

Trials and Tribulations of Cybersecurity Information Sharing



Christian Popov

ASOC, Senior Analyst



kristiyan.popov@telelink.com



[@ChrisPSecc](https://twitter.com/ChrisPSecc)



6/10/2019



Agenda

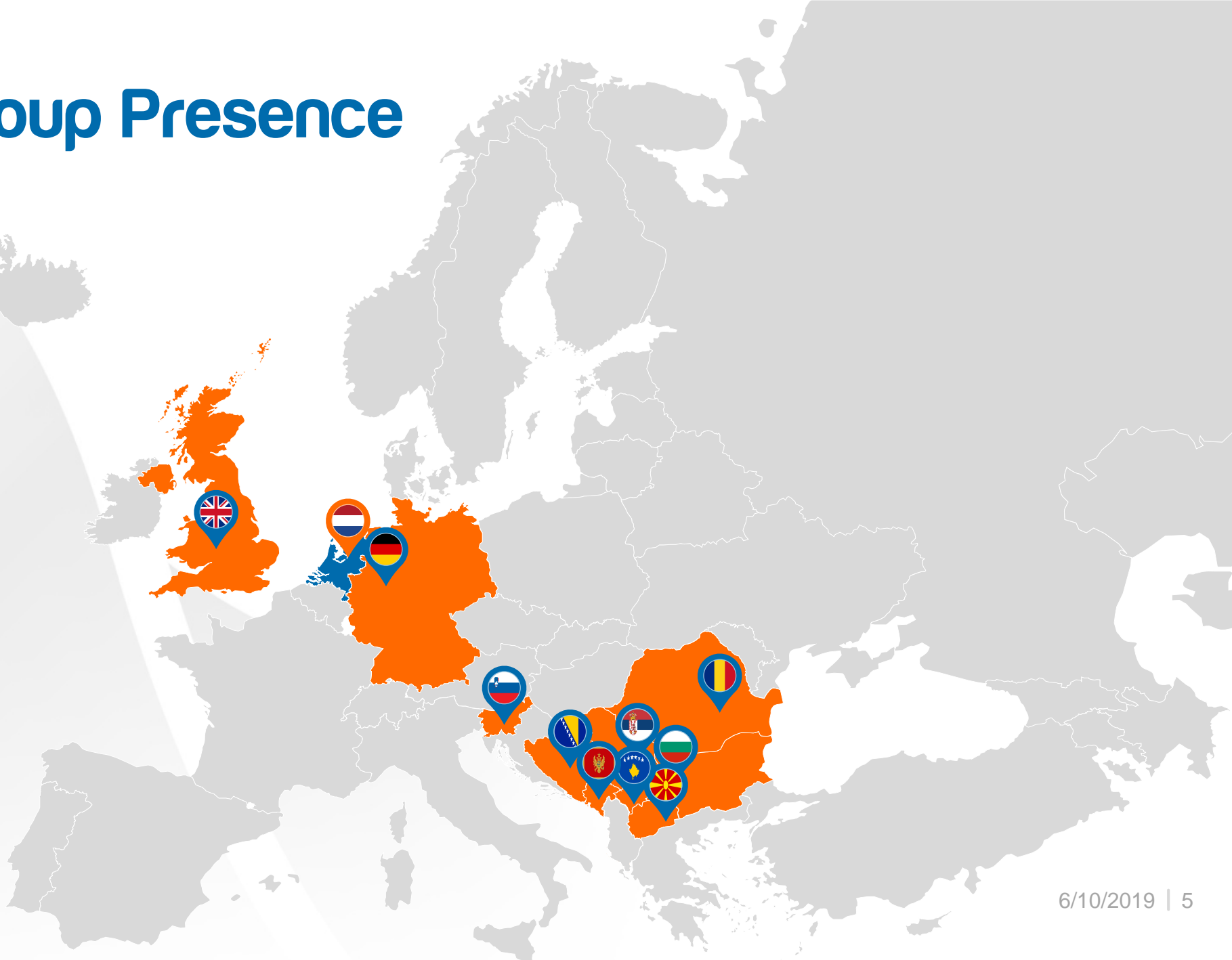
- The Information Age
- Cybersecurity Information Sharing
- Responsible Disclosure
- ASOC – Real Life Case Studies
- Telelink's ASOC and Information Sharing
- Conclusions

Telelink Group at a Glance

- **18 years of excellence**
- **Global network - presence in 10 countries**
- **Dedicated team of experts**
- **Partnerships with the leading global vendors**
- **€100M revenue in 2018, targeting over €100M in 2018**



Telelink Group Presence



Telelink Group Business Lines

Business Services



Engaging in business processes and customer needs in the field of IT infrastructure, information security, digital transformation, big data, and managed services

Infra Services



Engaging in delivering services for the construction and operation of communication infrastructure, delivery and integration of physical security systems, and building management systems

City Services



Engaging in developing and selling through partners Microsoft Azure based Smart City solutions

Labs



Engaging in research, development and training activities focusing on 5G networks and their application

TBS - Expertise and Services

Managed Services

-  Managed Enterprise Networks
-  Managed Security Services
-  Equipment as a Service
-  Data Protection Officer as a Service

Consulting Services

 Digital Transformation

 Cloud Enablement

 Governance, Risk, and Compliance

 Advisory Services

Digital Transformation

-  Data Management
-  Workplace Productivity
-  Transformation Strategies
-  Cloud Enablement
-  Business Intelligence and Analytics

Cloud Services

-  Microsoft Cloud Solutions
-  **Advanced Security Operations Center**

Information Security

-  Infrastructure and Endpoint Security
-  Securing Hybrid IT
-  Governance, Risk, and Compliance
-  Assessment and Response
-  Converged Security and Information Management




Support Services

-  Extended Warranty
-  Extended Support





Technical Services

-  Design Services
-  Deployment Services
-  App Development

Enterprise Networks

-  Wired and Wireless
-  Communication and Collaboration
-  Data Center Networking

Data Center

-  Automation and Orchestration
-  Computing and Storage
-  Business Continuity
-  Hybrid Data Center

Industry Partners



Microsoft
Partner



Gold Datacenter
Gold Cloud Platform
Silver Collaboration and Content
Silver Windows and Devices
Silver Cloud Productivity



Main Clients



CONTOURGLOBAL®



Lufthansa Technik
More mobility for the world



Progress®



ENERGO-PRO



Fibank
Първа инвестиционна банка



Medical University Plovdiv

ACIBADEM
CITYCLINIC



VP BRANDS
INTERNATIONAL



The Human Nature

“**Man is by nature a social animal**; an individual who is unsocial naturally and not accidentally is either beneath our notice or more than human.

Society is something that precedes the individual.

Anyone who either cannot lead the common life or is so self-sufficient as not to need to, and therefore does not partake of society, is either a beast or a god. ”

Aristotle



The Internet Nature

Big Data

Machine Learning

AI

Dark Blockchain

Information Sharing

Social Media



Cybersecurity Information Sharing



Cybersecurity Information Sharing

Analyst to
Analyst

Public
Disclosure

Analyst to
Enterprise

Enterprise to
Enterprise

Responsible
Disclosure

Analyst to Analyst

- Every day security researchers and analysts share information on trending topics in information security in order to help people better protect themselves from threats.
- Topics:
 - Indicators of compromise (IoCs)
 - New attack tactics (Tactics, Techniques, Procedures)
 - Defense tactics and detection (YARA rules, sigma rules, SIEM use cases)
 - Emerging threats
 - Security News
 - Experience and advice

**Do not share private/company information!
If you're not sure if you can share it publicly - don't!**

Analyst to Analyst

Catalin Cimpanu @campuscodi Following

Security researchers discover Linux version of Winnti malware

Winnti Linux variant used in 2015 in the hack of a Vietnamese gaming company.

[zdnet.com/article/securi ...](#)



9:17 PM - 19 May 2019

Florian Hansemann @HanseSecure Following

Lateral Movement Using internetexplorer.Application Object (COM)

#infosec #pwntest #redteam



Lateral Movement Using internetexplorer.Application Objec...
introduction Use Object COM (InternetExplorer.Application) For Execute using Types Exploit-internet Explorer For Execute ==> in Add On Internet Explorer For Get Execute Code using Lateral...
homjxi0e.wordpress.com

12:15 AM - 18 May 2019

Florian Roth @cyb3rops Following

With Sysmon logging & @markus_neis' Sigma rule you can detects non-standard programs connecting to RDP port 3389/tcp

e.g. malware exploiting #CVE20190708 to spread within a network

[github.com/Neo23x0/sigma/ ...](#)

Andreas Sfakianakis @asfakian Follow

MuddyWater Hacking Group Upgrades Arsenal to Avoid Detection



MuddyWater Hacking Group Upgrades Arsenal to Avoid Detection
The MuddyWater threat group has been updating its tactics, techniques, and procedures (TTPs) to include a number of new anti-detection techniques designed to bleepingcomputer.com

3:16 PM - 20 May 2019

1 Retweet 4 Likes

Jake Williams @MalwareJake Following

During an incident, you are hunting for snakes in the grass. If you've never hunted for snakes before, everything that rustles the grass looks like a snake. If you don't know what normal looks like, your job will be MUCH harder...

RedDrip Team @RedDrip7 Following


New approaches used by #OceanLotus #APT group, that leverage macro to load code hidden in the table by minimal white font and executes the downloaded payload through MSBUILD.exe. Either AES or RC4 is used for decryption.

url: hxxp://139.59.30.109:8090/abcv
virustotal.com/#/file/abb9798 ...

Public Disclosure

- Communicating the vulnerability to the public should have a broad impact to reach the awareness of the users, and it usually takes one of two possible paths.
 1. **Easy way** – publish blog post, share on cybersecurity forums and control the information
 2. **Hard way** – connect directly with a journalist from a responsible media, work together, but loose control over the information
- Handling the public disclosure comes with quite a bit of stress for the inexperienced as once the story starts rolling publicly you are not in control anymore.

Public Disclosure

 **Vulmon Vulnerability Feed**
@VulmonFeeds Following

CVE-2019-7038

Adobe Acrobat and Reader versions 2019.010.20069 and earlier, 2019.010.20069 and earlier, 2017.011.30113 and earlier version, and 2015.006.30464 and earlier have an out-of-bounds read vulnerability. S...

[vulmon.com/vulnerabilityd ...](https://vulmon.com/vulnerabilityd...)


11:24 PM - 26 May 2019

 **Exploit Database**
@ExploitDB Follow

[remote] Shopware - createInstanceFromNamedArguments PHP Object Instantiation Remote Code Execution (Metasploit)



9:04 AM - 26 May 2019

 **Sploitus**
@sploitus_com Follow

Mac OS X Feedback Assistant Race Condition

[sploitus.com/exploit?id=PAC ...](https://sploitus.com/exploit?id=PAC...)

#Exploit #Sploitus

5:25 PM - 22 May 2019

 **Vulmon Vulnerability Feed**
@VulmonFeeds Following

CVE-2019-7093

Creative Cloud Desktop Application (installer) versions 4.7.0.400 and earlier have an insecure library loading (dll hijacking) vulnerability. Successful exploitation could lead to privilege escalation...

[vulmon.com/vulnerabilityd ...](https://vulmon.com/vulnerabilityd...)

6:01 PM - 26 May 2019

 **Exploit Database**
@ExploitDB Follow

[webapps] Opencart 3.0.3.2 - 'extension/feed/google_base' Denial of Service PoC



9:04 AM - 26 May 2019

Analyst to Enterprise (disclose at your own risk...)

- Whenever an security researcher finds a security flaw he/she has a choice to make:
 1. Disclose/Notify the affected party
 2. Keep it a secret and potentially use the vulnerability
 3. Do nothing
- Most security researchers will opt to contact the company or vendor and notify them.
- However that is not always the case...

Analyst to Enterprise (Disclose at your own risk...)

Bad Packets Report
@bad_packets

WARNING
@Forbes Magazine subscription website (forbesmagazine.com) is infected with #magecart malware.

Exfil domain: fontsawesome[.]gq (🇷🇺)
@urlscanio results:
urlscan.io/result/8630561 ...
Deobfuscated code:
pastebin.com/3AR7wQ70



9:30 PM - 14 May 2019

Phishing Radar
@WhoPhishYou

Hi @waze, please investigate malicious and phishing websites that may target your customers immuniweb.com/radar/?id=PUfV ... #infosec #cybercrime

donald.waze.com Phishing Test
59 phishing websites target donald.waze.com and its customers.
immuniweb.com

MalwareHunterTeam
@malwrhunterteam

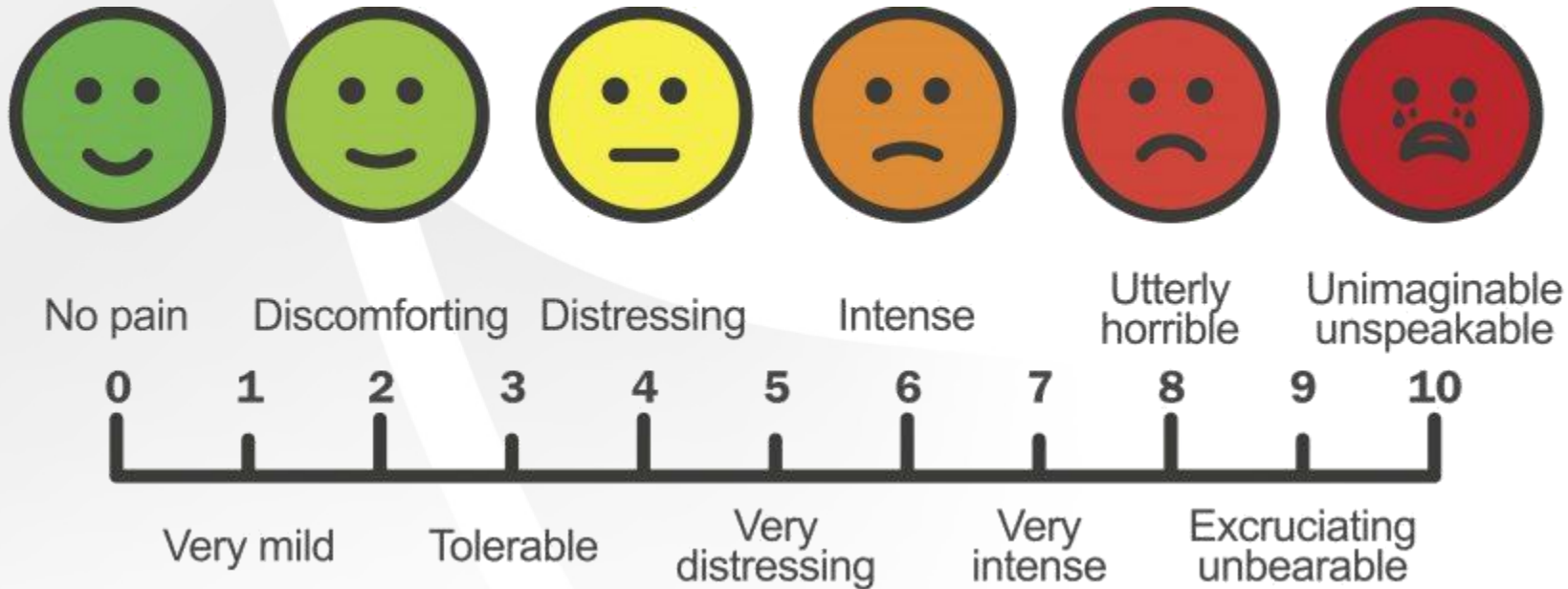
Hey @GranoSuomi, we just found one of your Project Managers got phished about 30-40 minutes ago.
Ask @JayTHL for the details as soon as you read this & maybe you will be able change pw before the actor logs in...
Also, don't forget to say thanks to MS for making this possible.

The Reactions

Thank you!!
You are the best!
We're sending
you all the \$\$\$!!

Whatever

Who are you??
How did you get this
information??
We are getting our
lawyers!



The Legal Action(s)

 **Ask Cybergibbons!**
@cybergibbons Following

The person who operates the site sent my employer a letter threatening legal action and claimed I had hacked their site.

 Muppets.



White hat banned for revealing vulns in news sites used by London ...
Vendor claims claims of vulns are tosh
theregister.co.uk

3:05 AM - 26 May 2019

 **donlobo**
@donlobo Follow

Indian Researcher Who Showed E-Voting Security Flaws Jailed, Denied Bail, Charged With Theft : <http://bit.ly/bvXP5z> #india #awful

10:00 AM - 27 Aug 2010

 **Jody**
@orwellsanimal Follow

ow.ly/1AMPKt Carrier IQ pursues legal action against security researcher who outlined keylogging rootkit in most smartphones

10:57 PM - 21 Nov 2011

 **Technical Muscle**
@TechnicalMuscle Follow

German software company has threatened legal action against a security researcher: German... <http://goo.gl/fb/N57O8>

12:04 AM - 30 Apr 2011

Cybersecurity Information Disclosure

Lawsuits threaten infosec research — just when we need it most

Security researchers and reporters have something in common: both hold the powerful accountable. But doing so has painted a target on their backs — and looming threats of legal action and lawsuits have many concerned.

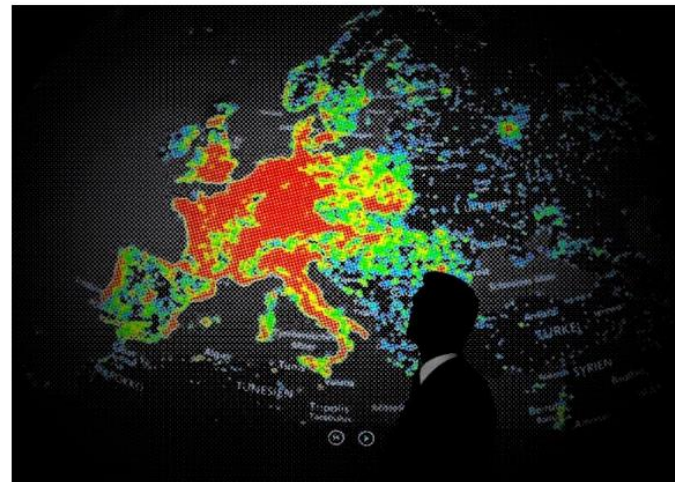
By Zack Whittaker for Zero Day | February 19, 2018 -- 13:00 GMT (13:00 GMT) | Topic: Security

Recommended Content:

White Papers: Futureproofing Your Startup with Cloud-Based Phone Systems

If you're starting a new business, you've likely been planning, saving and preparing for a while. But with limited startup funds, you've got to make the most of every investment dollar. That includes not only choosing the right technology from...

Download Now







NEW YORK, NY -- This year, two security reporters and one researcher will fight for their professional lives in court.

RECOMMENDED FOR YOU

Futureproofing Your Startup with Cloud-Based Phone Systems
White Papers provided by Vonage

DOWNLOAD NOW

MORE FROM ZACK WHITTAKER

-  Security: Online security 101: Tips for protecting your privacy from hackers and spies
-  Security: US government's "do not buy" list shuts out Russia, China
-  Security: New Spectre attack can remotely steal secrets, researchers say
-  Security: Flaw let researchers snoop on Swann smart security cameras

NEWSLETTERS

ZDNet Security

Your weekly update on security around the world

The Vulnerability Disclosure Process: Still Broken

Author:
Tom Spring

September 5, 2018
/ 1:03 pm

7 minute read

Skip to:

- The System is Broken
- Room for Things to Go Wrong
- Pen-Testing vs. Bounty Programs
- Safe Harbor
- Dark Markets
- IoT Offers Unique Challenges
- Stepping Off the Hamster Wheel

Share this article:



Despite the advent to bug bounty programs and enlightened vendors, researchers still complain of abuse, threats and lawsuits.

Responsible Disclosure Policy

Responsible Disclosure

At the Acme Corporation, we consider the security of our systems a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present.

If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. We would like to ask you to help us better protect our clients and our systems.

Please do the following:

- We will respond to your report within 3 business days with our evaluation of the report and an expected resolution date,
- If you have followed the instructions above, we will not take any legal action against you in regard to the report,
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission,
- We will keep you informed of the progress towards resolving the problem,
- In the public information concerning the problem reported, we will give your name as the discoverer of the problem (unless you desire otherwise), and
- As a token of our gratitude for your assistance, we offer a reward for every report of a security problem that was not yet known to us. The amount of the reward will be determined based on the severity of the leak and the quality of the report. The minimum reward will be a €50 gift certificate.

- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission,
- We will keep you informed of the progress towards resolving the problem,
- In the public information concerning the problem reported, we will give your name as the discoverer of the problem (unless you desire otherwise), and
- As a token of our gratitude for your assistance, we offer a reward for every report of a security problem that was not yet known to us. The amount of the reward will be determined based on the severity of the leak and the quality of the report. The minimum reward will be a €50 gift certificate.

We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate publication on the problem after it is resolved.

Enterprise to Enterprise

Following the various Responsible disclosure policies companies can still share the vulnerabilities found in their own or another company's product



Google Security Blog
The latest news and insights from Google on security and safety on the Internet

Disclosing vulnerabilities to protect users across platforms

March 7, 2019

Posted by Clement Lecigne, Threat Analysis Group

On Wednesday, February 27th, we reported two 0-day vulnerabilities – previously publicly-unknown vulnerabilities – one affecting Google Chrome and another in Microsoft Windows that were being exploited together.

To remediate the Chrome vulnerability (CVE-2019-5786), Google released an update for



UNIT 42 / UNIT 42 VULNERABILITY RESEARCH TEAM DISCOVERS 23 NEW VULNERABILITIES FEBRUARY 2019 DISCLOSURES – ADOBE AND MICROSOFT

Unit 42 Vulnerability Research Team Discovers 23 New Vulnerabilities February 2019 Disclosures – Adobe and Microsoft

By **John Harrison**
February 22, 2019 at 12:00 PM
Category: **Unit 42, Unit 42**
Tags: **adobe, microsoft, vulnerabilities, zero-day**

As part of Unit 42's ongoing threat research, we can now disclose that Palo Alto Networks Unit 42 threat researchers have discovered 23 new vulnerabilities addressed by the Adobe Product Security Incident Response Team (PSIRT) as part of their **February 2019 APSB19-07 security update release** and 2 vulnerabilities addressed by the **Microsoft Security Response Center (MSRC)** as part of their February 2019 security update release. Severity ratings ranged from Important to Critical for each of these vulnerabilities.

Responsible Disclosure



What Happens when a Vulnerability is Found?

- A security researcher will **privately** report the breach to the company and will allow the team a reasonable timeframe to fix the issue, but in the case they do not, they may publicize the exploit to alert the public.
- Disclosing a vulnerability to the **public** is known as full disclosure, and there are different reasons why a security researcher may go about this path.

Vulnerability Disclosure

A security researcher may disclose a vulnerability if:

- They are unable to get in contact with the company.
- Their vulnerability report was ignored (no reply or unhelpful response).
- Their vulnerability report was not fixed.
- They felt notifying the public would prompt a fix.
- They are afraid of legal prosecution.

Responsible Disclosure Examples



ASOC – Real Life Case Studies



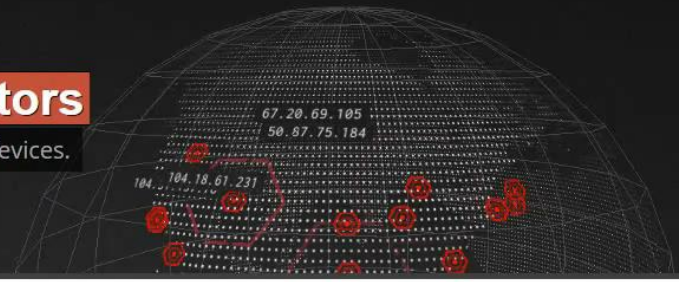


The search engine for Refrigerators

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account

Getting Started



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.



56% of Fortune 100



1,000+ Universities

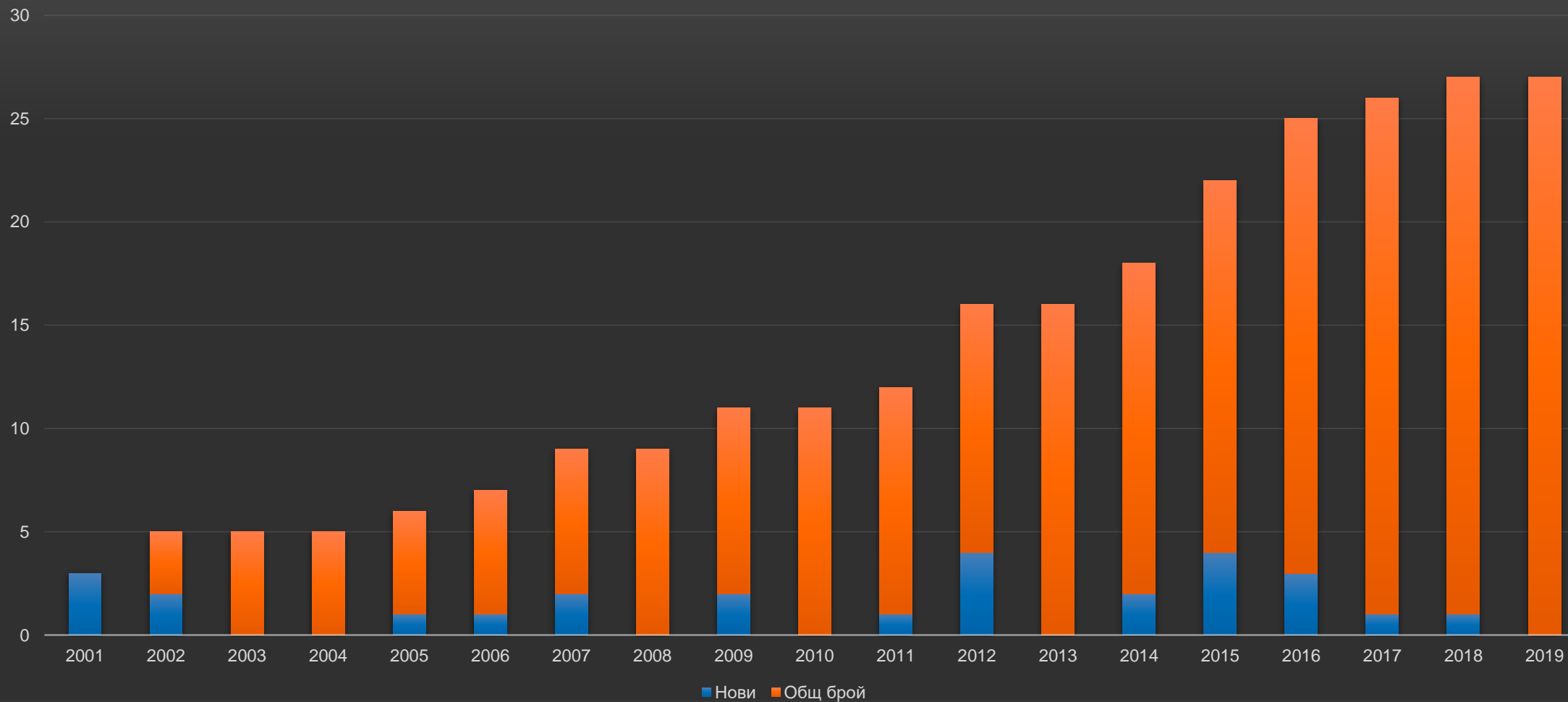
Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.



Analyze the Internet in Seconds

Shodan has servers located around the world that crawl the Internet 24/7 to provide the latest Internet intelligence. Who buys Smart TVs? Which countries are building the most wind farms? What companies are affected by Heartbleed? Shodan provides the tools to answer questions at the Internet-scale.

Microsoft RDP CVE



The Vulnerable SCADA System

Reply Reply All Forward IM



ср 12.9.2018 10:14

Alexander Tzokev

Контакти

Във връзка с проучване за потенциални уязвимости открихме такива на система на ваш клиент.

Искаме да се свържем с компанията, използваща посочения по-долу IP адрес и да ги информираме за проблемите, но нямаме контактна информация.

IP адресът е [REDACTED] и като доставчик е посочен "Vida optics TVV Ltd.".

Моля, да ни изпратите контакти или ако адресът не е към ваша AS да ни информирате.

Предварително ви благодаря.

Alexander Tzokev | Department Manager - ASOC
Telelink Business Services | alexander.tzokev@telelink.com
M: +359 879 676 712 | www.telelink.com



The Vulnerable SCADA System

Shodan.io search,
found IP
addresses and
analysis

Contacted ISP1
...
No answer

Contacted ISP2
...
No answer

...

Encountered Problems

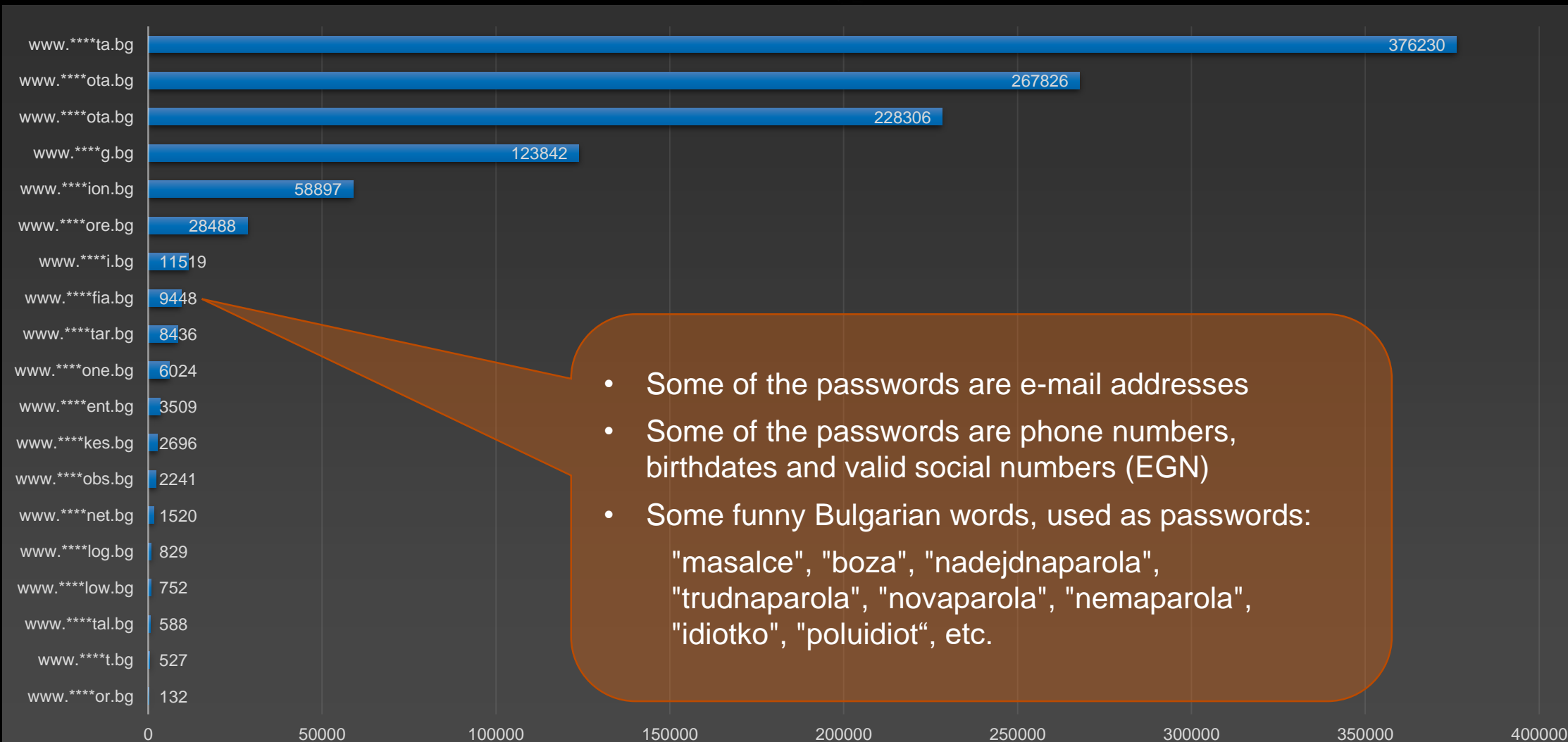
- Limited contact information
- No feedback

Collections #1-5

- 900+ GB archives, containing text files with leaked accounts (in most cases *email:password*)
- Passwords are in clear text and cryptographic hashes
- 6 000 000 000+ accounts
- 19 domains ending with “.bg” and containing “-bg” in the name were found



"THEY WERE WAY AHEAD OF US IN PASSWORDS."



Collections #2-5

Analysis of some of the Bulgarian sites

Collections #1-5

Searching for leaked password of colleagues and sending alerts to them

Alerting the affected sites and/or companies

Research and analysis of the leaked passwords

Encountered Problems

- Analyzing all the data
- Contacting Bulgarian companies and academical institution (owners of the leaked sites).
- Bipolar reactions were observed.

Lessons Learned

Contacting the cybersecurity targets (victims) is a complex task.



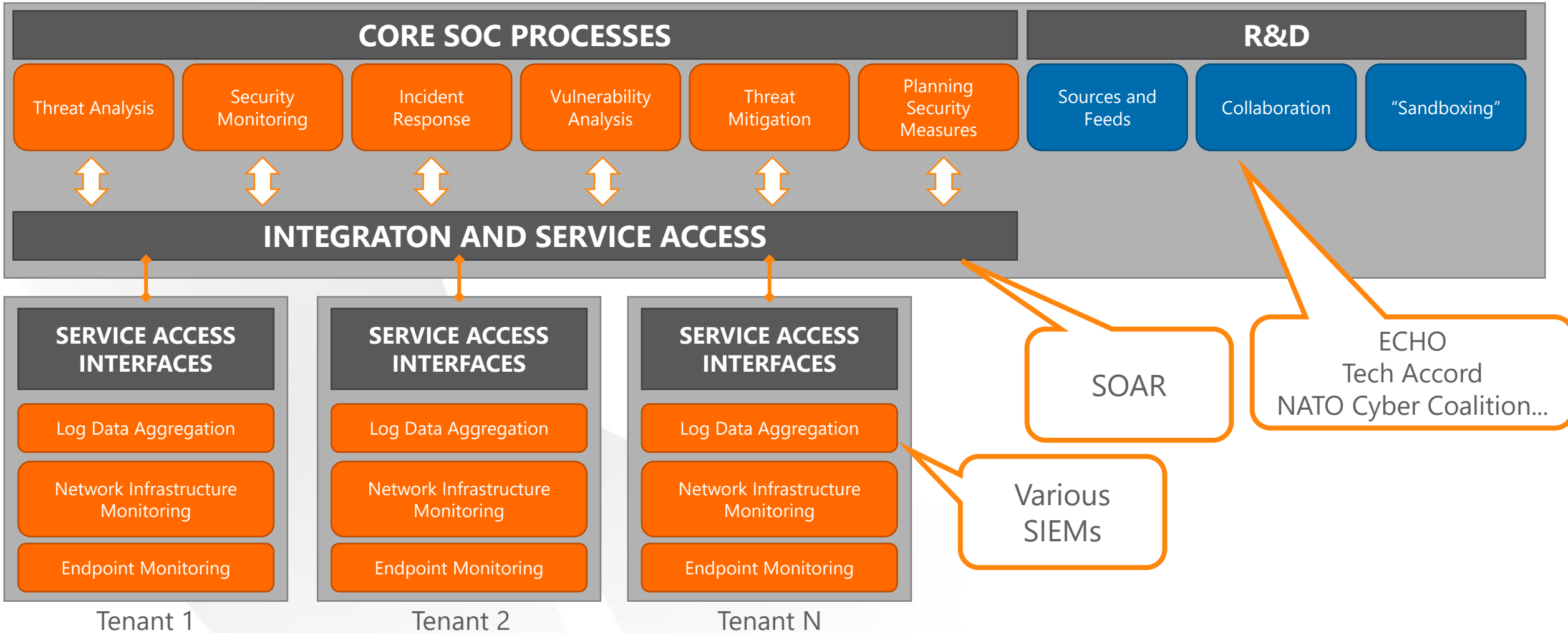
Telelink's ASOC and Information Sharing



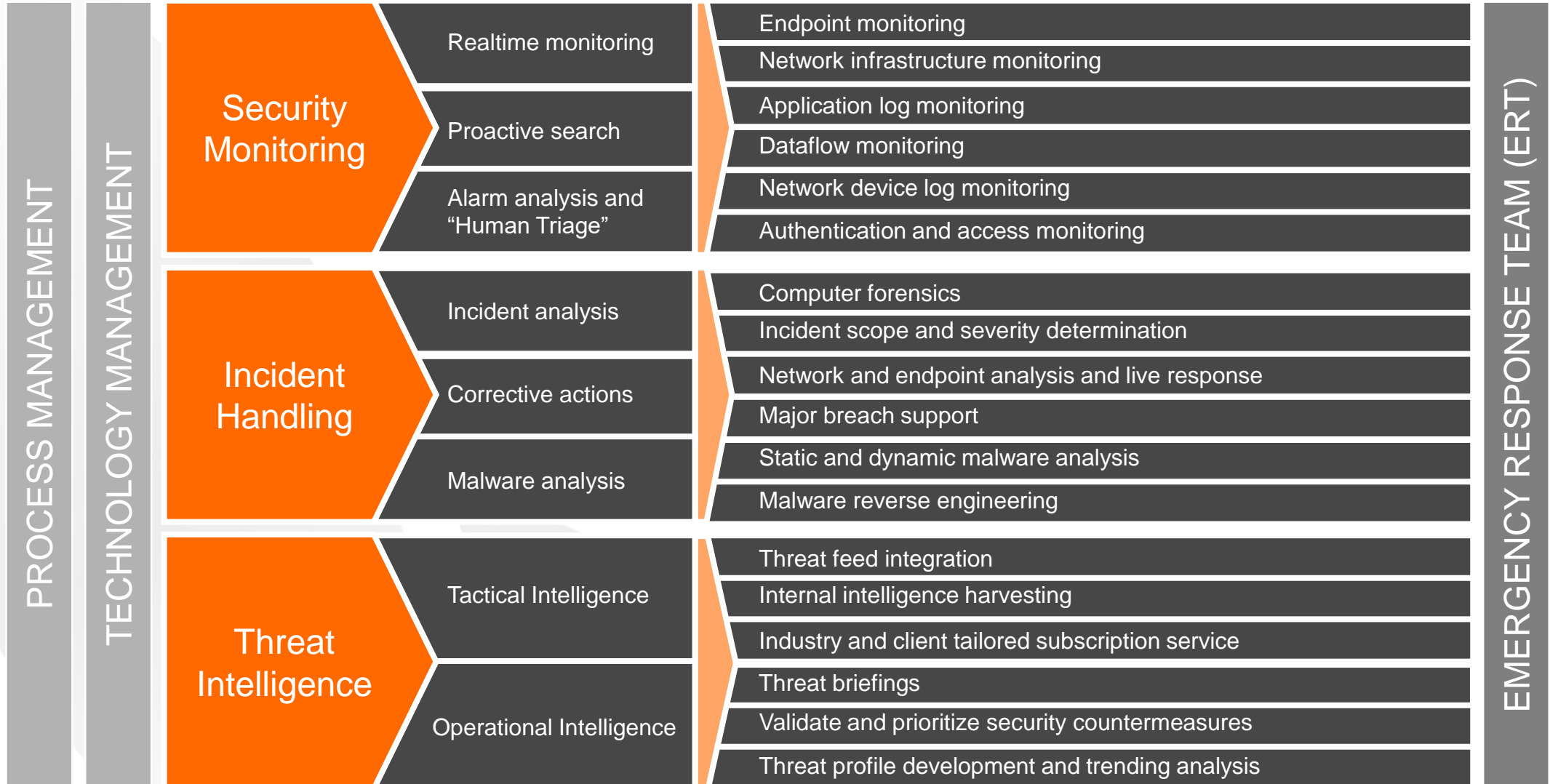
Telelink Holistic Approach to Cybersecurity



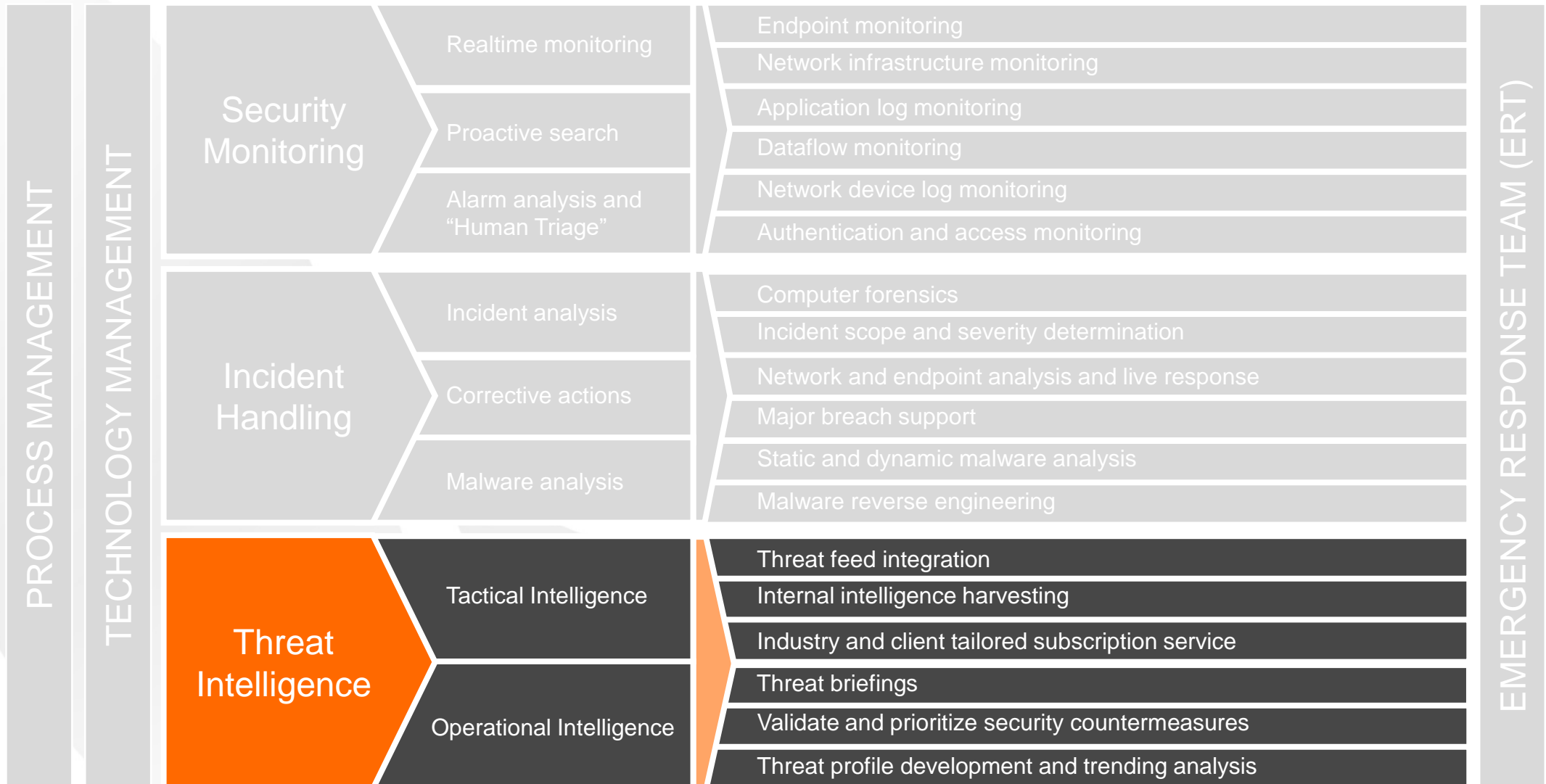
The ASOC Structure



ASOC

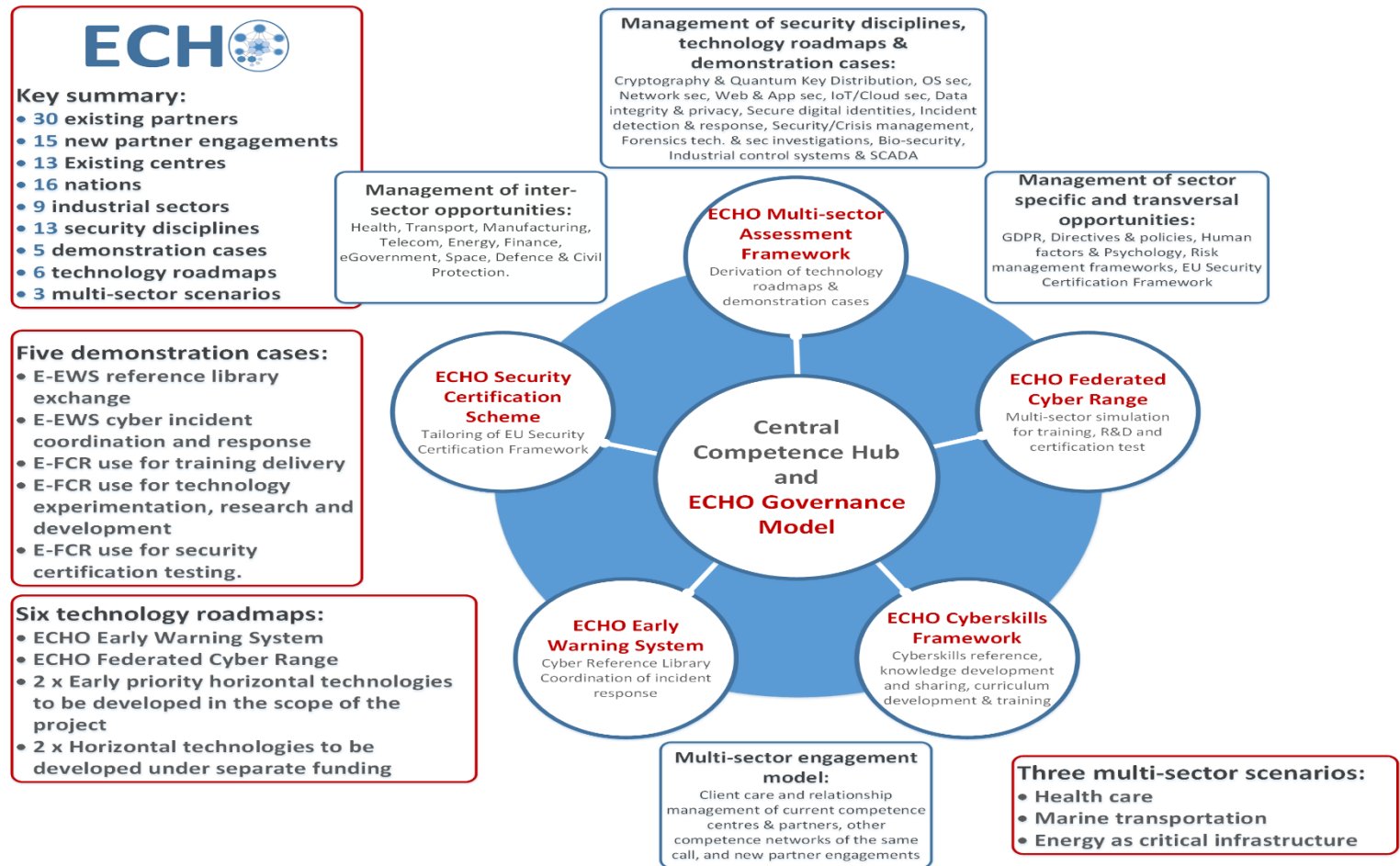


ASOC



ECHO - EUROPEAN NETWORK OF CYBERSECURITY CENTERS AND COMPETENCE HUB FOR INNOVATION AND OPERATIONS

- Research and Development project, funded by EU, Part of Horizon2020
- Consortia consisting of 30 partners, including Royal Military Academy of Belgium, RHEA systems, Universities, Ship builders, etc...
- 48 months, started in February 2019



ASOC Information Sharing

 **Alexander Tzokev**
February 9 · 🧑
<http://www.tzokev.com/malko-za-osint/>



 **Alexander Tzokev**
November 26, 2018 · 🧑
<http://www.tzokev.com/hackback/>




TZOKEV.COM
"Hackback" или "око за око, зъб за ..."
"I'm a fighter. I believe in the eye-for-an-eye business. I'm no cheek turner. I..."

 **Chris P**
@ChrisPSecc

Hello Mr. #Hawkeye 🧑 #Infostealer #Malware

Hash: 7cfab1e8dce36d0f4efd0311790abc79
Email subject: Orden de Recibo No 1042190A
Source IP: 41.190.31[dot]238
[virustotal.com/#/file/319d45f ...](http://virustotal.com/#/file/319d45f...)

5:50 AM - 15 May 2019

 **Chris P**
@ChrisPSecc

2019-04-29 03:14:04 34.73.232[dot]136 is pushing a #WordPress #phishing login page. IP belongs to @Google @googlecloud ?

pastebin.com/U6qJ6SJM

 **Iliya Dafchev**
@IliyaDafchev Following

An analysis of why the new evasion module fail to evade Windows Defender

[#metasploit](#) [#meterpreter](#) [#evasion](#)
[#defender](#) [#security](#) [#malware](#) [#hacking](#)

 **Beating Windows Defender. Analysis of Metasploit's new e...**
A research on why the new defender evasion modules fail to evade
idafchev.github.io

12:54 PM - 23 Jan 2019

 **Iliya Dafchev**
@IliyaDafchev Following

I contacted Microsoft and they fixed their detection logic, so this bypass shouldn't work anymore if you have the latest Defender AV definitions.

 **Office 365 AMSI Bypass (fixed)**
Microsoft fixed their detection logic, so this doesn't work anymore.
idafchev.github.io

3:59 AM - 24 Mar 2019



Conclusions



Conclusions

- Security information sharing is still maturing.
- There are still some gray areas and risks around disclosing vulnerabilities.
- Security researches should seek out proper channels for disclosing vulnerabilities and share information.
- Companies need to develop their own disclosure policies.
- **There is much to be gained from sharing information.**
- **Sharing is caring.**

 [@TBS_Infosec](https://twitter.com/TBS_Infosec)



Thank you for your attention!

