S21sec

Committed to cybersecurity

CyberSecurity: Cooperation as a way of defense

EIN2016 – April, 29th 2016 (Academia Militar, Lisboa)

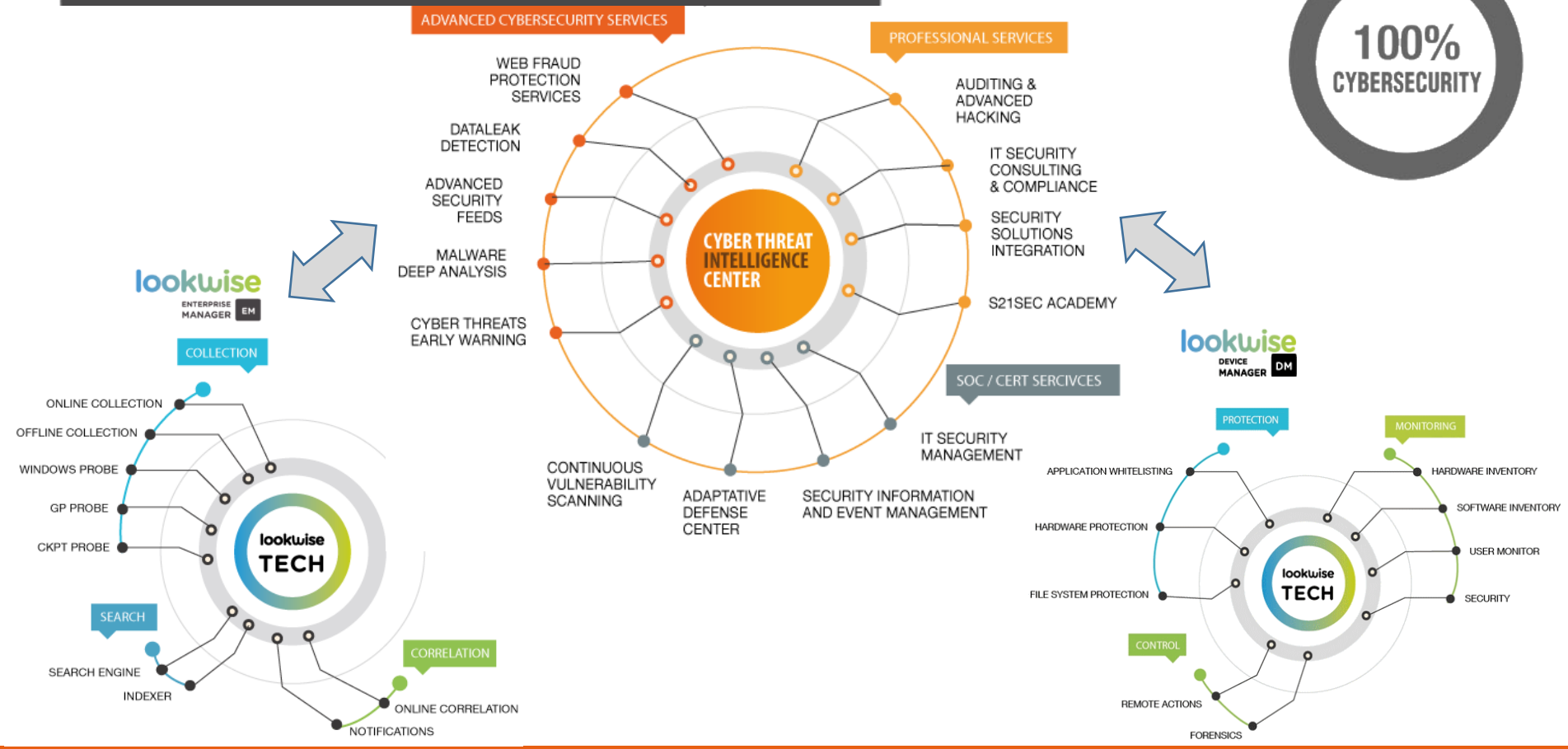
www.s21sec.com


16 YEARS
experience
in the
business of
cibersecurity.

DELIVERING INNOVATION AND QUALITY AS A STANDARD

CYBER THREAT INTELLIGENCE CENTER

PURE PLAY CYBERSECURITY COMPANY



S21sec

We collaborate with Governmental and Public Sector Institutions

We are involved in International Forums dedicated to Cyber

We also work on EU projects

S21sec

Cooperation with the EC3

BRIEF HISTORY OF THE COOPERATION OF S21SEC WITH THE POLICE AUTHORITIES AND DEFENSE ORGANISMS.

In 2015 S21sec signs a MoU with EC3. S21sec becomes the first Spanish enterprise (and one of two in the Iberian Peninsula) who has signed this type of agreement in order to fight against European and worldwide cybercrime.

EUROPOL AND S21SEC START COOPERATION TO COMBAT CYBERCRIME

11 February 2015

Europol's European Cybercrime Centre (EC3) has signed a Memorandum Of Understanding with S21sec, allowing for cooperation in the joint fight against cybercrime. The two organisations will start to exchange knowledge and expertise on cybercrime, and will cooperate to combat online fraud and make the Internet a safer space.

S21sec

BRIEF HISTORY OF THE COOPERATION OF S21SEC WITH THE POLICIAL AUTHORITIES AND DEFENSE ORGANISMS.

In 2016 S21sec agrees to take part of the Internet Security Advisory Group from Europol EC3.

EC3 ADVISORY GROUPS

Established by the EC3 Programme Board and reporting to it, dedicated advisory groups have been created in order to foster closer cooperation with its leading non-law enforcement partners. They help to strengthen practical cooperation between law enforcement and key domains, such as internet security and financial services.

INTERNET SECURITY

Mandate:

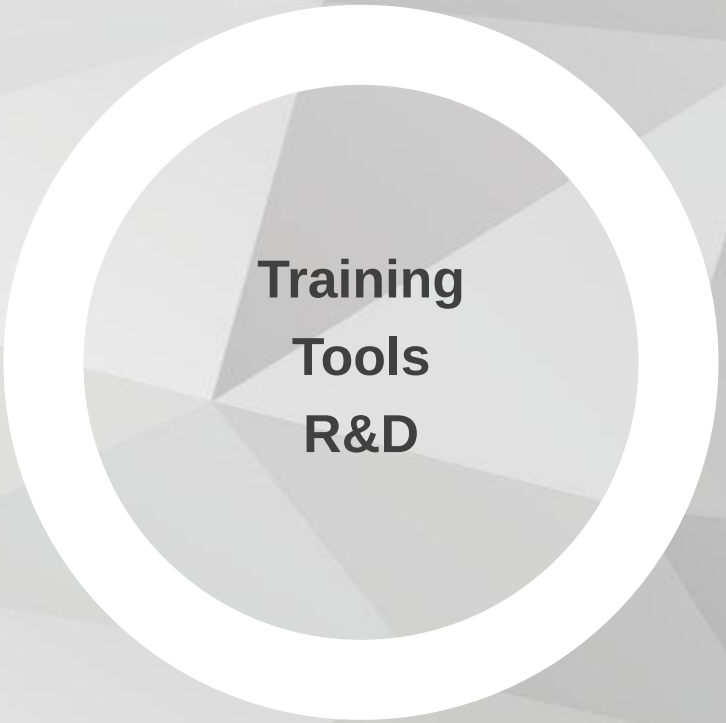
With a view of getting a clear overview of the needs and priorities for internet security in the context of the cross-border fight against cybercrime, the purpose of the Group is to:

- bring knowledge and expertise to the Programme Board on matters related to internet security;
- update and share all relevant information and expertise on developments in the area of internet security;
- assist the Programme Board in defining priorities for the work of the EC3 in this area, including advising on the cooperation with CERTs and other relevant partners and on developing concepts for enhanced prevention of cybercrime;
- assist the EC3 Programme Board in striking the right balance between disruption and prevention on the one hand and investigation and prosecution on the other.

Members

Akamai, Anubis Networks, Belgacom group, Bitdefender, Blackberry, Check Point, Cisco, CSIS – Norwegian Center for Cyber and Information Security, ENISA, FireEye, Fortune 500, Fox-IT, GroupIB, Hewlett Packard Enterprise, IRISSCERT, Kaspersky, McAfee, Microsoft, Mnemonic, Trend Micro, UNICRI, SSH Communications Security, Stuart Hyde Associates, Symantec, S21Sec, the Shadowserver Foundation EU and a representative from the European Commission (DG Home)

Needs identified by the police authorities



WHAT CAN PRIVATE COMPANIES GIVE TO POLICE AUTHORITIES AND SECURITY ENTITIES?

- Training:
  - From the most common topics that every company can adopt, up to highly specialized courses.
  - Local and online training, with a high demand nowadays from multiple entities, not only the ones that work directly with cybercrime and actively fighting it.
  - What drives others and inspire trust are persons and not the companies itself.
  - CNEC:

CNEC
CENTRO NACIONAL
EXCELENCIA EN CIBERSEGURIDAD

SPANISH NATIONAL CENTRE OF EXCELLENCE ON CYBERSECURITY
Final Project results
European Cybercrime Training and Education Group
Europol, The Hague

- 2 year project: Nov 2012 – Nov 2014
- Beneficiaries
  - Universidad Autónoma de Madrid
  - S21sec
- Associate partners
  - Guardia Civil
  - Cuerpo Nacional de Policia

WHAT CAN PRIVATE COMPANIES GIVE TO POLICIE AUTHORITIES AND SECURITY ENTITIES?

- Tools:
  - Publicly available tolos rarely cover 100% the needs of policial authorities and other security entities.
  - There is an highly demand for tools that can help, and ease, day-to-day tasks as well as the work of policial investigation.
  - At a regional level (Iberia), the main constraint is the lack of budget and financial resources within public administration.
  - Digital Surveillance

WHAT CAN PRIVATE COMPANIES GIVE TO POLICE AUTHORITIES AND SECURITY ENTITIES?

- R&D:
  - Colaborative projects are the most advantegeous format for both parties, private and public sector.
  - Public sector are extremely keen for this type of colaborations.
  - Good opportunities to reach european funds.
  - CAPER:

CAPER

COLLABORATIVE INFORMATION, ACQUISITION, PROCESSING, EXPLOITATION AND REPORTING FOR THE PREVENTION OF ORGANISED CRIME

Success story

Dridex

Success story: DRIDEX

- **Dridex** is a banking malware that first appeared in July 2014.

  It's main propagation strategy is by using e-mail, with the use of stolen account or changed in the source.

From: *Wayne Moore [wayne44118@orionplastics.net]*

Date: *8 April 2015 at 09:03*

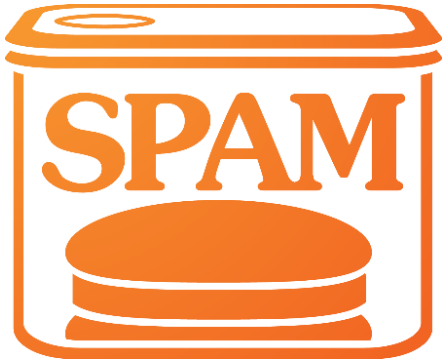
Subject: *TWO UNPAID INVOICES*

LAST WEEK I CALLED REGARDS TWO UNPAID INVOICES FROM JAN 2015 INVOICE # 029911 DATED 1/7/15 FOR $840.80 INVOICE # 030042 DATED 1/30/15 FOR $937.00

PLEASE ADVISE WHEN YOU SENT CHECK AND TO WHAT ADDRESS

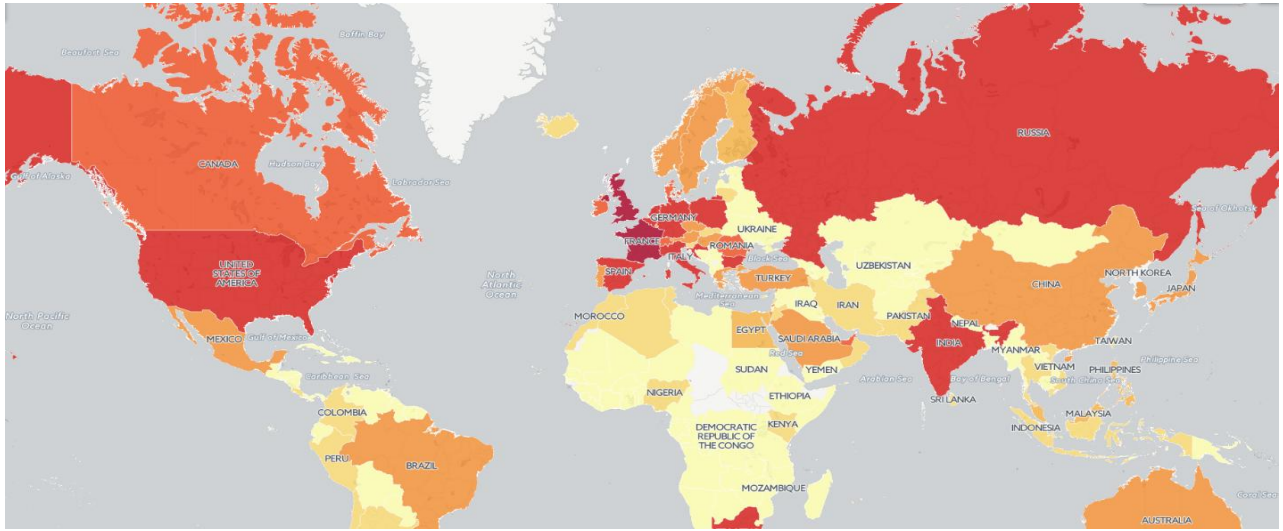
I HAVE ATTACHED THE NEW REMIT TO ADDRESS IN CASE YOU DON'T HAVE IT

REGARDS-WAYNE



Success story: DRIDEX

- **Dridex** major impacts was mainly in Europe and United States of America, through the use of two distinct malicious networks. The European network strongly attacked United Kingdom and France. During it's peak phase, there were roughly 344.000 infected devices.



COUNTRY	INFECTIONS
GB	46833
FR	22524
US	13350
IT	10924
BG	9268
HR	5066
BE	4508
PL	4012
IN	2969
ZA	2876

Success story: DRIDEX

- In October 2015, a joint operation between the **FBI**, **NCA** and **Europol** dismantled the Dridex infrastructure, which had an estimation of, at least, 50 Millions of dollars stolen. **S21sec** was a key player by adding its knowledge and experience to the investigation.

Forbes / Security

Cops Knock Down Dridex Malware That Earned 'Evil Corp' Cybercriminals At Least $50 Million

FBI and UK cops smash Dridex high-stakes bank-raiding botnet

The days may be numbered for an eastern European hacking gang and their banking malware botnet Dridex.

Success story: DRIDEX

- *During the last months of 2015* **Dridex** comes back.

  S21sec still is collaborating with Europol nowadays.

S21sec

Other colaborations

- ENISA
- ECSG
- INCIBE
- Others...

enisa
European Network and Information Security Agency

Smart Grid Security

1sec y ENISA abogan por coordinar trategias conjuntas para mejorar la guridad industrial en la Unión Europea

/ 2014
ec ha realizado el trabajo de campo y ha colaborado con ENISA en la elaboración del estudio sobre Testing nation Capability

n los principales riesgos de los mundos

a a la cabeza como el principal riesgo que perciben studio.

la información y redes, ENISA ha publicado un nuevo estudio sobre bre la seguridad en los mundos virtuales.

lo S21sec, compañía líder en seguridad digital, dando su visión y o: "**Security and privacy in massively-multiplayer online games and social and corporate virtual worlds**". Este es el segundo estudio en el que S21sec colabora con ENISA como fuente de datos, como ya hiciera el pasado año con el Estudio sobre Botnets, la amenaza silenciosa.

Published December 10, 2013
Authors • Adrian Pauna, ENISA, • Konstantinos Monreal Ibañez, S21sec, • Luis Tarrafe S21sec, • Jairo Alonso Ortiz, S21sec, • Goicoechea, S21sec

S21sec

- ECS

MEMBERS

CSIS LEXSI ANTICIPATE & RETALIATE S21sec FOX IT FOR A MORE SECURE SOCIETY

EUROPE'S LARGEST AND MOST AGILE **PROVIDER OF CERT EXPERTISE**

The ECSG is an expert consortium of like-minded, independent cyber security firms across Europe dedicated to reducing cyber risk and improving cyber defense through direct services and expert advocacy. The ECSG is a not for profit foundation based in the Netherlands. Cyber security is what we breathe and live every day; it's not work, but a way of life. As independents, the only people we serve are our clients, whose security we take as seriously as our own.

Seeing the cyber security threat horizon morph and accelerate, while helping organizations both public and private as they struggle to respond, we decided to join forces for the common good. With more than 600 experts, the ECSG is now effectively the largest European provider of CERT Computer Emergency Response – services. By working together, we each bring our own firms' uniqueness to the table to deliver faster and more complete solutions in agile ways that a single, large organization simply cannot.

ECSG – EUROPEAN CYBER SECURITY GROUP

MORE THAN 1 MILLION PEOPLE **BECOME VICTIMS OF CYBER CRIME EVERY DAY**

- Identify and analyze the source of the breach
- Assess of the extent of the damage and the depth of the intrusion
- Develop a containment strategy to ensure that no further harm results from the initial breach
- Communicate effectively with customers, regulators, law enforcement, media, and other key stakeholders
- Deliver post-incident reporting with specific recommendations to improve your future security
- Liaise with law enforcement and assist with investigation, attribution, and prosecution

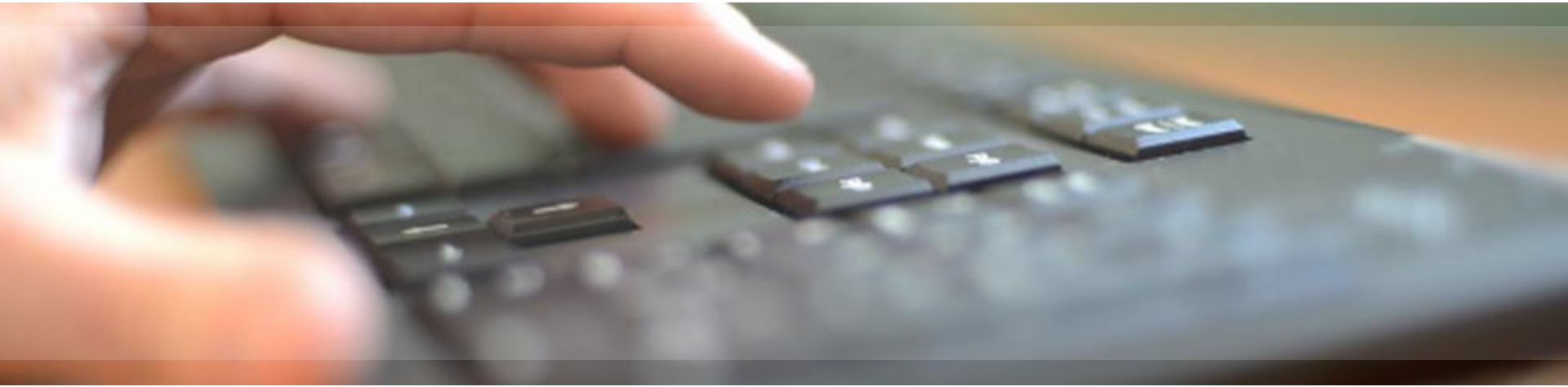
CyberSecurity: Cooperation as a way of defense

S21sec

REFLECTIONS - CONCLUSIONS

- The collaboration between police authorities and private companies working of these fields of knowledge is of outmost importance
- Multiple opportunities with distinct scopes and objectives
- Working with local, regional and european authorities
- Private sector = €€€, but...
  - There are **common interests** (internet security, fraud prevention, social engagement and compromise, etc)
  - **Other benefits** taken from this collaboration (reputation, visibility, internally positioning)
  - **Complementarity** with comercial activity
- There is the need to involve other entities from the privately held sector
  - Search for a common ground that motivates other to participate
  - Collaborative Social Responsibility (CSR) inclusion?

NOMBRE: Carlos Silva
ENTIDAD: S21sec
CONTACTO: csilva@s21sec.com



SPAIN

MADRID
C/ Valgrande, 6
C.P. 28108
Alcobendas
Tel.: +34 902 222 521
Fax: +34 91 6616679

BARCELONA
Passeig de Gracia,
56 - 4.D
C.P. 08007
Tel.: +34 902 222 521
Fax: +34 91 6616679

SAN SEBASTIÁN
P.E. Zuatzu.
Ed. Urgull, 2º
C.P. 20018
Tel.: +34 902 222 521
Fax: +34 91 6616679

PAMPLONA
PE. La Muga, 11-1
C.P. 31160
Orcoyen
Tel.: +34 902 222 521
Fax: +34 91 6616679

LEÓN
Avda. José Aguado, 41
Ed. INTECO
C.P. 24005
Tel.: +34 902 222 521
Fax: +34 91 6616679

PORTUGAL

LISBOA
Rua do Viriato, 13B,
4º andar
1050-233 Lisboa
Portugal
+351 220 107 120
+351 220 107 121

OPORTO
Lugar do Espido
-Via Norte
4470-177 Maia
Portugal
+351 220 107 120
+351 220 107 121

MEXICO

MÉXICO DF
Mariano Escobedo 510, planta alta
Colonia anzures
Delegación Miguel Hidalgo
11590 México D.F.
T +52 55 33 00 52 00

UK

READING
Davidson House
Forbury Square
Reading
RG1 3EU
United Kingdom

www.s21sec.com

THANKS