EN

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

From January 2019 to April 2020

Sectoral/ thematic threat analysis

ENISA Threat Landscape

Overview

Apart from indicating adversaries' motivations, it provides evidence about the most common attack techniques and threat exposure applying to a particular sector, thus indicate protection requirements and priorities. With respect to themes, the analysis of threats and challenges associated with specific emerging technologies contributes to the process of assessing, evaluating and mitigating future risks.

Contextualised cyber threat intelligence (CTI) for sectors is an important preparedness tool for drawing conclusions on expected cyberattacks within a specific sector.

_Sector incident statistics vs. assessed exposure of emerging sectors

Contextualisation of sectoral CTI is mainly based on cybersecurity incidents encountered in a sector. Although this is a standard method for existing and established IT components and digital services, it does not cover emerging technologies. This is mainly because no incident information exists for technologies that are only at a pilot or experimental phase. CTI for emerging technologies is contextualised through threat assessments of asset categories pertinent to a specific sector. ENISA performs such assessments for emerging sectors such as 5G, IoT[5] and smart cars[6]. Sectorial and thematic threat landscapes and assessments of baseline protection are the methods used by ENISA to contextualise CTI.

In this report, besides sectorial CTI relying on incident-based statistics, we present a summary of assessed CTI for emerging technology sectors based on ENISA work.


“During the next decade, cybersecurity risks will become harder to assess and interpret due to the growing complexity of the threat landscape, adversarial ecosystem and expansion of the attack surface.”
in ETL 2020

Overview

The urgent need for accurate and up-to-date sectoral incident statistics

Sectoral incident statistics are an essential tool to understand the dynamics of threat evolution, adversaries' motives, exposure of assets, and actions on objectives. Because of the complexity of attacks, dependencies among the assets targeted and the cross-sector nature of the abused vulnerabilities exploited, incidents statistics have some inherent uncertainties that emanate from the following facts.

- In various sector statistics, we see a number of **incidents classified as 'unknown'**[1,2]. This percentage varies from 1,5% to 5%. If these incidents could be associated with some of the known sectors, this percentage could influence the order of targets. Moreover, the significant amount of unknown attack techniques (approximately 15%), add some uncertainty to the assessment of threat agents' motives.
- Most **attacks take more than one-step** (average three) to reach their objectives of the final target. In many cases, multiple targets from various sectors are involved in a single attack. Hence, an incident recorded within a sector may result from several incidents in other sectors that are intermediate steps in the attack. Such dependencies among incidents may affect the accuracy of incident statistics.
- Apart from the number of incidents per sector, an important element for the statistical analysis is the **nature of attack techniques used**. This information may provide useful evidence about the most frequently used attack vector and can help contribute to prioritise necessary protective measures necessary for a particular sector.

- The materialization of threats depends heavily on existing **opportunities that are explored by adversaries**. Because of the COVID-19 pandemic, for example, IT environments have become decentralized. This weakens the corporate security controls applied within a company's network, which explains the shift in attacks from corporate targets to individual targets.[1] This example is indicative of the need to 'translate' observed changes in statistics in the light of emerging opportunities.
- Current statistics are developed with various criteria in mind. **Variations in the criteria** of statistics impede comparisons between incident statistics. For example:
    - Depending on the information collector's stakeholders/contributors data base of the data about statistic may not cover all sectors evenly;
    - Classification of incidents may be based on their frequency of occurrence, irrespectively of the magnitude of the damage (e.g. size of breached information) or its impact.
- An essential element of sectoral statistics is the **frequency of occurrence** of individual cyberthreats. This gives an impression of the most common attack method used in a sector. Such statistics may provide guidance on the required level of preparedness or maturity of individual security controls that reduce exposure to the relevant cyber threats.
- Given the above facts pertinent to incident statistics, this report provides an approximate ranking of sectors in terms of observed incidents, together with a trend drawn from the emerging dynamics of the potential exposure of each sector. Moreover, some information on the most popular attack vectors per sector is also given. For this purpose, information from various publications has been consolidated.[1,2,3,4]

Trends in incidents

SECTOR	MOST POPULAR THREATS/ATTACKS	INCIDENTS TRENDS
Individual	• Phishing • Malware • Information leakage • Data theft	→ Stable
Multiple industries	• Web application attacks • Phishing • Malware	↑ Increasing
Public Administration, Defence, Social Services	• Malware • Phishing • Web based attack	→ Stable slightly decreasing
Financial/Banking/ Insurance	• Web application attacks • Insider threat (unintentional abuse) • Malware • Data theft	→ Stable
Health/Medical	• Malware • Insider threat (unintentional abuse/error) • Web application attacks	↑ Increasing
Education	• Malware • Ransomware • Web based attacks	→ Stable slightly decreasing
Information and Communication	• Web application attacks • Insider threat (unintentional abuse/error) • Malware	→ Stable
Professional/Digital Services	• Web application attack • Insider threat (unintentional abuse/error) • Malware	→ Stable
Arts, Entertainment and gaming[8]	• Web application attacks • Malware • Phishing	→ Stable
Manufacturing	• Malware • Web application attacks • Insider threat (unintentional abuse/error)	→ Stable

SECTOR	INFLUENCING FACTORS
Individual	Self-isolation due to COVID-19 lockdown measures has led to dispersed/ decentralized IT environments and isolation of users who are easier to fool and have fewer security controls in place, than was the case in centralized environments.
Multiple industries	Remote users due to COVID-19 lockdown measures have facilitated attacks via phishing and leakage of sensitive information (i.e. credentials).
Public Administration, Defence, Social Services	Use of cloud services may have influenced the security of public offerings. Nonetheless, social services have received significant amount of attacks due to financial aids offered to citizens during COVID-19 pandemic.
Financial/ Banking/ Insurance	The complexity of the financial sector makes it hard to interpret the threat landscape, as different domains within financial services and banking may face entirely different cyber risks and threats.
Health/Medical	The attention paid by cybercriminals to health targets has increased considerable due to financial motives and the importance of the sector during COVID-19 pandemic.
Education	Although stable, this sector has been targeted in 2020 by cyberespionage campaigns due to interest in COVID-19 research results.
Information and Communication	This sector is constantly under pressure due to the difficulties in protecting a huge attack surface, introduced by digital media platforms. For online media organizations, attacks that cause reputational damage are one of the biggest threats.
Professional/ Digital Services	Although stable, this sector has been targeted in 2020 by various campaigns in an attempt to leak information from users of digital services teleworking from home during COVID-19 pandemic.
Arts, Entertainment and gaming	The change from a licensed to subscription business model adopted by the gaming industry made this sector more attractive to cyber criminals.[8]
Manufacturing	Supply chain attacks and attacks to industrial control systems are the main threat to manufacturing companies since these are able to shut down a complete production line. The theft of intellectual property data is another serious threat to this sector.

Threats on emerging technologies

Next generation of mobile communications or 5G

RELATED COMPONENTS – ASSET GROUPS	THREAT EXPOSURE
Core Network	Abuse from remote access, Authentication traffic spikes, Abuse of user authentication/authorization data, Abuse of third party hosted network functions, Abuse of lawful interception function, Application programming interface (API) exploitation, Exploitation of poorly designed architecture and planning, Exploitation of misconfigured or poorly configured systems/networks, Erroneous use or administration of the network, systems and devices, Fraud scenarios related to roaming interconnections, Lateral movement, Memory scraping, Manipulation of network traffic, network reconnaissance and information gathering, Manipulation of network configuration data, Malicious flooding of core network components, Malicious diversion of traffic, Manipulation of the network resources orchestrator, Misuse of audit tools, Opportunistic and fraudulent usages of shared resources, Registration of malicious network functions, Traffic sniffing, Side-channel attacks
Access Network	Abuse of spectrum resources, Address Resolution Protocol (ARP) poisoning, Fake access network node, Flooding attack, IMSI catching attacks, Jamming the radio frequency, MAC spoofing, Manipulation of access network configuration data, Radio interference, Radio traffic manipulation, Session hijacking, Signalling fraud, Signalling storms

RELATED COMPONENTS – ASSET GROUPS	THREAT EXPOSURE
Multi Edge Computing	False or rogue MEC gateway, Edge node overload, Abuse of edge open application programming interfaces (APIs)
Virtualisation of Network Functions and Software Defined Networks	Abuse on Data Centres Interconnect (DCI) protocol, Abuse of cloud computational resources, Network virtualisation bypassing, Virtualised host abuse
Physical Infrastructure	Manipulation of hardware equipment, Natural disasters affecting the network infrastructure, Physical sabotage/vandalism of the network infrastructure, Threat from third parties' personnel accessing MNO's facilities, Universal Integrated Circuit Card (UICC) format exploitation, User equipment compromising
All above 5G asset groups	Denial of Service (DoS), Data breach, leak, theft destruction and manipulation of information, Eavesdropping, Exploitation of software and hardware vulnerabilities, Malicious code or software, Compromised supply chain, vendor and service providers, Targeted threats/attacks, Exploiting flaws in security, management and operational procedures, Abuse of authentication, Identity theft or spoofing

Threats on emerging technologies

Internet-of-things (IoT)

RELATED COMPONENTS – ASSET GROUPS	THREAT EXPOSURE
Human factor	Insider threat, Teamwork issues, Internal limitations, Hacktivism, Loss of support services, Utility outage, Network outage, Unintentional modifications, Sabotage, Violation of rules and regulations, Breach of legislation, Contract Requirements, Failure to meet contractual requirements (e.g. software maintenance), Software exploitation, Social engineering, Identity theft.
Software design	Insider threat, Hacktivism, Unintentional modifications, Erroneous use or administration of devices and systems, Sabotage, SDLC process failures, Third party failures, Failure to meet contractual requirements (e.g. software maintenance), Software exploitation, Loss/leakage of information.
Software development	Insider threat, Hacktivism, Loss of support services, Unintentional modifications, Erroneous use or administration of devices and systems, Sabotage, Vandalism and theft, Software vulnerabilities, SDLC process failures, Maintenance failures, Abuse of authorisation, Software exploitation, Manipulation of SDLC infrastructure, Loss/leakage of information.
Software deployment	Insider threat, Hacktivism, Loss of support services, Unintentional modifications, Erroneous use or administration of devices and systems, Sabotage, Vandalism and theft, Software vulnerabilities, SDLC process failures, Third party failures, Abuse of authorisation, Software exploitation, Manipulation of SDLC infrastructure, Denial of Service, Manipulation of information, Disclosure, Loss/leakage of information.

RELATED COMPONENTS – ASSET GROUPS	THREAT EXPOSURE
Data	Insider threat, Hacktivism, Loss of support services, Unintentional modifications, Erroneous use or administration of devices and systems, Sabotage, Vandalism and theft, Software vulnerabilities, SDLC process failures, Third party failures, Abuse of authorisation, Software exploitation, Manipulation of SDLC infrastructure, Denial of Service, Manipulation of information, Disclosure, Loss/leakage of information.
Maintenance	Insider threat, Hacktivism, Utility outage, Network outage, Unintentional modifications, Erroneous use or administration of devices and systems, Damage caused by a 3rd party, Sabotage, Vandalism and theft, Attacks with physical access, Forced Access, Contract Requirements, Software vulnerabilities, SDLC process failures, Third party failures, Failure to meet contractual requirements (e.g. software maintenance), Maintenance failures, Abuse of authorisation, Software exploitation, Manipulation of SDLC infrastructure, Denial of Service, Manipulation of information, Disclosure, Loss/leakage of information
Software components	Insider threat, Hacktivism, Loss of support services, Unintentional modifications, Erroneous use or administration of devices and systems, Damage caused by a 3rd party, Information leakage, Sabotage, Vandalism and theft, Attacks with physical access, Forced Access, Contract Requirements, Software vulnerabilities, SDLC process failures, Third party failures, Failure to meet contractual requirements (e.g. software maintenance), Maintenance failures, Abuse of authorisation, Software exploitation, Manipulation of SDLC infrastructure, Denial of Service, Manipulation of information, Disclosure, Loss/leakage of information

Threats on emerging technologies

Smart cars

RELATED COMPONENTS – ASSET GROUPS	THREAT EXPOSURE
Car sensors and actuators	Denial of Service,Malware, Manipulation of Information, OEM targeted attacks, Unauthorised activities, Identity theft, Abuse of authorisations, Manipulation of information, , Threats targeting autonomous sensors, Threats against AI and ML, Sabotage, Vandalism, Theft, Side-channel attacks, Fault injection, Theft, Failure or malfunction of a sensor/actuator, Software vulnerabilities exploitation, Communication protocol hijacking, Man-in-the-middle attack / Session hijacking, Unintentional change of data or car components configuration, Using information and/or devices from an unreliable source, Erroneous use of configuration of car components, Network outage, Failure to meet contractual requirements, Violation of rules and regulation/Breach of legislation/Abuse of personal data.
Decision Making Algorithms **Car ECUs, processing and decision making components** **Smart cars Infrastructure and Backend systems**	Denial of Service, Malware, Manipulation of Information, OEM targeted attacks, Unauthorised activities, Identity theft, Abuse of authorisations, , Manipulation of information, Threats against AI and ML, Sabotage, Vandalism, Theft, Theft, Failure or malfunction of a sensor/actuator, Software vulnerabilities exploitation, Failure or disruption of service, Communication protocol hijacking, Data replay, Man-in-the-middle attack / Session hijacking, Unintentional change of data or car components configuration, Using information and/or devices from an unreliable source, Erroneous use of configuration of car components, Loss of GNSS signal, Network outage, Failure to meet contractual requirements, Violation of rules and regulation/Breach of legislation/Abuse of personal data

RELATED COMPONENTS – ASSET GROUPS	THREAT EXPOSURE
Vehicle Functions **Car sensors and actuators** **Car ECUs, processing and decision making components**	Denial of Service, Malware, Manipulation of Information, OEM targeted attacks, Unauthorised activities, Identity theft, Abuse of authorisations, Manipulation of information, Threats targeting autonomous sensors, Threats against AI and ML, Sabotage, Side-channel attacks, Fault injection, Theft, Failure or malfunction of a sensor/actuator, Software vulnerabilities exploitation, Failure or disruption of service, Communication protocol hijacking, Data replay, Man-in-the-middle attack / Session hijacking, Unintentional change of data or car components configuration, Using information and/or devices from an unreliable source, Erroneous use of configuration of car components, Car depleted battery, Network outage, Failure to meet contractual requirements, Violation of rules and regulation/Breach of legislation/Abuse of personal data
Software management **Car ECUs, processing and decision making components** **In-vehicle communication components**	Denial of Service, Malware, Manipulation of Information, OEM targeted attacks, Unauthorised activities, Identity theft, Abuse of authorisations, Sabotage, Side-channel attacks, Fault injection, Theft, Failure or malfunction of a sensor/actuator, Software vulnerabilities exploitation, Failure or disruption of service, Communication protocol hijacking, Man-in-the-middle attack / Session hijacking, Unintentional change of data or car components configuration, Using information and/or devices from an unreliable source, Network outage, Failure to meet contractual requirements, Violation of rules and regulation/Breach of legislation/Abuse of personal data
Inside vehicle Communication Components	Denial of Service, Malware, Manipulation of Information, OEM targeted attacks, Unauthorised activities, Identity theft, Abuse of authorisations, Manipulation of information, Sabotage, Side-channel attacks, Fault injection, Theft, Failure or malfunction of a sensor/actuator, Software vulnerabilities exploitation, Communication protocol hijacking, Data replay, Man-in-the-middle attack / Session hijacking, Unintentional change of data or car components configuration, Using information and/or devices from an unreliable source, Erroneous use of configuration of car components, Network outage, Failure to meet contractual requirements, Violation of rules and regulation/Breach of legislation/Abuse of personal data

Threats on emerging technologies

Smart cars

RELATED COMPONENTS – ASSET GROUPS	THREAT EXPOSURE
Communication Networks and Protocols. **Car ECUs, processing and decision making components** **In-vehicle communication components**	Denial of Service, Malware, Manipulation of Information, OEM targeted attacks, Unauthorised activities, Identity theft, Abuse of authorisations, Sabotage, Theft, Failure or malfunction of a sensor/actuator, Software vulnerabilities exploitation, Communication protocol hijacking, Data replay, Man-in-the-middle attack / Session hijacking, Unintentional change of data or car components configuration, Using information and/or devices from an unreliable source, Erroneous use of configuration of car components, Network outage, Failure to meet contractual requirements, Violation of rules and regulation/Breach of legislation/Abuse of personal data.
Nearby External Components **Smart cars Infrastructure and Backend systems**	Denial of Service, Malware, Manipulation of Information, OEM targeted attacks, Unauthorised activities, Identity theft, Abuse of authorisations, Manipulation of information, Sabotage, Vandalism, Theft, Software vulnerabilities exploitation, Failure or disruption of service, Communication protocol hijacking, Man-in-the-middle attack / Session hijacking, Unintentional change of data or car components configuration, Using information and/or devices from an unreliable source, Loss of GNSS signal, Network outage, Failure to meet contractual requirements, Violation of rules and regulation/Breach of legislation/Abuse of personal data

RELATED COMPONENTS – ASSET GROUPS	THREAT EXPOSURE
Servers, Systems and Cloud Computing Smart cars Infrastructure and Backend systems	Denial of Service, Malware, Manipulation of Information, OEM targeted attacks, Unauthorised activities, Identity theft, Abuse of authorisations, Manipulation of information, Sabotage, Software vulnerabilities exploitation, Failure or disruption of service, Communication protocol hijacking, Data replay, Man-in-the-middle attack / Session hijacking, Unintentional change of data or car components configuration, Using information and/or devices from an unreliable source, Loss of GNSS signal, Network outage, Failure to meet contractual requirements, Violation of rules and regulation/Breach of legislation/Abuse of personal data
Information	Denial of Service, Malware, Manipulation of Information, OEM targeted attacks, Unauthorised activities, Identity theft, Abuse of authorisations, Manipulation of information, Threats targeting autonomous sensors, Threats against AI and ML, Sabotage, Vandalism, Theft, Side-channel attacks, Fault injection, Theft, Failure or malfunction of a sensor/actuator, Software vulnerabilities exploitation, Failure or disruption of service, Communication protocol hijacking, Data replay, Man-in-the-middle attack / Session hijacking, Unintentional change of data or car components configuration, Information leakage, Using information and/or devices from an unreliable source, Erroneous use of configuration of car components, Loss of GNSS signal, Network outage, Failure to meet contractual requirements, Violation of rules and regulation/Breach of legislation/Abuse of personal data
Humans	Denial of Service, Malware, Manipulation of Information, OEM targeted attacks, Unauthorised activities, Identity theft, Abuse of authorisations, Manipulation of information, Sabotage, Vandalism, Theft, Failure or malfunction of a sensor/actuator, Software vulnerabilities exploitation, Failure or disruption of service, Communication protocol hijacking, Data replay, Man-in-the-middle attack / Session hijacking, Unintentional change of data or car components configuration, Information leakage, Using information and/or devices from an unreliable source, Erroneous use of configuration of car components, Loss of GNSS signal, Car depleted battery, Network outage, Failure to meet contractual requirements, Violation of rules and regulation/Breach of legislation/Abuse of personal data

References

1. "April 2020 Cyber Attacks Statistics". June 3, 2019. HACKMAGEDDON. https://www.hackmageddon.com/2020/06/03/april-2020-cyber-attacks-statistics/

2. "Data Breach Investigation Report" 2019. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

3. "CIRCL - Operational Statistics" 2019. CIRCL. https://www.circl.lu/opendata/statistics/

4. "Survey: The Third Annual Study on the State of Endpoint Security Risk". 2020. https://engage.morphisec.com/2020-endpoint-security-risk-study

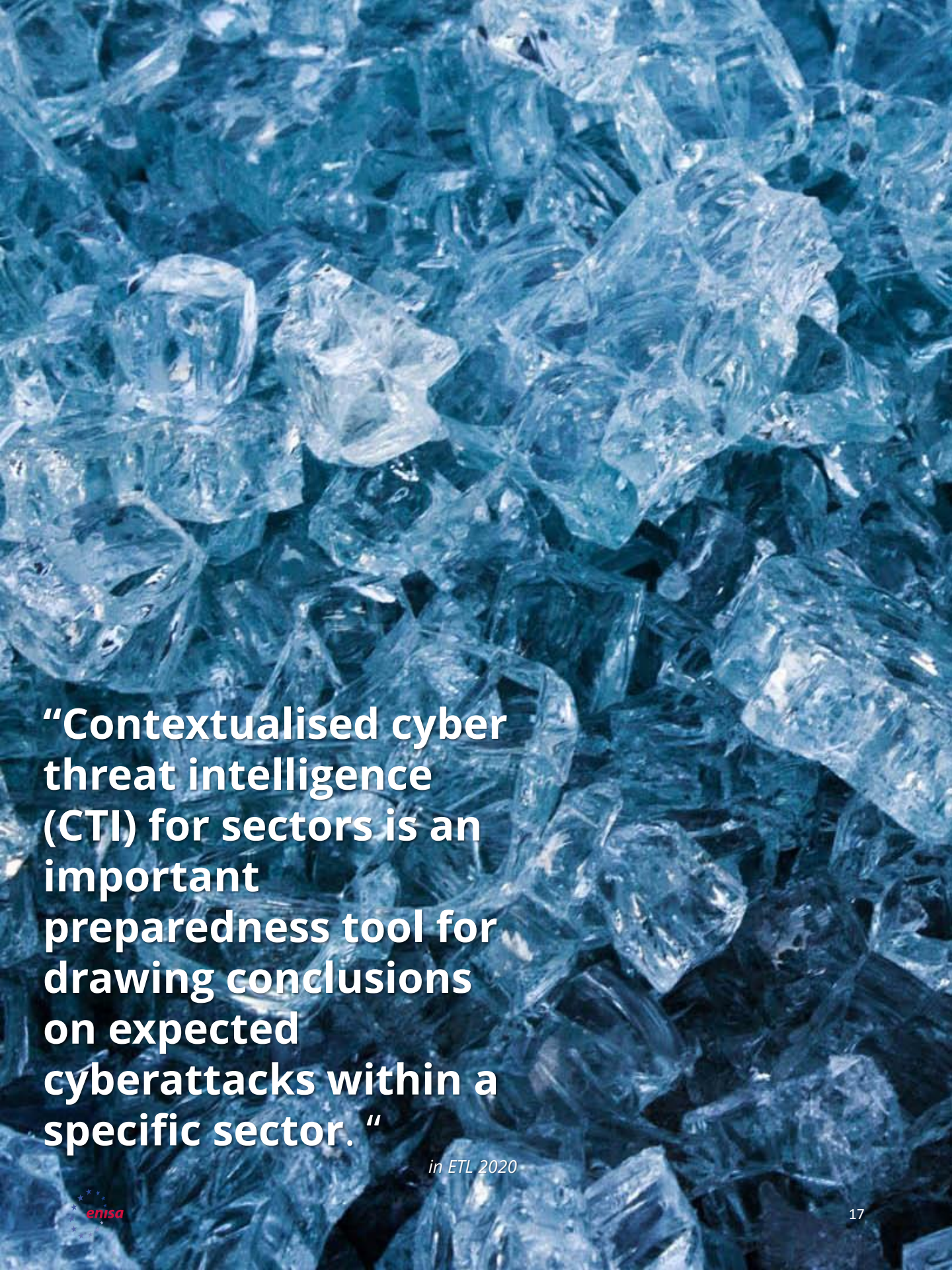
5. "Good Practices for Security of IoT - Secure Software Development Lifecycle". November 19, 2019. ENISA. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

6. "ENISA good practices for security of Smart Cars". November 25, 2019. https://www.enisa.europa.eu/publications/smart-cars

7. The selected order of sectors has been performed by consolidating statistics from various incident-based reports. It provides medial values for the reporting period (2019-Q1 2020) and may slightly deviate from values presented in monthly or quarterly reports.

8. "Player vs. Hacker: Cyberthreats to Gaming Companies and Gamers'. March 16, 2020. Security Intelligence. https://securityintelligence.com/posts/player-vs-hacker-cyberthreats-to-gaming-companies-and-gamers/

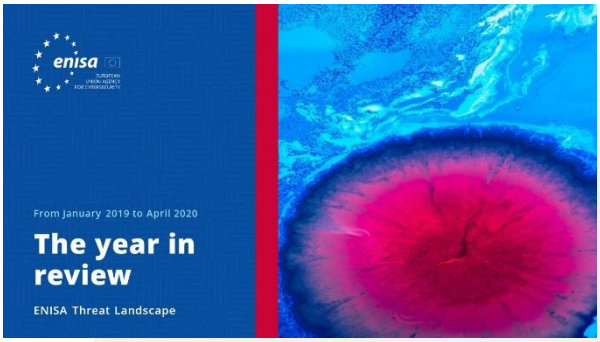
9. It is worth mentioning that the threat exposure has been assessed via detailed threat categories that have been developed by ENISA (see https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view) and is used for various sectorial assessments. Due to the absence of incident data for emerging sectors, the threat assessment goes at a greater detail to obtain a more exhaustive approach.



“Contextualised cyber threat intelligence (CTI) for sectors is an important preparedness tool for drawing conclusions on expected cyberattacks within a specific sector. “

in ETL 2020

Related



ENISA Threat Landscape Report
The year in review

Contextualised threat analysis between January 2019 and April 2020.

READ THE REPORT

ENISA Threat Landscape Report
List of Top 15 Threats

ENISAs' list of the top 15 threats of the period between January 2019 and April 2020.

READ THE REPORT

ENISA Threat Landscape Report
Research topics

Recommendations on research topics from various quadrants in cybersecurity and cyberthreat intelligence.

READ THE REPORT

READ THE REPORT

ENISA Threat Landscape Report
Main incidents in the EU and Worldwide

Main cybersecurity incidents happening between January 2019 and April 2020.

READ THE REPORT

ENISA Threat Landscape Report
Emerging trends

Main trends in Cybersecurity observed between January 2019 and April 2020.

READ THE REPORT

ENISA Threat Landscape Report
Cyber Threat Intelligence overview

The current state of play of cyberthreat intelligence in the EU.

About

_ The agency

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contributors
Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) and *all members of the ENISA CTI Stakeholders Group:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) and Thomas Hemker.

Editors
Marco Barros Lourenço (ENISA) and Louis Marinos (ENISA).

Contact
For queries on this paper, please use enisa.threat.information@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, 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.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu