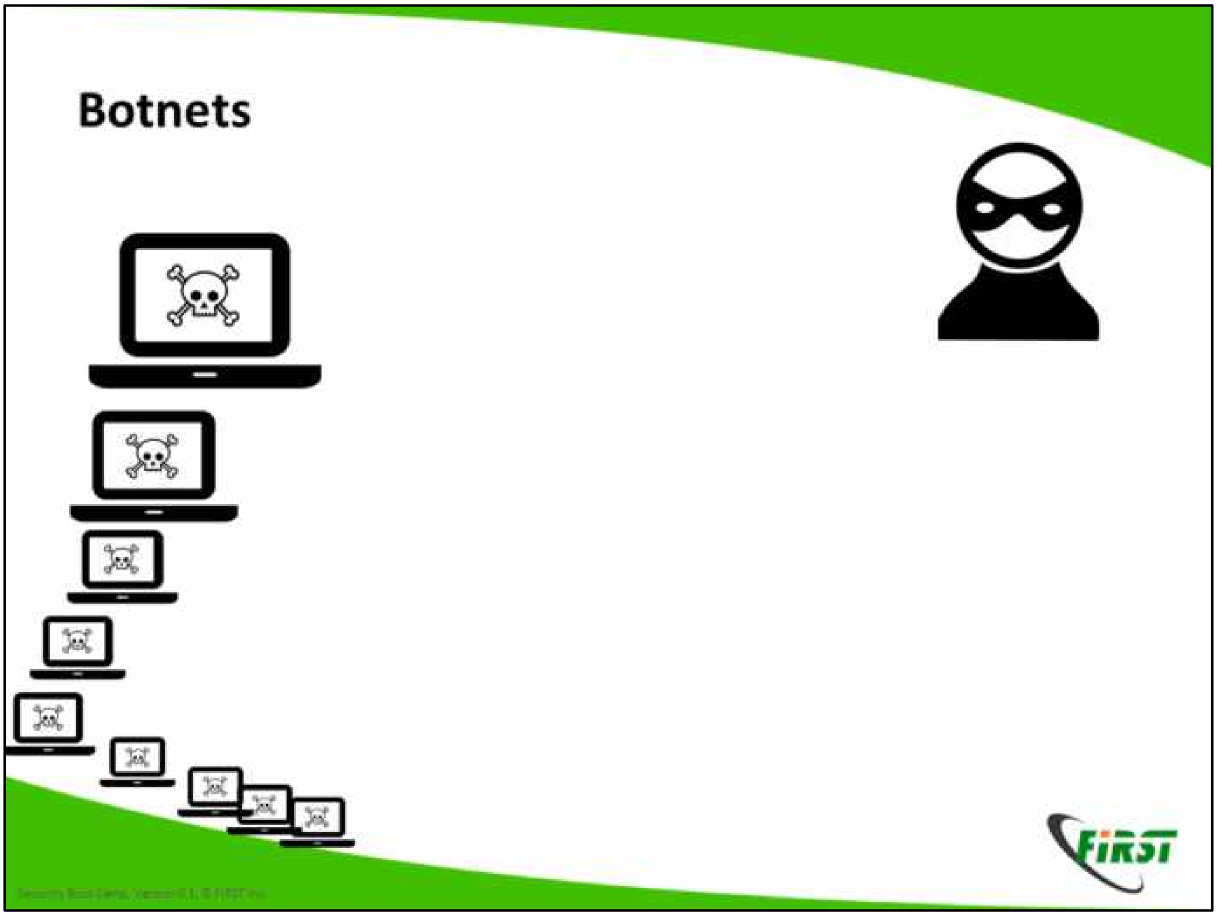
Drive by

Changes on the website are often subtle. Affected are all websites, not just the ones you don’t tell your parents about. An interesting variation is malverizing, where an Add provider is misused to distribute malware through the add. This is much harder to detect, as ads change.



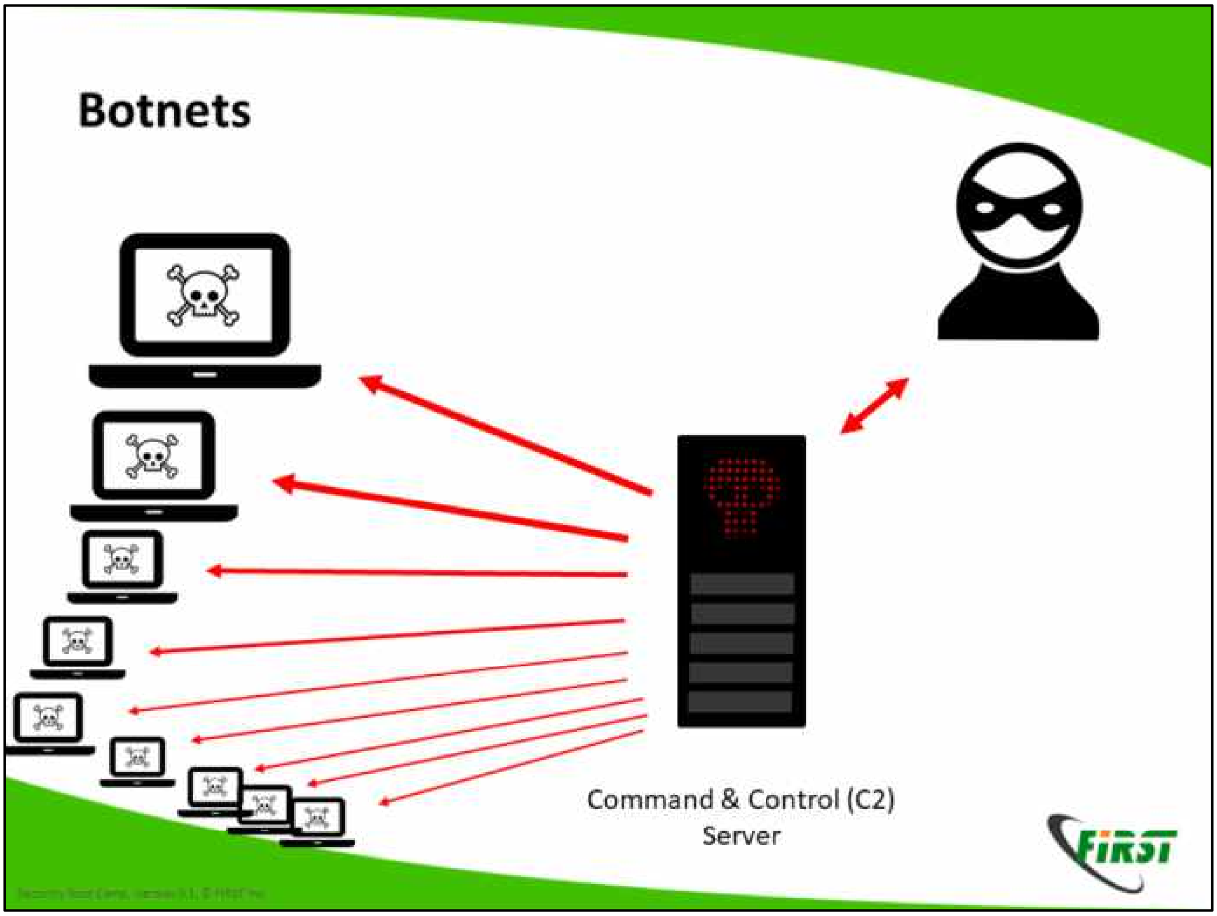
Botnets

One hacked computer is not particularly interesting



Botnets

But thousands are



Botnets

Command & Control (C2)
Server

Security Boot Camp, Version 3.1, © FIRST Inc

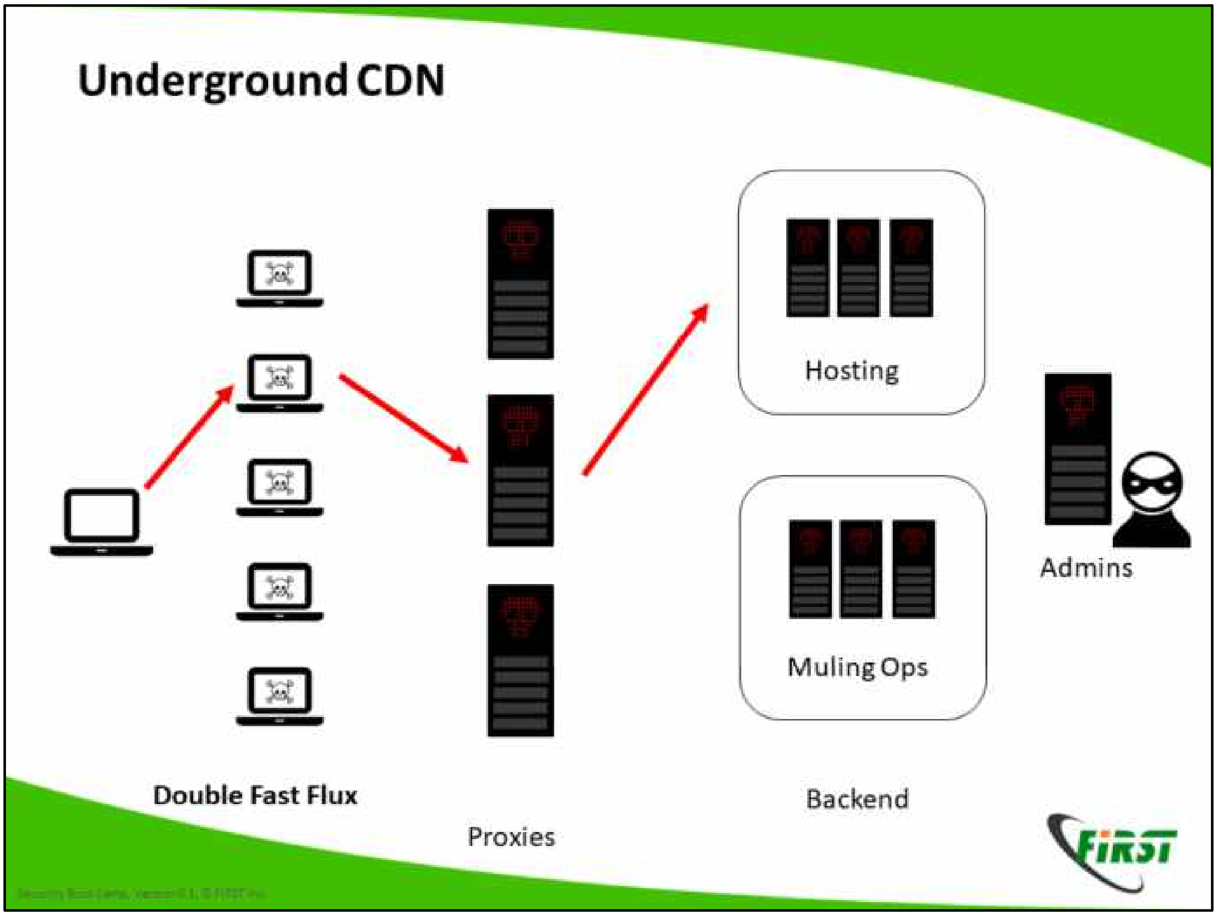
But thousands are interesting. This is the great thing about the internet: Everything scales. Botnets can have from a few hundreds to millions of members. Being cynic one could say they were the first cloud services.

Avalanche Network

CC0 88101559 | Dreamstime Stock Photos

Avalance Takedown
Avalance was a underground hosting infrastructure leveraging Domainnames (first.org) for robustness. To stop its operation 800’000 domain names had to be taken down in dozens of TLDs (.com, .ru). This requires the collaboration with many organisations not traditionally considered part of the CSIRT community. In particular registrars (the domain name eco system) as well as law enforcement.
Both these communites have very different rules:
Registras, in particular the ones responsible for ccTLDs are often very regulated and very reluctant to act.
Law Enforcement is bound very much by legal procedures and typically has a different goal: Arresting criminals vs getting the infrastructure back up.
This makes collaboration often difficult. Policy and law makers can help here. For example the close collaboration of the Registry CSIRT in Switzerland with the regulator has led to the creation of a law that allows the registry to effectively act against cyber crime.
THis was a long effort and required that all involved parties gain a common understanding of the issues.

Underground CDN



Hosting

Muling Ops

Admins

Double Fast Flux

Proxies

Backend

Conclusion

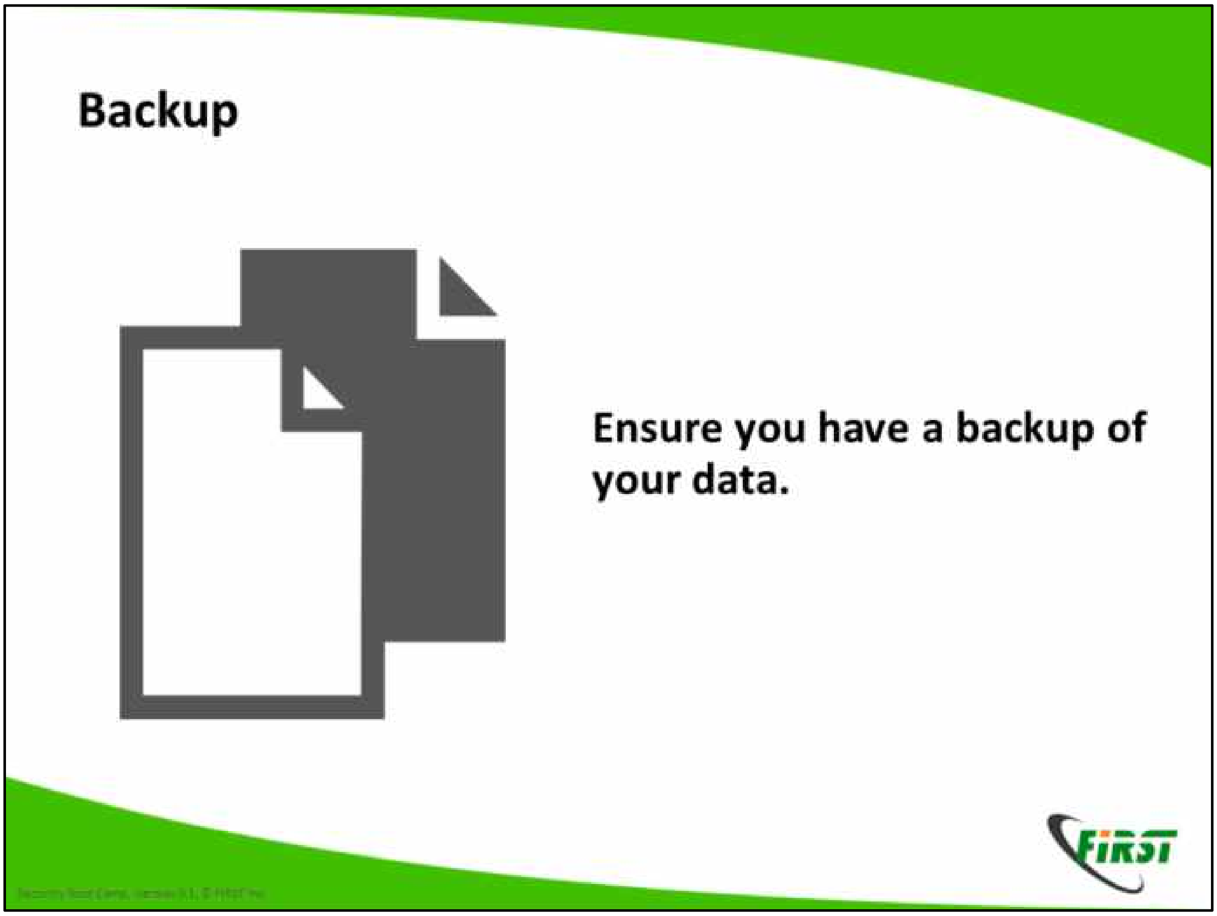
Hacking is an entire industry, with many specialisations. It’s not done by teenagers, but by professionals.

Protecting Yourself

https://www.stopthinkconnect.ch/

Updates

Keep your Operating System and software on all your devices up to date.



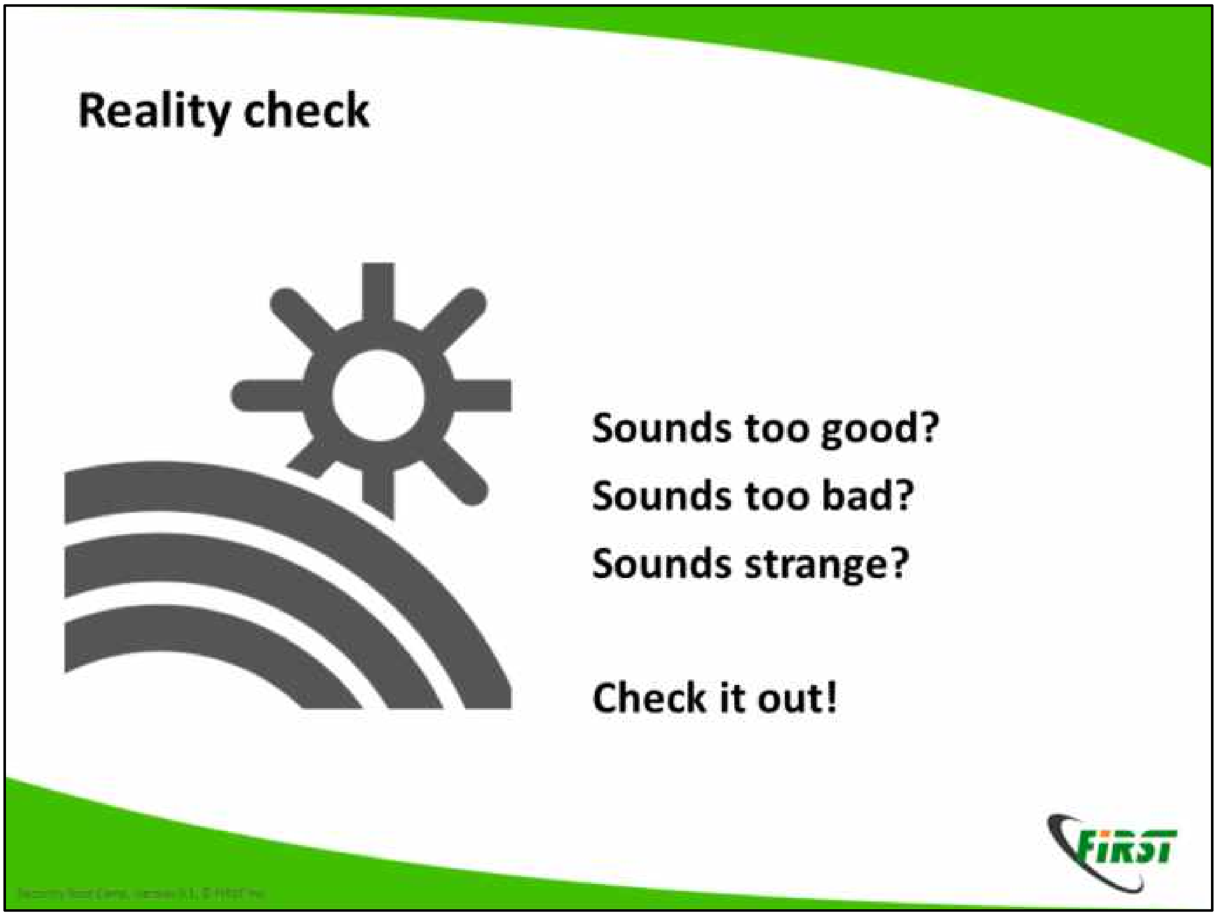
Backup

Ensure you have a backup of your data.

Security Boot Camp, Version 3.1, © FIRST Inc

Strong Passwords

Use strong passwords. Don't reuse them. Enable 2 factor authentication.



Reality check

Sounds too good?

Sounds too bad?

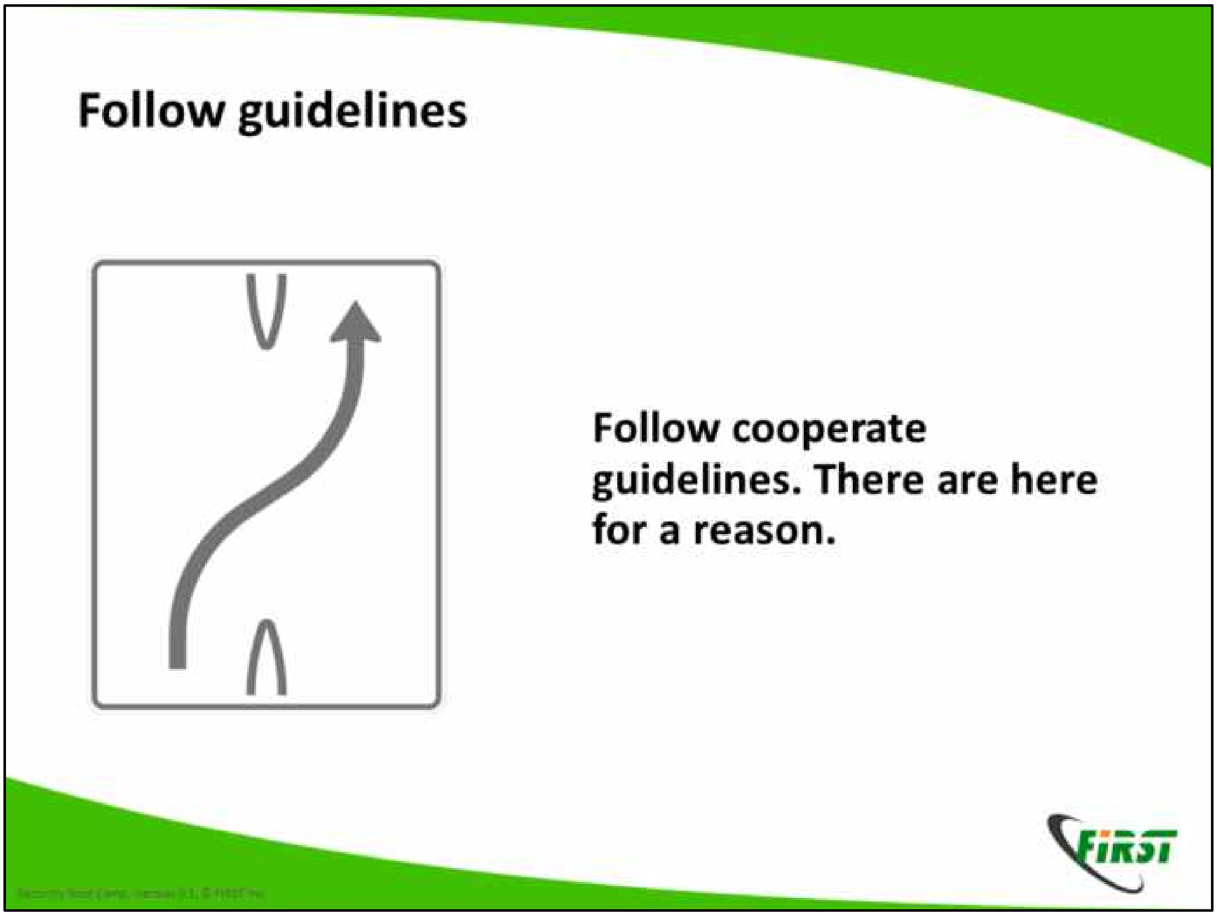
Sounds strange?

Check it out!

Help

You made a mistake?
Something not working?

Get help!



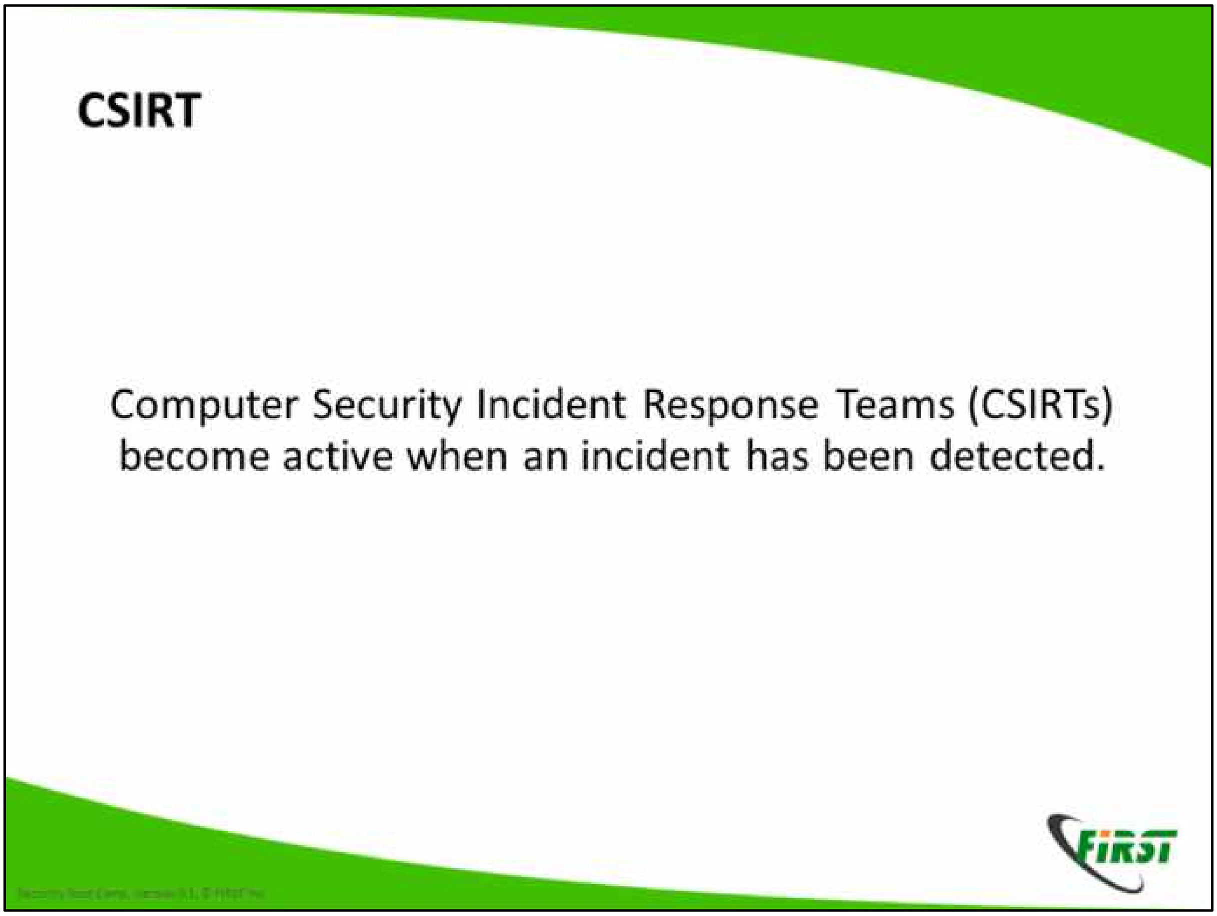
Follow guidelines

Follow cooperate guidelines. There are here for a reason.

Incident Response

CSIRTs are often compared to fire fighters. One could define them as a team of experts coming to action during a cyber security incident. This definition is probably to narrow, CSIRTs today take on many different task, both reactive and proactive.

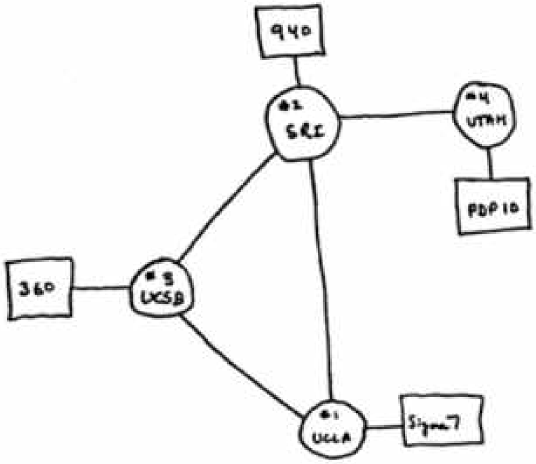
CC0 https://pixabay.com/en/firemen-firefighter-fire-flames-78111/



CSIRT

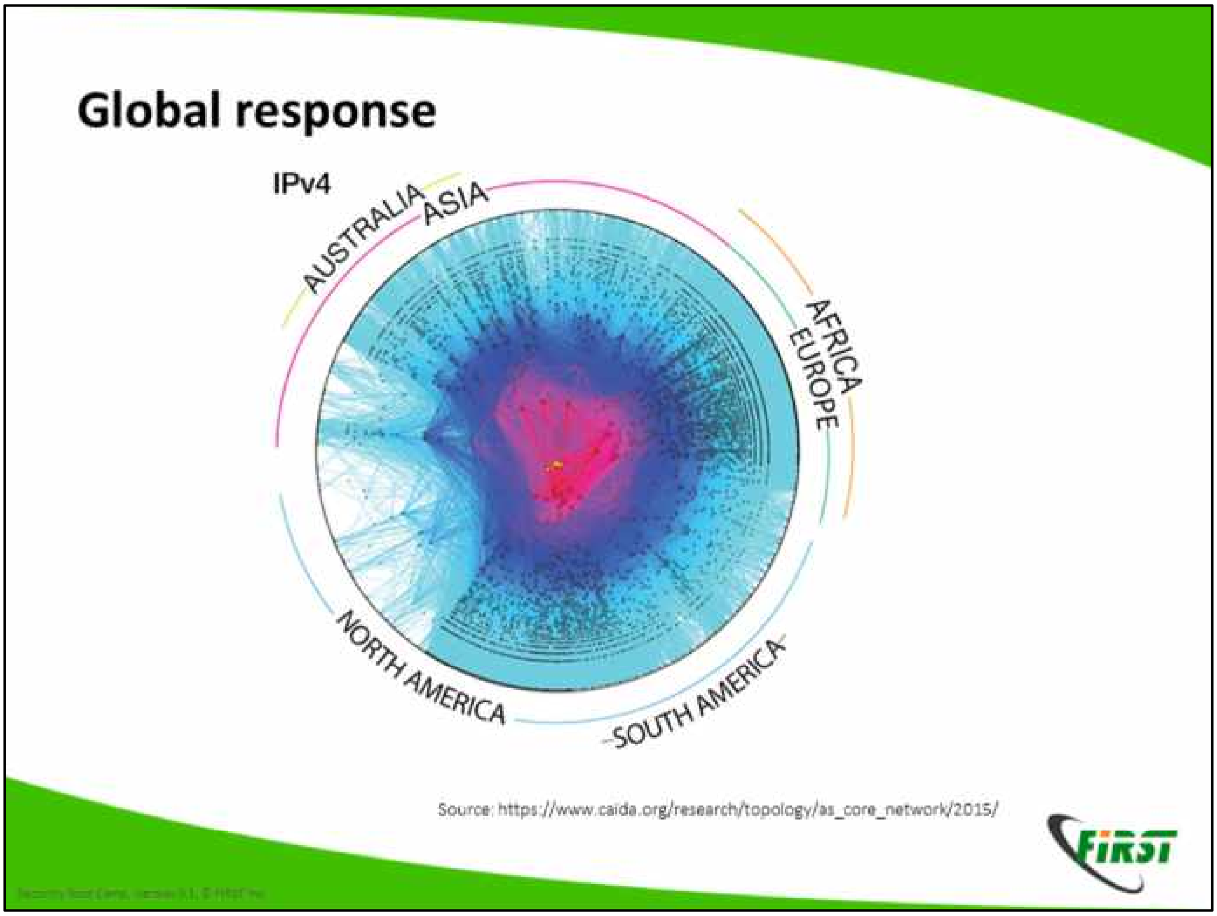
Computer Security Incident Response Teams (CSIRTs) become active when an incident has been detected.

Global response



Source: https://www.darpa.mil/about-us/darpa-history-and-timeline?PP=2

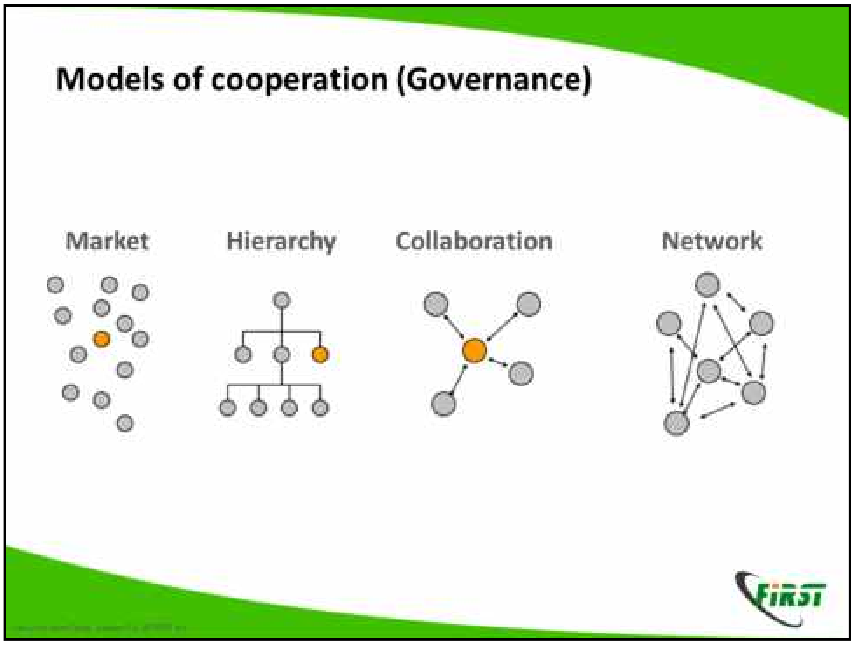
The internet used to be national, in 1969. Response was easy at the times, you just needed three other phone numbers ;-)



Global response

Source: https://www.caida.org/research/topology/as_core_network/2015/

Not so any more. You need to act fast and across many borders.



Models of cooperation (Governance)

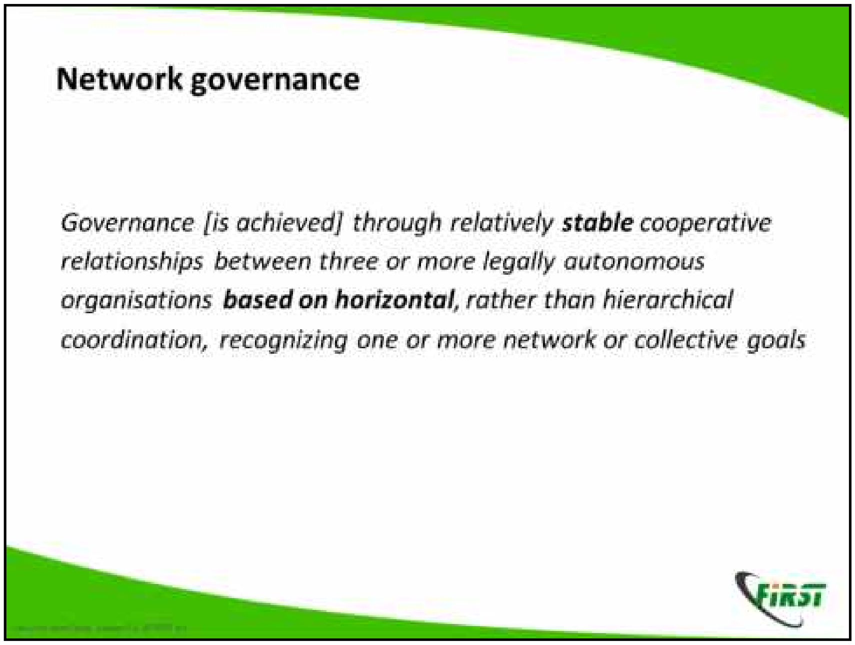
Market

Hierarchy

Collaboration

Network

There are different forms of governance. Common ones include Market (you pay for what you want), Hierarchy (Company's , Army), Collaboration, and lastly network govenance. 1-3 Don’t work: You can’t pay for a server to be taken down, you can’t order it (try it). Collaboration doesn’t scale, we are dealing with thousands of independent players (each of the dots on the previous figure). So let’s look at network governance



Network governance

Governance [is achieved] through relatively ***stable*** *cooperative relationships between three or more legally autonomous organisations* ***based on horizontal****, rather than hierarchical coordination, recognizing one or more network or collective goals*

Here, we’re essentially saying that we work with other towards a common goal at eye level over some time, without any paperpwork.
Common examples: Disaster recovery (Haiti, New Orleans, Puerto Ricco, …) typically grassroot groups working together. In Haity the US Army relied on a google maps project run by a bunch of MIT students for their intel!

Two ingredients for successful coordination

A common goal

A high level of trust

To be effective Networks need a common goal and a high level of trust.
Mind you: Networks are not feel good groups. Its often tough!

Thank you to FIRST for allowing us to use this presentation

Security Boot Camp, Version 3.1, © FIRST Inc.