

HIGH LEVEL EVENT 2015



CYBER 7
SEVEN MESSAGES TO
THE EDGE OF CYBER-SPACE





EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY

SCIENCE AND TECHNOLOGY PARK OF CRETE (ITE)
VASSILIKA VOUTON, 700 13, HERAKLION, GREECE

PO BOX 1309, 710 01 HERAKLION, GREECE

TEL: +30 28 14 40 9710

hle@enisa.europa.eu | www.enisa.europa.eu

#HLE15eu

ATHENS OFFICE

1 VASS. SOFIAS & MEG. ALEXANDROU
MAROUSI 151 24, ATHENS, GREECE

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

© European Union Agency for Network and Information Security (ENISA), 2015

Reproduction is authorised provided the source is acknowledged.

CATALOGUE NUMBER: TP-04-15-745-EN-C

ISBN: 978-92-9204-133-5

DOI: 10.2824/850678



HIGH LEVEL EVENT 2015

CYBER 7

SEVEN MESSAGES TO
THE EDGE OF CYBER-SPACE





ABOUT ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

AUTHORS

Louis Marinos, ENISA.

CONTACT

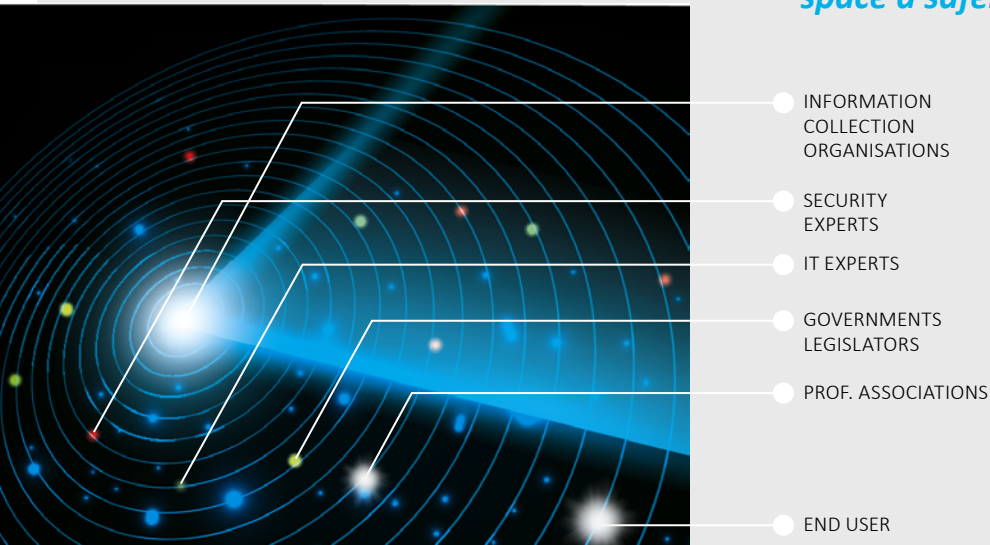
For media enquiries about this paper, please use press@enisa.europa.eu.

CONTENTS

Executive Summary	8
1 Creating CONTEXT means making more cyber-security sense	10
2 Intelligent SHARING of cyber threat intelligence	12
3 The issue with the STATISTICS and metrics	14
4 ATTACK METHODS become more mean and pervasive	16
5 CYBER THREAT AGENTS: the big unknown in the cyber-equation	18
6 The new field of cyber-abuse: INTERNET OF THINGS	20
7 DATA BREACHES: the debris of cyber-space	22

EXECUTIVE SUMMARY

“ We are facing a dire reality: Either we manage to disseminate our knowledge on cyber threats to the end users, or we will not be in the position to make cyber space a safer place.



For this, we will need to reach out to all relevant communities and stakeholders: security experts, IT engineers, professional users of information technology, politicians, legislators, consumer organisations, professional associations and end users – just to mention the most relevant/important ones.

But cyber security is like a solar system: the gravity centre is the knowledge maintained by organisations that collect and analyse cyber-security information. Around this centre we have security professionals, IT professionals, governments and organisations, and end users. The more we move away from the gravity centre, the less the technical details are relevant; and the less cyber-security knowledge is available. Yet, in order to maintain the solar system, we need to transmit portions of that knowledge to all entities up to the edge of the cyber universe, the end user. The knowledge flow is the gravity force keeping all entities together in the cyber-space.

Just as in our solar system, sending objects to remote destinations is a very laborious task: A remote location in the cyber universe can be reached by compact messages that have been sent out with high energy and efficiency. In doing so, we will need to invest efforts to simplify and consolidate our

message while departing from technical details and detail knowledge on cyber security and cyber threats. In other words: to make them more easily digestible by a wider community, for which technical details are irrelevant.

In this short report, we try to consolidate the findings from our work on the assessment of cyber threats in 2015 and make them end-user-ready. In order to reach our stakeholders with properly crafted messages, we have created 7 compact messages that correspond to conclusions from the analysis of this year's cyber threats, in particular:

- 1** CONTEXT is more relevant than the volume of information
- 2** SHARING is promising but does not yet work properly
- 3** cyber threat STATISTICS will need to be elaborated
- 4** cyber ATTACK METHODS become more pervasive
- 5** THREAT AGENTS need to be looked at more closely
- 6** INTERNET OF THINGS is here to stay, so is the cyber threat exposure that it represents
- 7** lessons from DATA BREACHES in 2015

It remains to see how long these messages will travel and how they will arrive to their final destination at the edge of cyber space in the most important recipient: THE END-USERS!

This short paper is based on the work of the ENISA Threat Landscape that is being conducted for the period of 2015. Previous versions of the ENISA Threat landscape can be found here¹. Though not pre-empting the upcoming ENISA Threat Landscape 2015, this report is a preview of important observations made in 2015 and target non-technical audience.

¹ https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape#b_start=0

1

CREATING CONTEXT MEANS MAKING MORE CYBER-SECURITY SENSE

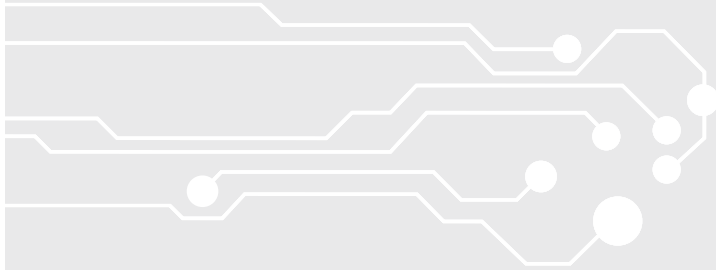
The processes behind incident management and collection of security information are very data intensive. They result in big amounts of data that are not easy to process, filter, analyse and interpret. Entities managing such information, are therefore forced to use tools but also manually process this information. The objective is to isolate information that is relevant to misuse, breaches, intrusions etc.

While individual incidents can be identified by using automated means, significant human intervention is necessary when trying to analyse and understand the whereabouts of an incident, e.g. tracing an incident from its origin to its final outcome. Equally laborious is to identify the consequences or lessons learned from an incident and accordingly adapt the defences. The total amount of information and knowledge collected during the processing and analysis of incidents is often referred to as “Cyber Threat Intelligence”. Many security experts speak about creation of “Cyber Intelligence” as the result of “End-to-End” analysis of cyber threats and their consequences.

Cyber threat intelligence is about creating knowledge and context out of security incident data. It allows for deriving qualitative information that spans the (short) lifetime of individual cyber security incidents. To this extent, cyber threat intelligence is considered as one of the most valuable assets in managing cyber security in the future.

Currently, we see a lot of vendors in cyber security developing products and offerings in the area of cyber threat intelligence. In such offerings, technical information has been already transformed to intelligence by adding the necessary context². Some of the offerings go as far as dynamically adjusting technical security systems (e.g. firewalls), based on collected threat intelligence.

² <http://go.recordedfuture.com/threat-identification-report>



Having said all that, the message we would like to convey is:

In cyber-security, it is important to create as much as possible long-living contextual information and knowledge on threats from the vast amount of short-living incident data. The acquired KNOWLEDGE and CONTEXT should be of high quality and be transferrable to all relevant players in the cyber space.

2

INTELLIGENT SHARING OF CYBER THREAT INTELLIGENCE

The advantages of information sharing are obvious: if one gains from experience of others, quick wins are more easily achieved. Since some years now, information sharing tops discussions within experts and wish lists of regulators. Technical solutions are already in place or are in final deployment phases. They cover exchange of technical information according to the type of operated technical systems (so called Indicators of Compromise – IoC).

This trend is also observed within sharing schemes involving humans. They are usually formed within sectors and/or groups of organisations with similar cyber-security interests. Albeit various sectoral sharing schemes have been already established, they are still in early maturity stages and members are about to establish the same language. The information exchanges are unstructured and ad hoc. Often it might be necessary to determine at which level of cyber threat intelligence the exchanges take place, i.e. information context, quality and quantity.

Analysis of relevant information in 2015³ showed some deficiencies in sharing technical information. Firstly, for some types of cyber threat intelligence, shared information is often not relevant for the entire sharing scheme, i.e. the overlap is too small. In order to recover from this deficiency, it seems that all sharing schemes should share all information with each other. This is an immense task that is practically unattainable.

Secondly, it seems that the spread of cyber-attacks is faster than the spread of coincidentally related cyber-threat intelligence. In other words, in order to achieve a deceleration of cyber-attacks spread, it is necessary to increase speed of information sharing. Obviously, even if sharing of technical information can be properly accelerated through the use of automated tools, increased speed in sharing contextual information is unequally difficult to achieve. Here, we need to achieve firstly a balanced level of cyber-threat capabilities, then a common understanding and finally increased levels of trust.

3 http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf



We believe that we are still at an early stage with regard to efficient sharing schemes. Therefore, the message we would like to convey is:

SHARING of cyber-threat intelligence will be more efficient if the context of shared information is known and if there is a balance of knowledge among the participating parties. There is a lot of work to be done to achieve this.

3

THE ISSUE WITH THE STATISTICS AND METRICS

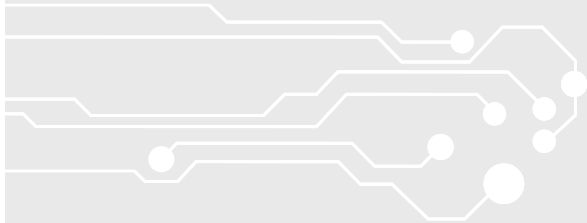
Being the science of information collection, analysis and interpretation, statistics are a fundamental tool for cyber threat analysis. Various statistic methods are being used within the cyber threat intelligence reports issued by vendors. Some of those use percentage based on a standardised number of devices (e.g. X% infection rate per 10.000 devices). Others present their result as percentages based on the entire base of similar objects (e.g. X% of entire malware are Trojans).

Besides the method to present quantities in the achieved results, there is a significant variety in the qualitative methods used. For example, vendors of end device protection services count the hostility of cyber space by the number of scanned attacks. Others, count encountered infections, online infections, or local infections. Others speak about data breaches or information leakages, that is, attacks with successful outcome. It is evident that it is a challenge to “normalize” such data under a common qualitative and quantitative denominator.

Finally, an intensively discussed issue is the system to measure the importance of incidents. Obviously the impact of an incident is an important element. But impact cannot be easily measured, as often the owners of the assets at stake are not willing to publicly speak about values. Hence, number of occurrence is being used as an alternative, together with other metrics such as recovery costs, recovery time, sectoral relevance, etc.

All the above-mentioned facts make comparability of findings very difficult if not impossible. An interesting approach published recently⁴, discusses a model for extrapolating cyber-threat statistics. It argues that in order to achieve comparability, it is necessary to assess the actual nature and size of the cyber-space. This, indeed, might be a promising approach allowing for a common basis for statistical analysis; and might produce surprising results about how secure the cyber-space really is.

⁴ https://www.cigionline.org/sites/default/files/no16_web_1.pdf



The message we would like to convey regarding statistical and measuring practices is:

The STATISTIC and METRICS models used in cyber-threat intelligence require elaboration. Otherwise the quality and comparability of the achieved results will remain questionable. This is an obstacle in the creation of usable, contextual cyber threat intelligence.

4

ATTACK METHODS BECOME MORE MEAN AND PERVERSIVE

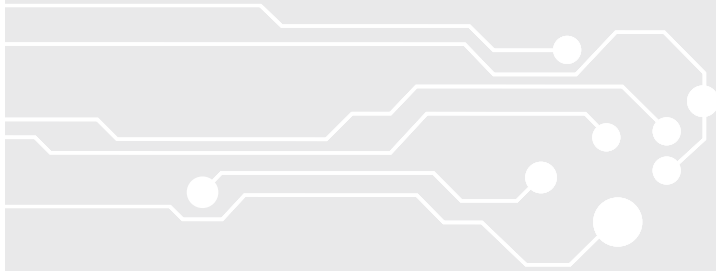
Like all humans, adversaries also go through a learning curve. After 20 years of cyber security attacks, there are significant achievements in cyber-attack methods and tactics. This seems quite natural, given the amount of resources invested in this area. Since cyber-attack capabilities belong to the arsenal of nation states, cyber-attacks have reached a new quality in striking power and stealthiness. The concern that the “cyber-weapons” and attack tactics of nation states might be copied by cyber-criminals is evident.

But threat agents in cyber space are also mean: which of the users would suspect an office document? Yet, in 2015 old style Visual Basic attacks, packaged within office documents have a revival. This is a ca. 20 years old method that has been relaunched and the success rates are an impressive demonstration of the efficiency of old attack methods. And this is quite natural, as almost no one in the user community today maintains memories about such old “low end” attacks. But in this way, the objective of getting victims by surprise has been achieved.

But also “high end” attacks have been encountered in 2015. A threat agent group called Equation Group⁵ has demonstrated how an attack can evade detection but also state-of-the-art protection measures, by installing malicious code in hardware components (i.e. Hard Disk Drives and Bios). Such malicious code would “survive” hard disc formatting and re- installation of the operating system. In other words, the infected computer might never recover from such an attack, making replacement the only secure recovery method.

This shows the range of sophistication of contemporary attacks. But there are also some good news: most of the attacks launched by cyber-criminals are “medium-tech”. This means that with average, baseline security controls in place, a large amount of the attacks can be defeated.

⁵ <http://www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage>



The message we would like to convey with regard to attack methods is:

Most of the attacks are based on low-end, low to medium-tech ATTACK METHODS. Keep calm, maintain long memory and implement baseline protection. If you are someone who might be targeted by cyber-espionage, you are at high risk.

5

CYBER THREAT AGENTS: THE BIG UNKNOWN IN THE CYBER-EQUATION

Unlike common crimes, criminal investigation in the cyber-space is a quite new area. Successes of law enforcement are rather scarce but very popular in the media. This is often due to the “hype” nature of cyber-crime, but also because they are not so common. And they are not common because it is not common or even not obvious for end-users to take legal actions against hackers.

The actual reason behind this fact is that cyber-crime is not yet being perceived by victims in the same way as common crime. Sometimes it is not even reported. In other words, the investigation chain from an incident, to the identification of the breach, to the performance of forensic analysis and to attribution, has gaps. Only relatively “big” criminal cases that harm the wealth of nations or large organisations are analysed and sentenced.

One can conclude that attribution in cyber-space is at initial maturity levels. Nonetheless, in the reporting period we have seen some cases where cyber-threat intelligence has been collected and has led to attribution⁶. And this is important in order to demonstrate the usage of this tool in attribution of cyber-criminals, albeit the fact that the method may still require high capabilities and costs that often are not available in medium sized organisation and law enforcement agencies.

⁶ http://cdn2.hubspot.net/hubfs/454298/Project_CAMERASHY_ThreatConnect_Copyright_2015.pdf?t=1443030820943&submissionGuid=7a5a9a18-f0a9-4bd8-8b0c-3e7d86d9baae

⁷ https://www.f-secure.com/documents/996508/1030743/Threat_Report_H2_2014



Prominent security experts have already identified and formulated the need for (better) attribution of cyber-crime⁷. Irrespectively whether organizations are in the position to perform this task on their own or not, we can just underline this and repeat our message that:

Efforts to increase attribution rates of CYBER THREAT AGENTS are necessary. This will lead primarily to sentence already performed criminal activities, but it will also achieve precedent and increase the knowledge about who is the enemy.

6

THE NEW FIELD OF CYBER-ABUSE: INTERNET OF THINGS



At the beginning there was some abuse of smart TVs, later we have seen refrigerator botnets. Within three years, the abuse of Internet of Things (IoT) infrastructures has become mainstream business for cyber-criminals. In the reporting period we have seen massive abuse of home appliances within Denial of Service attacks. In 2015 the FBI has issued an alert for users of IoT devices⁸. IoT is an impressive demonstration of speed in identifying and opening up new areas of (malicious) opportunity. It also demonstrates how important it is to have security by design, or – on the opposite -how costly it is to add ex-post security to an ecosystem.

Abusing available functions of IoT components is not the worst misuse scenario in IoT environments: information leakage and the materialization of privacy risks in these ecosystems may lead even to threatening of human life. Together with data mined from social networking information, IoT data may be misused to craft the perfect spear phishing attacks.

Let alone the potential value of massive consumer data on their life-style, such as: daily routines, eating habits, cultural preferences, health status, etc.

⁸ <http://www.ic3.gov/media/2015/150910.aspx>



Given the level of security in IoT, the knowledge level of end-users, the yet unknown attack scenarios and the inexistence of contextual information about IoT incidents, it becomes evident that cyber-threats to IoT are here to stay.

The INTERNET OF THINGS is at the edge of the cyber-space. As such, cyber-security must be embedded and ready-to-use without any technical knowledge. In order to achieve this, a bigger cooperation between producers and operators of technical systems, but also society and service providers will be necessary.

7

DATA BREACHES: THE DEBRIS OF CYBER-SPACE

The scrapyard of the cyber-space consists of data breached through cyber-security incidents. They are the cyber-debris from damages that have found place due to successful incidents. Certainly, the known data breaches are not the only ones that took place. It is assumed that the real number of data breaches is much higher than the ones reported.

Though always unfortunate for businesses and end-users, incidents are very important in cyber-security. Their analysis goes up to the identification of their root causes and – when possible – to the final attribution. Hence, from existing incidents numerous lessons are learned and conclusions are drawn. This knowledge/intelligence helps security professionals in the development of better protection. For this reason, legislators consider making security incident reporting mandatory, at least for incidents above a certain impact threshold. ENISA plays already a role in incident reporting in the Telecommunication sector⁹.

Evidence in 2015 has indicated that the speed of breach discovery is much lower than the speed to compromise a system¹⁰. Moreover, discussions about impact thresholds for incident reporting will need to take place, together with acceptable models for the calculation of data breach monetization. Together with a “normalization” of data breach statistics, such measures will allow for the homogenization of data breach information. Data breach information and lessons learned will need to put as quickly as possible to the disposal of experts in order to increase reaction/discovery time.

⁹ https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2014/at_download/fullReport

¹⁰ http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf



The message we would like to convey regarding data breaches is:

Lessons learned from DATA BREACHES are one of the most valuable resources for cyber intelligence. Lessons learned need to be made available for all relevant stakeholders at the highest speed possible. The form of this information need to be such, that it can be immediately translated to corrective actions.



CATALOGUE NUMBER: TP-04-15-745-EN-C
ISBN: 978-92-9204-133-5
DOI: 10.2824/850678

