



Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI

Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI



Asociația pentru Securitatea Sistemelor Informatice a fost înființată în 2012, ca un liant între sectorul public și mediul de afaceri

ANSSI este o organizație neguvernamentală, nonprofit, profesională și independentă.

Asociația reunește 50 de membri, companii având în total aproximativ 25000 de angajați

Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI



Cele mai mari daune: MyDoom - 38.5 miliarde USD

Un vierme polimorf care se raspandea prin email si permitea atacatorului sa preia controlul calculatorului

Social media – 1.7 miliarde conturi active (aprox 2/3 total utilizatori)

600.000 conturi Facebook compromise zilnic

- Like jacking
- Link jacking
- Phishing

99% calculatoare au vulnerabilitati

60% dintre angajati iau cu ei datele la plecare

1 singur grup transnational

- 1 miliard USD in 2 ani
 - 100 de banci
 - 30 de tari
- spear phishing**

68% din sumele pierdute nu pot fi recuperate

Cyber's Most Wanted

Select the images of suspects to display more information.

Search for

Filter by

Filter

Sort by:

Results: 26 Items



IRANIAN DDoS ATTACKS



EVGENIY MIKHAILOVICH BOGACHEV



JOSHUA SAMUEL AARON



NICOLAE POPESCU



FIRAS DARDAR



AHMED AL AGHA



ALEXSEY BELAN



VIET QUOC NGUYEN



PETERIS SAHUROVS



SHAILESHKUMAR P. JAIN



Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI



10 milioane de adrese mail – achiziționate inițial cu 1000 dolari
(prin bitcoin)

1 milion de mail-uri ajung la destinație (10%, prin spam
snowshoe, cost expediere 5000 dolari)

500.000 mail-uri sunt deschise (jumătate dintre cele care trec de
filtre)

50.000 de destinatari accesează adresa web din email (10% dintre
cei care deschid mail-ul)

5.000 de destinatari introduc datele solicitate în pagina web (10%
dintre cei care ajung pe pagina web falsă)

Cost pagina web 4=10.000 dolari

Obs. Procentul celor păcăliți este de 0.05% din totalul
destinatariilor

5.000 de seturi de date privind carduri bancare = 300.000 dolari
(60 dolari/buc)

Sumarizând:

Total investiție = aproximativ 16-20.000 dolari

Venituri = 300.000 dolari

Profit = 1500%!

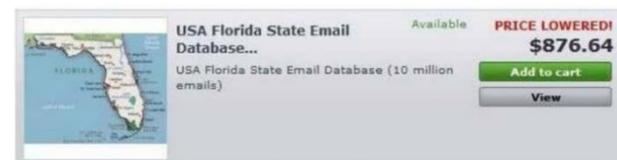


Figure 2. Florida residents email addresses for sale.



Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI



Tendinte globale

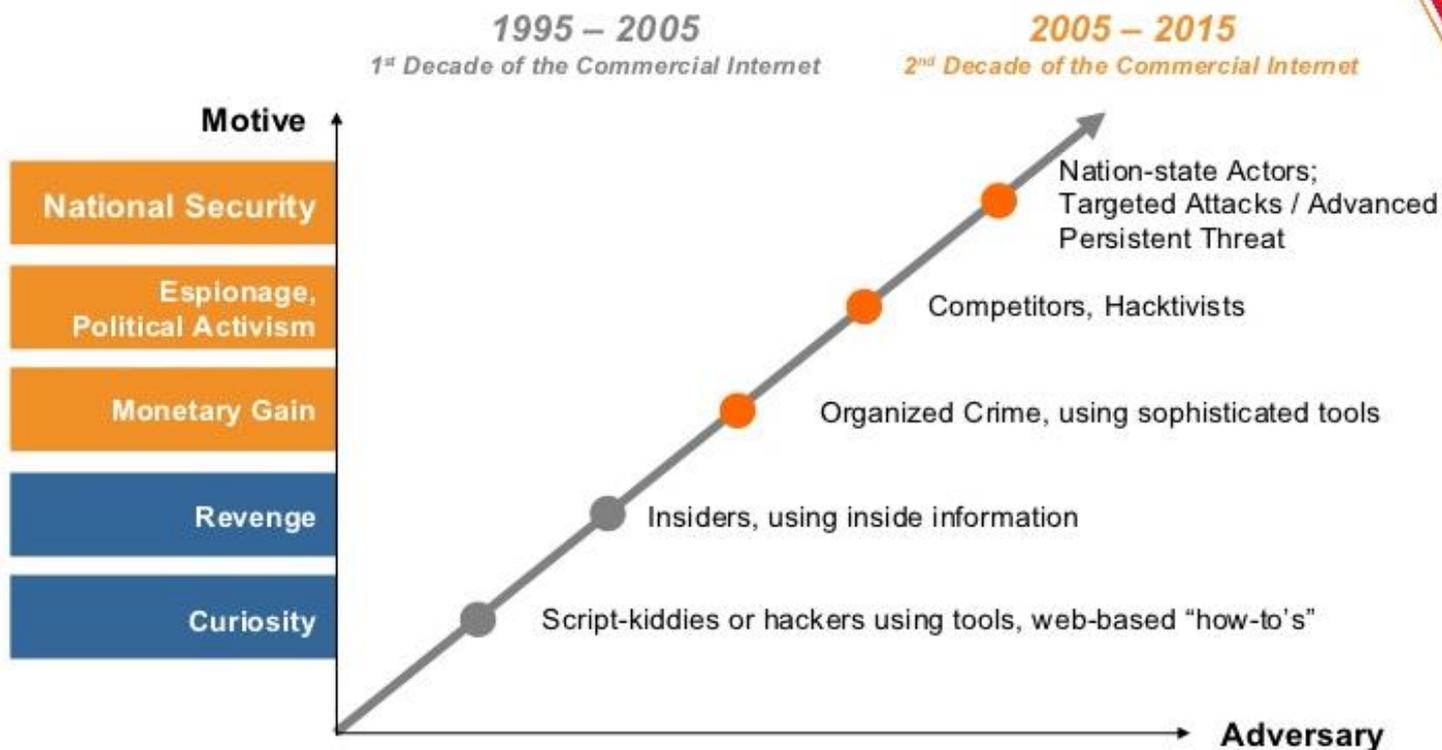
Entitatile ostile

C(ybercrime)aaS

+

Finantele subterane

Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI



Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI



Entitățile ostile

- Grupările de criminalitate informatică, grupările hacktiviste și teroriste
- Actorii statali

Roluri

- Finantator
- Dezvoltator
- Distribuitor
- Client

Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI



Cybercrime-as-a-Service

- Research-as-a-Service
- Crimeware-as-a-Service
- Cybercrime Infrastructure-as-a-Service
- Hacking-as-a-Service

 **France Email Database 1 million** Available **PRICE LOWERED!**
 France Email Database 1 million **\$495.49**
[Add to cart](#)
[View](#)

Prices for zero-day vulnerabilities.

Adobe Reader	\$5,000-\$30,000
Mac OS X	\$20,000-\$50,000
Android	\$30,000-\$60,000
Flash or Java Browser Plug-ins	\$40,000-\$100,000
Microsoft Word	\$50,000-\$100,000
Windows	\$60,000-\$120,000
Firefox or Safari	\$60,000-\$150,000
Chrome or Internet Explorer	\$80,000-\$200,000
IOS	\$100,000-\$250,000



Email Password Cracking made easy..!!
Request an E-mail Password :-
 Fill in the below form to the best of your knowledge. Make sure that the email addresses are entered correctly. Once submitted, check your email for a confirmation mail. Add our email address(es) in your address-book, to prevent our emails and the proofs landing in bulk folder. Once you verify the order by clicking on the confirmation link sent to you, we will process your order.

Your Name

Your Email Address

Confirm your Email Address

Your Country

Most Urgent Urgent Just do it whenever you can

Victim Name

Victim Email Address

Confirm Victim Email Address

Victim Victim Country

Victim Language

Optional Information :-

How you know us

Your Yahoo! Chat ID

Your MSN Chat ID

Preferred Mode of Payment

Bonus offered (if any)

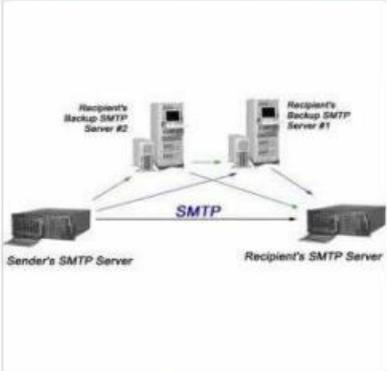
Any Instructions ?

[Submit your Order](#)

Available **PRICE LOWERED!**
 (10 million) **\$876.64**
[Add to cart](#)
[View](#)

Home > Smtip Relay Server > Smtip Relay Server for 30 000 000 emails

SMTP RELAY SERVER FOR 30 000 000 EMAILS



Smtip Relay Server for 30 000 000 emails for the one month.

PRICE LOWERED!
\$13,340.25 tax incl.
~~\$14,822.50 tax incl.~~
 (price reduced by 10 %)

Quantity :

Availability: 999 items in stock

[Add to cart](#)
[Add to my wishlist](#)


 Click here to pay

10- th version.

Packages:

- â€¢ Minimum: DDoS Bot, no free updates, no modules = \$450
- â€¢ Standart: DDoS Bot, 1 month free updates, password grabber module = \$499
- â€¢ Bronze: DDoS Bot, 3 months free updates, password grabber module, 1 free rebuild = \$570
- â€¢ Silver: DDoS Bot, 6 months free updates, password grabber module, 3 free rebuilds = \$650
- â€¢ Gold: DDoS Bot, lifetime free updates, password grabber + "hosts" editor modules, 5 free rebuilds, 8% discount on other products. = \$699
- â€¢ Platinum: DDoS Bot, lifetime free updates, password grabber, unlimited free rebuilds, 20% discount on other products. = \$825
- â€¢ Brilliant: DDoS Bot, lifetime free updates, unlimited free rebuilds, all modules for free, 25% discount on other products. = \$999

Other:

- â€¢ ReBuild (URLs changing) â€¢ \$35.
- â€¢ Sources - ~3500-5000\$, discuss individually
- â€¢ New features - discuss individually.
- â€¢ Web-Panel reinstalling (1st time is free) - \$50



Botnet services

CHEAP PROFESSIONAL DDOS SERVICE

Cheap Professional **DDOS** Service
Trusted
Strong/Fast Service
Takes down Large Website/Forum/Game Servers etc.
No time limit

PRICE

1 - 4 hours / 2\$ per hour
5 - 24 hours / 4\$ per hour
24 - 72 hours / 5\$ per hour
1 month / 1000\$ fix price

PAYMENT ACCEPTED

Paypal (Verified users only)
Liberty Passerby
Western Union
MoneyBookers

CONTACT

Yahoo Messenger : _____
Msn : _____
Skype : _____

credit card

	US		EU	
Visa Classic	\$15	\$80	\$40	\$150
Master Card Standard		\$90		\$140
Visa Gold/Premier	\$25	\$100 \$200	\$45	\$160 \$250
Visa Platinum	\$30	\$110	\$50	\$170
Business/Corporate	\$40	\$130	\$60	\$170
Purchasing/Signature	\$50	\$120	\$70	
Infinite			\$130	\$190
Master Card World		\$140		
AMEX	\$40		\$60	
AMEX Gold	\$70		\$90	
AMEX Platinum	\$50			

Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI



Finantele subterane

anonimat
viteza de transfer
cost redus
transfer ireversibil



Payment purpose	Payment for	Common payment mechanisms	Example
Victim payment	Extortion	Bitcoins, Bank Transfer, paysafecard	Payment extorted as a result of a ransomware or DDoS attack
	Fraud	Bitcoins, Bank Transfer, Western Union	Loss to an online fraud/scam
Criminal to criminal payment	Counter AV	PayPal	Testing of malware against commercial AV products
	Data	Bitcoins, Ukash, Western Union, Webmoney	Purchase of compromised financial data such as credit cards
	DDoS	Bitcoins	DDoS service for hire
	Hosting	Bitcoins	Purchase of hosting (including bulletproof)
	Malware	Visa, MasterCard, WebMoney, PayPal	Purchase of malware, such as RATS and banking trojans
	Trade on hidden service	Bitcoins, Ukash, paysafecard	Purchase of drugs or weapons
Payment for legitimate service		Bitcoins, Bank transfer, Visa, MasterCard	Hosting, hardware, software, travel, accomodation etc
Money movement		Bitcoins, Bank transfer, Western Union	Movement of money to maintain control of funds or hide/break a financial trail, including „cashing-out” of compromised financial accounts. This also includes exchange to, from or between virtual, digital and fiat currencies

Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI



Internet of Things

IoBadT – vulnerabilitati intrinseci (voite?)
Compromitere – atac, spionaj etc.

Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI

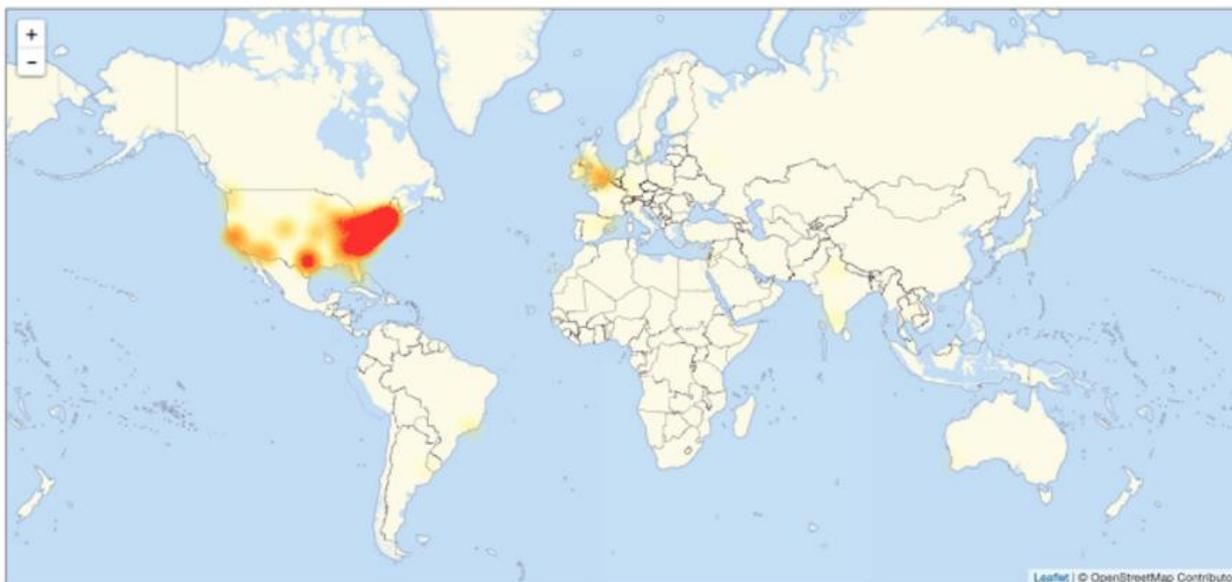


Wired: “All of this is possible only because Chrysler, like practically all carmakers, is doing its best to turn the modern automobile into a smartphone. Uconnect, an Internet-connected computer feature in hundreds of thousands of Fiat Chrysler cars, SUVs, and trucks, controls the vehicle’s entertainment and navigation, enables phone calls, and even offers a Wi-Fi hot spot. And thanks to one vulnerable element, which Miller and Valasek won’t identify until their Black Hat talk, Uconnect’s cellular connection also lets anyone who knows the car’s IP address gain access from anywhere in the country”

Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI



outage map



Dyn DNS: Twitter,
Spotify, SaneBox,
Reddit, Box, Github,
Zoho CRM, PayPal,
Airbnb, Freshbooks,
Wired.com, Pinterest

According to Dyn DNS, the DDOS started at 11:10 UTC and is mostly affecting its customers in the East Coast of the United States, specifically Managed DNS customers.

Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI



Now Klaba added further information on the powerful DDoS attacks, the CTO of the OVH claimed that the botnet used by attackers is powered by more than 150,000 Internet of Things (IoT) devices, including cameras and DVRs.

The overall botnet is capable of launching attacks that exceed 1.5 Tbps.



Octave Klaba / Oles @olesovhcom

22 Set

Last days, we got lot of huge DDoS. Here, the list of "bigger that 100Gbps" only. You can see the simultaneous DDoS are close to 1Tbps !
pic.twitter.com/XmlwAU9JZ6



Octave Klaba / Oles
@olesovhcom

 Segui

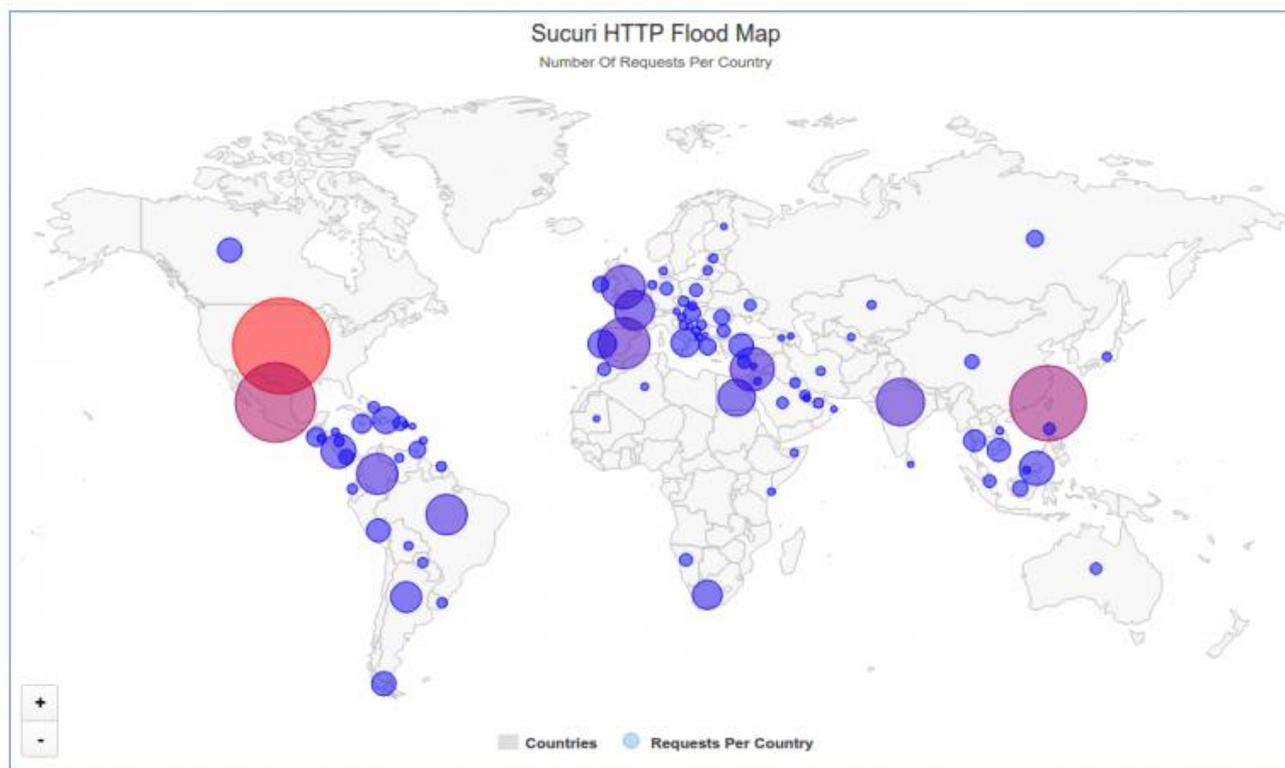
This botnet with 145607 cameras/dvr (1-30Mbps per IP) is able to send >1.5Tbps DDoS. Type: tcp/ack, tcp/ack+psh, tcp/syn.

15:31 - 23 Set 2016

  614  412

OVH hosting provider
DDoS attack

Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI



CCTV Botnet:
105 tari
25000+ IPs
24% Taiwan
12% US

Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI

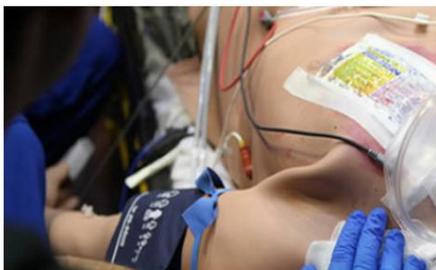


NEWS ANALYSIS

Researchers hack a pacemaker, kill a man(nequin)

Researchers decided you don't need to be a pen tester to wirelessly hack a pacemaker, to successfully launch brute force and denial of service attacks that can kill iStan simulated humans.

MORE



CNET > Security > Samsung's warning: Our Smart TVs record your living room chatter

Samsung's warning: Our Smart TVs record your living room chatter

Technically Incorrect: Samsung's small print says that its Smart TV's voice recognition system will not only capture your private conversations, but also pass them onto third parties.

Security

February 8, 2015
2:10 PM PST



by *Chris Matyszczyk*
@ChrisMatyszczyk



Technically Incorrect offers a slightly twisted take on the tech that's taken over our lives.

Why worry about Big Brother?

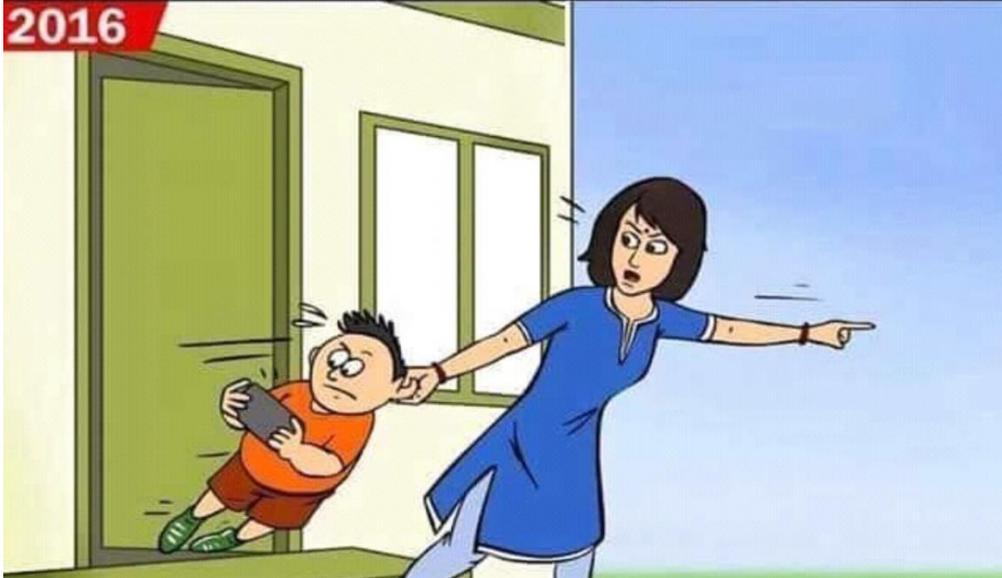
It's your big Samsung TV that's watching you.
Oh, and listening to you.



1996



2016



Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI



Amenințari

- Denial of service
- Botneți și atacuri malware
- Accesul neautorizat la date
- Breșe accidentale
- Protectie redusa la nivel de conexiune

Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI



Internet of Things

Cel mai întâlnit scenariu este utilizarea de botneți alcătuiți din mii de dispozitive din domeniul IoT, cunoscute și sub denumirea de thingboți, care sunt utilizați pentru a trimite mesaje de spam sau pentru coordonarea unor atacuri DDoS. Rezumând, un thingbot poate fi utilizat pentru:

- spam
- coordonarea un atac împotriva unei infrastructuri (critice)
- furnizarea de malware.
- ca punct de intrare în rețeaua unei companii.

Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI



OTA (Online Trust Alliance): IoT / Orice vulnerabilitate din noiembrie 2015 si pana in prezent ar fi putu fi evitata

Gartner: 2015-5 miliarde IoT, 2020 – 21 miliarde IoT

Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI



Actiuni in sensul cresterii nivelului de securitate cibernetica:

Organizatiile apeleaza la instrumente mai sofisticate pentru **prevenirea** atacurilor si **reducerea impactului** lor + **competente tehnice**

Vendorii de tehnologie – **identificarea vulnerabilitatilor**

Coalizarea vendorilor de solutii de securitate

Evolutia **cadrului legislativ**

- roluri si responsabilitati
- caracterul transfrontalier
- tratarea unitara cu actiunile din lumea reala
- instrumente, mecanisme si proceduri

Cooperarea **public-privat**

Asociația Națională pentru Securitatea Sistemelor Informatice ANSSI



Pasii urmatiori:

Cadrul legal, compatibil UE si NATO, in domeniul securitatii cibernetice

Parteneriatul Public-Privat Contractual (cPPP)

CERT-uri sectoriale

Conditii tehnice minime pentru sistemele informatice, raportat la natura informatiilor tranzactionate

SLA-uri pentru vendorii de tehnologie

Standarde ocupationale

Mentenanata sistemelor si auditarea periodica

Cultura de securitate – infomare, instruire, cooperare



**Asociația Națională pentru
Securitatea Sistemelor Informatice
ANSSI**

Va multumesc!