EN

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

From January 2019 to April 2020

Ransomware

ENISA Threat Landscape

Overview

Ransomware has become a popular weapon in the hands of malicious actors who try to harm governments, businesses and individuals on a daily basis. In such cases, the ransomware victim may suffer economic losses either by paying the ransom demanded or by paying the cost of recovering from the loss, if they do not comply with the attacker's demands. In an incident in 2019, Baltimore, Maryland suffered a lockout and recovery is expected to pay US $18,2 million (ca. €15,4 million), although the city refused to pay the ransom.[1] With the growing number of incidents growing, it is evident that becoming a victim is not an 'if' but rather a 'when' hypothesis. However, in the majority of countries' fights against ransomware, several challenges need to be addressed, such as the lack of coordination and collaboration between agencies and authorities, and the lack of legislation, that clearly criminalises ransomware attacks.

Although cyber insurance policies exist since early 2000[2], ransomware attacks are one of the main reasons for the increased interest in this type of insurance during the last 5 years. In some of the 2019 incidents[7], the ransom or the costs of recovery was covered by such contracts. Unfortunately, if potential ransomware targets are known to be insured, the attackers assume that they will most probably be paid. Another downside for the victim is that insurance providers are paying the ransom in advance to mitigate the damage and to keep the victim's reputation intact. However, such compliance by paying ransoms encourages the hacker community and ensures neither the victim's recovery nor their reputation.[3]

__Findings

€10,1_billion estimated to be paid in ransoms during 2019

The amount of paid ransoms was US €3,3 billion more than in 2018.

365%_increase in detections in businesses in 2019

Ransomware detection in machines in business environments increased compared with the fists half of 2018.[22]

66%_of healthcare organisations experienced an attack

More than 66% of healthcare organisations experienced a ransomware attack in 2019.[23]

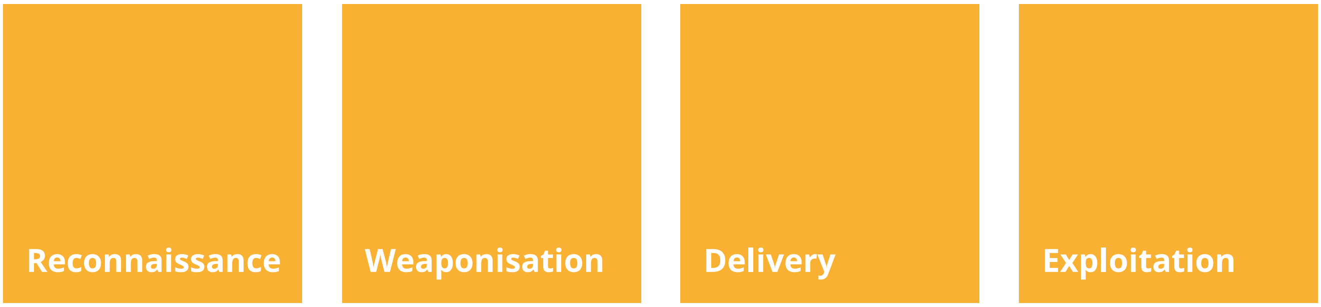
45%_of attacked organisations paid the ransom

This is the percentage of organisations attacked in 2019 that paid the ransom and half of them still lost their data.[37]

28%_of security incidents were attributed to malware

Ransomware was the second most common functionality following malware C2 and was related to one-third (28%) of security incidents.[32]

Kill chain



Reconnaissance

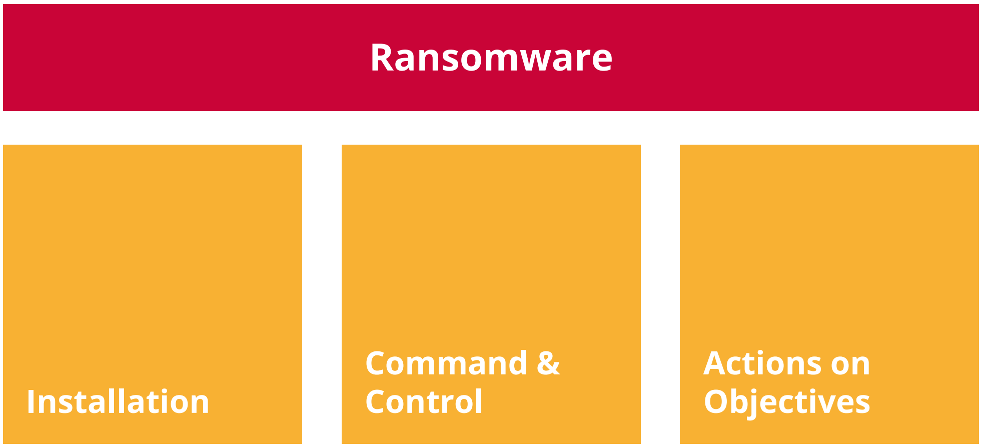
Weaponisation

Delivery

Exploitation

🟥 *Step of Attack Workflow*

🟧 *Width of Purpose*



Ransomware

Installation

Command & Control

Actions on Objectives

The Cyber Kill Chain® framework was developed by Lockheed Martin, adapted from a military concept related with the structure of an attack. To study a particular attack vector, use this kill-chain diagram to map each step of the process and reference the tools, techniques and procedures used by the attacker.

MORE INFORMATION

Description

_Ransomware aims higher

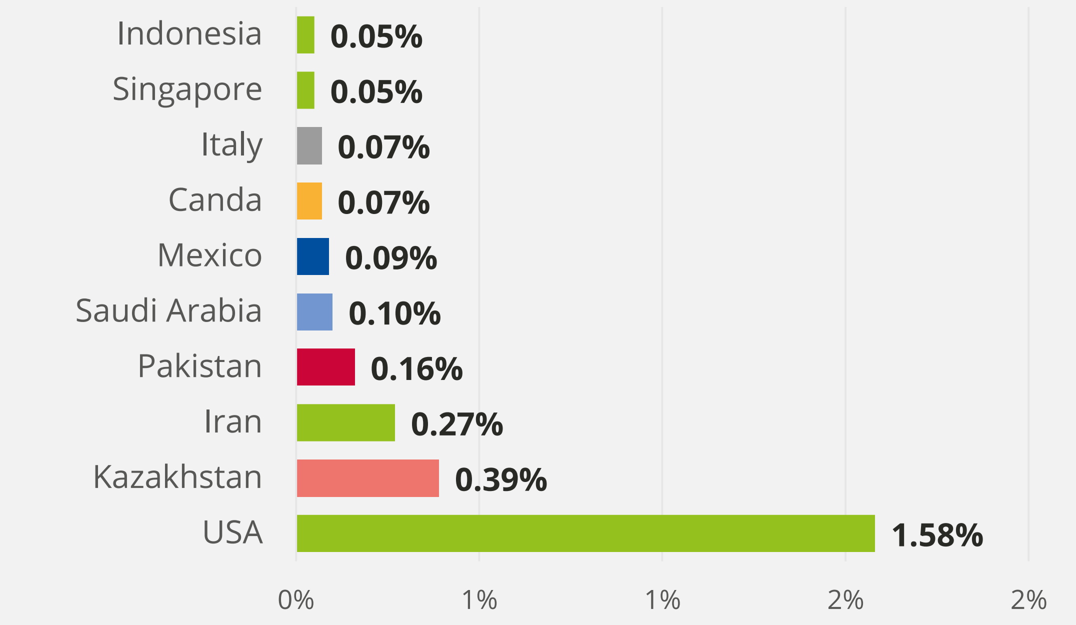
The Q1 and Q2 2019, ransomware attacks were fewer than those recorded in the same period during the previous 3 years. However, these ransomware attacks focused on high-profile targets. Throughout 2018, the deployment of Remote Access Trojan (RAT), downloaders and backdoors was noted but, during that year, that malware remained idle.[9,10] It is now concluded that this software provided the attackers with the intelligence to identify vulnerable high-profile targets, willing to pay higher amounts of ransom. Following this vein, in the reporting year, ransomware expanded to other sectors beyond the healthcare industry, targeting industrial and manufacturing firms. Recently, the LockerGoga ransomware family was used to damage systems that control the physical equipment in production plants.[11]

_Cyber insurance more popular

Cyber insurance policies in 2019 represented an US $8 billion (ca. €6,7 billion) market in the United States alone. Although such products exist since the Y2K or Millennium bug, in recent years they have become more appealing to governmental organisations, cities, healthcare organisations and several other potential high-risk ransomware targets. The SamSam attack in Atlanta, Georgia and the Lake City, Florida, incident were covered by such policies.[16] As the ransom demands increase, cyber-insurance policies are becoming increasingly necessary for organisations and companies. However, common sense suggests that the victims must avoid caving in to demands, if possible. When the ransom demands are met not only is the attacker encouraged to repeat the act but the victim may also not recover as in several cases the attacker do not keep their end of the bargain.

_Open Remote Desktop Protocol (RDP) is a high risk

Several successful ransomware families such as SamSam, BitPaymer and CrySiS target RDP servers to initiate an attack.[20] Unfortunately, many organisations still use RDP instead of the more secure Virtual Private Network (VPN) for remote access. The problems with the RDP is that it suffers from vulnerabilities that can be exploited and the RDP service may rely on internet-facing servers which are easily accessed. More than 800.000 systems with RDP services have been reported to be unpatched and vulnerable; among them, systems in the IP range of the Microsoft Azure data centre.[51] Although Microsoft assured the public that these systems belonged to a third-party, an issue arises regarding cloud service providers' security.



Top 10 countries by share of users attacked by mobile ransomware Trojans in Q2 2919. Source: Kapersky[34]

Description

_ The most wanted

LOCKERGOGA_ was first reported in January 2019 in an attack on the French engineering consultancy company, Altran Technologies.[40] Its IT networks and all the applications went down and the company's operations in several countries were affected. LockerGoga is dropped and executed by the PsExec tool, which is a light-weight telnet replacement, able to pass some security checks as semi-valid software.[11] Once installed, the user accounts in the targeted system are modified and the system is forcibly logged-off. In addition, the tool files are self-renamed and self-relocated, and, as a result they become almost impossible to be located. In later versions of LockerGoga, the lock-down is so tight that the victims are not even able to see the ransomware note or the instructions for recovery, even if the demands are met. Only a few anti-malware and anti-virus products are able to detect and defend systems against LockerGoga and a specific decryptor does not exist.[10] Other than Altran Technologies, NorskHydro and two United States-based chemical companies, Hexion and Momentive were targeted by LockerGogain 2019.[41] For the NorskHydro attack alone, the cost of the damage was estimated at US $50 million (ca. €42 million).[21]

KATYUSHA_ is a ransomware trojan first used in October 2018. It encrypts the victim's files, deletes shadow copies and delivers attachments by e-mail. Katyusha uses the EternalBlueand DoublePulsar exploits to spread.[45] Unfortunately, no tools or decryptors are yet available for defence.

JIGSAW_ not only encrypts the victim's files, but it also deletes them if the demands are not met within the, most commonly, 24 hour deadline given. Furthermore, if the victim attempts something like shutting down their computer, the deletion rate increases. It is not an accident that this ransomware was named after a horror movie character.[45] However, security companies constantly releases updates for an efficient Jigsaw decryptor.[46]

PEWCRYPT_ was created at the beginning of 2019 and, unlike most ransomware its only goal is to force people to subscribe to the PewDiePie YouTuber channel. PewDiePie was in a popularity competition with an Indian Bollywood channel, T-Series and his fans decided to use PewCrypt to increase their idol's chances of winning. PewCrypt is a typical ransomware spread by spam e-mails and malicious online advertisements. It was created in the Java programming language. In March 2019, the author himself released a decryption tool.[47]

RYUK_ first appeared in August 2018 and was assumed to be associated with North Korean hacking groups. Soon enough, the Ryuk authors were proved to be the same group that became known for using the Hermes ransomware while also stealing its code. Ryuk's main characteristics are its use of military algorithms and its targeted attacks on big enterprises. Moreover, most of its victims are asked to pay the ransom in Bitcoins.[45]

DHARMA_ is a crypto virus that first appeared in 2016 but new versions are still being released. Dharma not only encrypts the victim's files but also deletes any shadow copies. In 2019, it was spread by contaminated files with popular, harmful or legitimate extensions such as '.gif', '.AUF', '.USA', '.xwx', '.best' and '.heets'. In September 2019, a security researcher released the Rakhnidecryptor[42] to help Dharma victims decrypt their files.

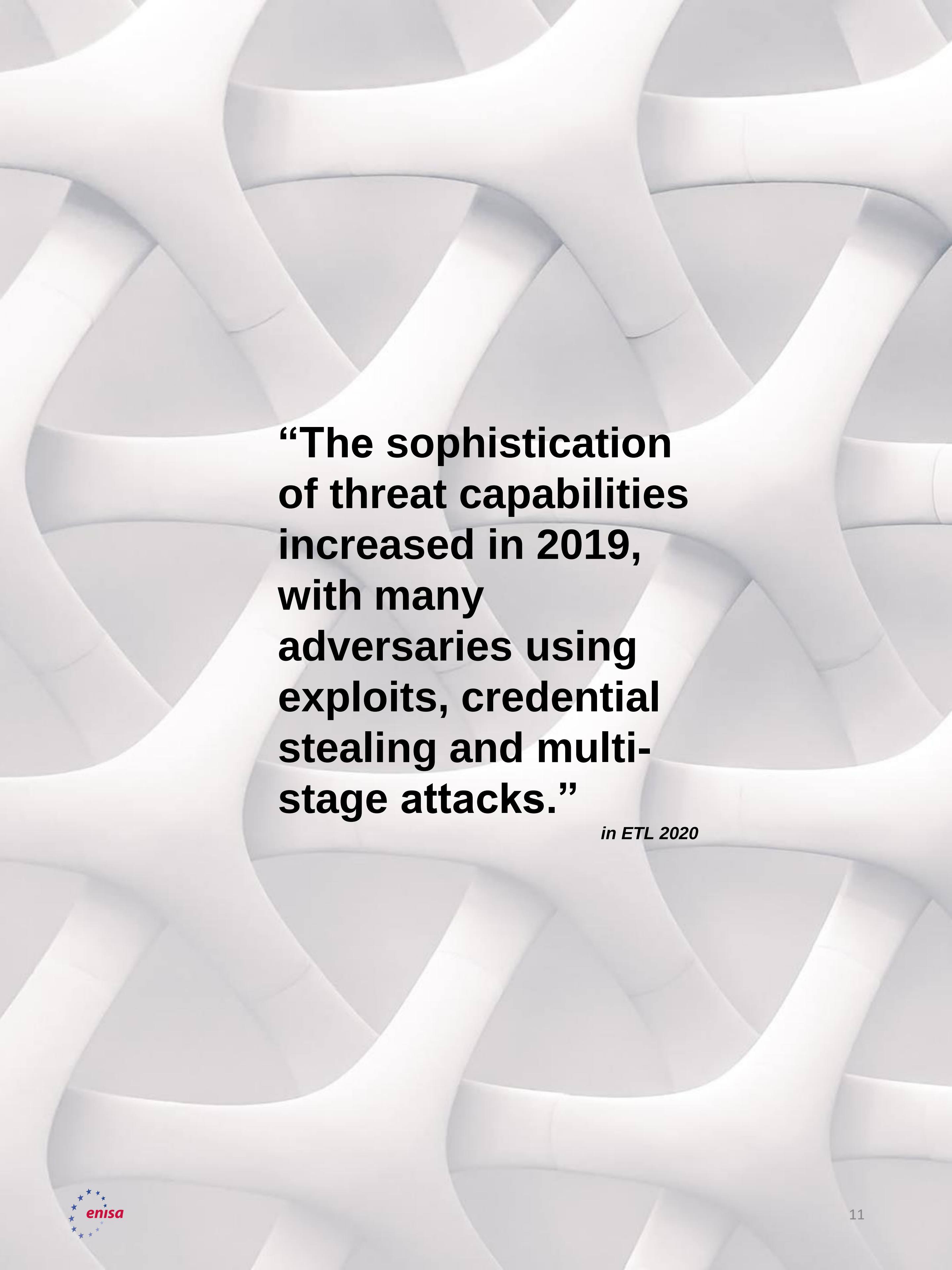
GANDCRAB_ was used for the first time in January 2018 and infected more than 50,000 systems in less than a month, becoming one of the most popular ransomwares of 2018.[43] It exploits Microsoft Office macros, VBScript and PowerShell to attack undetected.[45] GandCrab is similar to Cerber, it is based on the ransomware-as-a-service (RaaS) model and allows the developers and the criminals to share profit. A team created by Europol, the Romanian police, the General Prosecutor's Office and Bitdefender managed to produce a decryptortool[44] after hacking the GandCrab servers. The operators of GandCrab announced their retirement in Q2 2019 after collecting more than US $2 billion in ransom payments. However, the Sodinokibi ransomware, which is observed in small campaigns, is alleged to be GandCrab's successor.[10]

Description

_ The most wanted

REVIL or SODINOKIBI or SODIN_ first appeared in a web attack on the Italian WinRAR tool in June 2019. It is also suspected to be involved in three MSP attacks and a fourth one against the American company PerCSoft, the clientele of which is mainly from the healthcare sector.[48] Sodinokibi seems to be a product of the well-known cyber-espionage group FruityArmor, which has been active since 2016. Sodinokibi has affected several countries worldwide. Taiwan has suffered 17,56% of all recorded Sodinokibi attacks so far, making it Sodinokibi's most targeted country. In Europe, the most targeted countries are Germany (8,05%), Italy (5,12%) and Spain (4,88%). Sodinokibi is distributed by a RaaS model and encrypts the files needed for an attack to take place in a per-system manner. The attackers embed a 'skeleton key' within their code allowing them to remotely decrypt files, regardless of the original encryption.[49] However, if a computer has Russian, Armenian, Syrian or certain other keyboard layouts it is no possible for Sodinokibi's to encrypt it, a fact probably pointing to the origin of the authors.[50]

SAMSAM_ continues to target critical infrastructure globally for a fifth consecutive year. SamSam attacks mainly focus on hospitals, healthcare companies and governmental organisations to ensure fast payment of big ransoms. It exploits vulnerabilities of the Remote Desktop Protocol (RDP). To date the group responsible for the distributing SamSam has raised more than US $6 million (ca. €5 million) in ransom payments and has cost the victims more than US $30 million (ca. €25,4 million).[45] From the 2018 attack against on the city of Atlanta alone the damage and recovery costs amounted US $17 million (ca. €14,4 million).[43]



“The sophistication of threat capabilities increased in 2019, with many adversaries using exploits, credential stealing and multi-stage attacks.”

in ETL 2020

Description

_ Targeted sectors

NATION-STATES ARE STILL IN THE SPOTLIGHT_ In 2018, ransomware was used to target nation-state organisations as a money making tool. This trend continued in 2019, whereby nations or nation groups obfuscated their identity by using the very same tools created by other groups or nation-state actors. This manipulation of tools allows the attacker's origin to remain hidden and their nation to avoid any diplomatic consequences, especially when the target is a governmental or a state organisation.

In 2019, several attacks against governmental or state organisations took place such as the one in which the Californian city of Lodi[4] was asked to pay US $400.000 (ca. €340.000) in ransom to be released from a lock out of the Police Department's phone lines, the Public Works' emergency line, the City Hall's numbers and the city's payment data and financial systems. The city refused to comply and recovered from the attack by using backups. The Texas Department of Information Resources reported a coordinated ransomware attack on 23 small governmental organisations in August 2019.[5] The cost for the Texas county was estimated to be US $3,25 million (ca. €2,75 million). Baltimore suffered a RobbinHood attack causing a damage costing US $18,2 million (ca. €15,4 million), while the Lake City in Florida endured a Ryuk attack causing a loss of US $460.000 (ca. €389.768). The city of New Bedford in Massachusetts was also hit by ransomware attack in July 20196 and demanded the payment of a ransom of US $5,3 million (ca. €4,4 million). The city refused to pay the ransom and instead spent US $1 million to recover from the attack.[7]

EDUCATIONAL INSTITUTIONS ARE JOINING THE PARTY_ During 2019, we observed a shift in attacks towards educational institutions. According to a report released by the security company Emsisoft, 1.051 schools and colleges were victims of 62 ransomware incidents. In 2018, the incidents affecting educational institutions were only 11. The report declares that American schools were the second more common victims after the local municipalities.[8]

THE HEALTH SECTOR CONTINUOUS TO SUFFER_ Healthcare organisations were the favourite target of ransomware attackers during all of the previous years, and this trend also continued in 2019. Californian providers Wood Ranch Medical were hit during summer, and the electronic medical records of the company were completely destroyed (including the backups) as a result of its refusal to pay the ransom. The incident forced Wood Ranch Medical to announce that it would cease to operate by the end of the year.[12] In April 2019, the exact same exact sequence of events befell another medical provider, Michigan Brookside ENT and Hearing Centre[13], which was also forced to shut down. Furthermore, in Australia, two hospital groups were attacked: the GippslandHealth Alliance and the South West Alliance of Rural Health. The result was that hospitals in several cities including Warrnambool, Colac, Geelong, Warragul, Sale, and Bairnsdale could not fulfil normal patient procedures, as their systems went offline to limit the exposure.[14] In this sector, the data loss is equally damaging to the financial loss. For instance, more than 300.000 patients' Protected Health Information was leaked as a result of a ransomware attack placed in June 2019 against the Premier Family Medical group in Utah.[15]

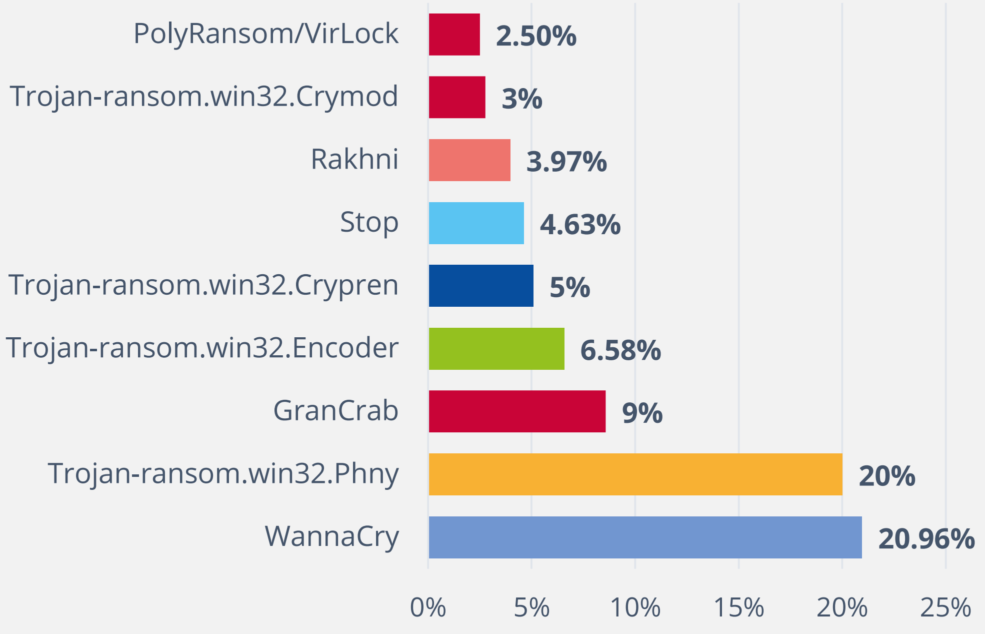
MSP ARE DOWN_ Numerous industries rely on managed service providers (MSP) and cloud service providers (CSP) to host sensitive information, that is essential to their operations. They also rely on them for the integrity of the data and the prevention of unauthorized access to them.[17] However, the GandCrab and Sodin ransomwares target vulnerabilities in the MSPs that expose their infrastructure and the data they host and, eventually, they allow the ransomware attack to spread to the entire MSP's clientele. The Webroot2FA, a common MSP tool, embeds such vulnerabilities and has been used in several cases during 2019.[18] This year, several MSPs were attacked within a period of three months only, such as PM Consultants, CloudJumper, Datto, PercSoft, TSM Consulting Services Inc. and IT By Design.[19]

Attack vectors

_ How

A new ransomware called Sodinokibi exploits the recently announced CVE-2019-2725 Oracle WebLogic Server's vulnerability to gain remote code execution abilities. The victim is infected with no action taken. Official patches have also been released for the Oracle WebLogic Server versions 10.3.6.0 and 12.1.3.0.[51] The same attack exploits the CVE-2018-8453 vulnerability to gain more (elevate) user privileges, terminate blacklisted processes, delete blacklisted files and exfiltrate host information.[48]

Another vulnerability, the CVE-2019-0708, is also used for planting ransomware. It allows unauthorized connection via Microsoft's remote desktop protocol (RDP). In May 2019, Microsoft released patches for the current operating system (OS) versions as well as for those versions that are not supported any more.[51]



Top ransomware attacks in 2019. Source: Kapersky[39]

Incidents

- The Baltimore County incident[1]
- Alabama hospitals attack[7]
- Lodi California City incident[4]
- Texas (Texas Department of Information Resources) incident[5]
- Lake City (Florida) Ryuk attack[7]
- New Belford (Massachusetts) incident[6]
- Ransomware attacks on > 500 schools and universities[8]
- Wood Ranch Medical (California) case[12]
- Michigan Brookside ENT and Hearing Centre incident[13]
- Gippsland Health Alliance and the South West Alliance of Rural Health (Australia) incidents[14]
- Premier Family Medical group (Utah) incident[15]
- MSPs PM Consultants, CloudJumper, Datto, PercSoft, TSM Consulting Services Inc. and IT By Design incidents[19]
- Microsoft Azure data centre incident[51]
- Altran Technologies LockerGoga attack[40]
- Norsk Hydro LockerGoga attack[7]
- Hexion and the Momentive LockerGoga attacks[41]
- Albany IT incident[60]
- Jackson County (Georgia) incident[61]
- Riviera Beach (Florida) incident[62]
- New Orleans incident[63]
- Danish hearing aid manufacturer Demant attack[64]

Mitigation

_Proposed actions

- Maintain reliable backups that follow the 3-2-1 rule (i.e. maintain at least three copies, in two different formats, keeping one of those copies off-site).[5]
- Invest in a cyber insurance policy covering ransomware attack damages.[21]
- Use network segmentation, data encryption, access control, and policy enforcement to ensure minimum exposure of data.
- Use methods such as monitoring to quickly identify infections.
- Monitor access to and status of the public infrastructure used.
- Create a security operation centre (SOC) staffed by skilled security personnel within every organisation or company.
- Use appropriate and updated tools for ransomware prevention.
- Define exactly and implement a minimum set of user data access rights to minimise the impact of attacks (i.e. fewer rights, less data encrypted).
- Implement robust vulnerability and patch management.
- Implement content filtering to filter out unwanted attachments, e-mails with malicious content, spam and unwanted network traffic.
- Install end-point protection by means of anti-virus programs but also by blocking execution of files (e.g. block execution in Temp folder).
- Use policies to control external devices and port accessibility.
- Use whitelisting to prevent unknown executables from being executed at endpoints.
- Invest in raising users' awareness of ransomware especially with regard to secure browsing behaviour.

_Decryptors

Significant progress has been achieved by EUROPOL and 163 partners with the ‘No more ransom project’.[65] The portal has added 28 tools in 2019 and can now decrypt 140 different types of ransomware infections. A handful of ransomware decryptors have been develop and many others updated. Examples are listed below.

RANSOMWARE	DECRYPTOR
Aurora[52]**, Muhstik**[53]**, Ryuk**[54]	Emsisoft
Rakhni, Aura, Autoit, Pletor, Rotor, Lamer, Lortok, Democry, TeslaCrypt, Chimera, Crysis, Jaff, Dharma, Cryakl, Yatron, FortuneCrypt,[55,56]	Kaspersky Lab
GandCrab[44]	Europol, Romanian Police and GPO, Bitfender
Jigsaw[46]	Avast
Mira[57]	F-Secure
Nemty[58]	Tesorion
PewCrypt[47]	PewCrypt author

References

1. "Washington idle as ransomware ravages cities big and small" September 28, 2019. Politico. https://www.politico.com/news/2019/09/28/ransomware-cities-washington-007376

2. "What you — and your company — should know about cyber insurance", August 20, 2019. Talos. https://blog.talosintelligence.com/2019/08/cyber-insurance-FAQs.html

3. "The State of Ransomware in 2019" June 17, 2019. IT Pro Today. https://www.itprotoday.com/threat-management/state-ransomware-2019

4. "California City Confirms Phone Line and Financial Data System Disruptions Caused by Ransomware". August 2, 2019. Trend Micro. https://www.trendmicro.com/vinfo/de/security/news/cybercrime-and-digital-threats/california-city-confirms-phone-line-and-financial-data-system-disruptions-caused-by-ransomware

5. "Coordinated Ransomware Attack Cripples Local Government Organizations in Texas", August 19, 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coordinated-ransomware-attack-cripples-local-government-organizations-in-texas

6. "The State of Ransomware in the US: Report and Statistics 2019". December 12, 2019. EMSISOFT blog. https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

7. "Alabama hospitals have been hit by a massive ransomware attack" October 3, 2019. https://www.foxnews.com/tech/alabama-hospitals-ransomware-attack

8. "500+ Schools Have Been Affected by Ransomware in 2019", October 4, 2019. Campus Safety, https://www.campussafetymagazine.com/safety/500-schools-ransomware-2019/

9. "Latest Quarterly Threat Report - Q1 2019" 2019. Proof Point. https://www.proofpoint.com/us/resources/threat-reports/latest-quarterly-threat-research

10. "Proofpoint Q2 2019 Threat Report - Emotet's hiatus, mainstream impostor techniques, and more". September 19, 2019. Proof Point. https://www.proofpoint.com/us/threat-insight/post/proofpoint-q2-2019-threat-report-emotets-hiatus-mainstream-impostor-techniques

11. "6 of the Biggest Cybersecurity Crises of 2019 (So Far)" September 24, 2019. EC-Council Blog. https://blog.eccouncil.org/6-of-the-biggest-cybersecurity-crises-of-2019-so-far/

12. "Ransomware Attacks Double in 2019: Medical Providers Can't Recover and Shut Down" October 3, 2019. https://www.natlawreview.com/article/ransomware-attacks-double-2019-medical-providers-can-t-recover-and-shut-down

13. "Michigan's Brookside ENT and Hearing Center forced to close due to a Ransomware Attack" April 23, 2019. SPAM Fighter. https://www.spamfighter.com/News-22154-Michigans-Brookside-ENT-and-Hearing-Center-forced-to-close-due-to-a-Ransomware-Attack.htm

14. "Victorian hospitals across Gippsland, Geelong and Warrnambool hit by ransomware attack". October 1, 2019. https://www.abc.net.au/news/2019-10-01/victorian-health-services-targeted-by-ransomware-attack/11562988?nw=0

15. "Ransomware Attack Affects 300,000 Patients in Utah". September 12, 2019. CISO Mag. https://www.cisomag.com/ransomware-attack-affects-300000-patients-in-utah/

16. "The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks". August 27, 2019. ProPublica. https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks

17. "CYBER THREATSCAPE REPORT". 2019. Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

18. "Ransomware Amounts Rise 3x in Q2 as Ryuk & Sodinokibi Spread". 2019. Coveware. https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread

19. "Armor Identifies 15 New Ransomware Victims in the Last 2 Weeks, All of them Educational Institutions – Threat Intelligence". September 20, 2019. Armor. https://www.armor.com/resources/armor-identifies-10-new-ransomware-victims-in-the-past-9-days/

20. “4 Ransomware Trends to Watch in 2019”. February 13, 2019. https://www.recordedfuture.com/ransomware-trends-2019/

21. “BDO Cyber Threat Insights - 2019 2nd Quarter Report”, July 2019. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdo-cyber-threat-insights-2019-2nd-quarter-report

22. “BDO’s Fall 2019 Cyber Threat Report: Focus on Healthcare”. October 2019. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdos-fall-2019-cyber-threat-report-focus-on-health

23. “Healthcare Cyber Heists in 2019” October 3, 2019. VMWare. https://www.carbonblack.com/resources/threat-research/healthcare-cyber-heists-in-2019/

24. “Australia | Global Threat Report | Defender Power On The Rise”. 2019. VMWARE. https://www.carbonblack.com/land/australia-global-threat-report-defender-power-on-the-rise/

25. “France | Global Threat Report | Defender Power On The Rise”. 2019. VMWARE. https://www.carbonblack.com/land/france-global-threat-report-defender-power-on-the-rise/

26. “Italy | Global Threat Report | Defender Power On The Rise”. 2019. VMWARE. https://www.carbonblack.com/land/italy-global-threat-report-defender-power-on-the-rise/

27. “Japan | Global Threat Report | Defender Power On The Rise”. 2019. VMWARE. https://www.carbonblack.com/land/japan-global-threat-report-defender-power-on-the-rise/

28. “Canada | Global Threat Report | Defender Power On The Rise”. 2019. VMWARE. https://www.carbonblack.com/land/canada-global-threat-report-defender-power-on-the-rise/

29. “Singapore | Global Threat Report | Defender Power On The Rise”. 2019. VMWARE. https://www.carbonblack.com/land/singapore-global-threat-report-defender-power-on-the-rise/

30. “UK | Global Threat Report | Defender Power On The Rise”. 2019. VMWARE. https://www.carbonblack.com/land/uk-global-threat-report-defender-power-on-the-rise/

31. “Anticipating the Unknowns”. March 2019. Cisco. https://ebooks.cisco.com/story/anticipating-unknowns/

32. “2020 Data Breach Investigations Report” 2020. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

33. “IBM Security Study: Taxpayers Oppose Local Governments Paying Hackers in Ransomware Attacks”. September 5, 2019. IBM. https://newsroom.ibm.com/2019-09-05-IBM-Security-Study-Taxpayers-Oppose-Local-Governments-Paying-Hackers-in-Ransomware-Attacks

34. IT threat evolution Q2 2019 statistics” 2019 Kaspersky, https://securelist.com/it-threat-evolution-q2-2019-statistics/92053/

35. IT threat evolution Q1 2019 statistics” 2019 Kaspersky, https://securelist.com/it-threat-evolution-q1-2019-statistics/90916/

36. “The state of industrial cybersecurity”. July 2019. Kaspersky. https://ics.kaspersky.com/media/2019_Kaspersky_ARC_ICS_report.pdf

37. “2019 Cyberthreat Defense Report” Cyber Edge Group. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

38. “Evasive Threats, Pervasive Effects”. August 27, 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/evasive-threats-pervasive-effects

39. IT threat evolution Q3 2019 statistics” 2019 Kaspersky, https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/

40. “What You Need to Know About the LockerGoga Ransomware.” March 20, 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware/

41. “BDO Cyber Threat Insights - 2019 2nd Quarter Report”, July 2019. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdo-cyber-threat-insights-2019-2nd-quarter-report

References

42. Ransomware Decryptor Tools**,** Kapersky https://noransom.kaspersky.com/

43. “ENISA Threat Landscape Report 2018”. January 28, 2019. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

44. “New GandCrab v5.1 Decryptor Available Now”, February 19, 2019. Bitdefender LABS. https://labs.bitdefender.com/2019/02/new-gandcrab-v5-1-decryptor-available-now/

45. “10 Ransomware Attacks You Should Know About in 2019” April 28, 2019. Allot. https://www.allot.com/blog/10-ransomware-attacks-2019/

46. Ransomware Decryptor Tools. Avast. https://www.avast.com/ransomware-decryption-tools

47. PewCrypt Ransomware Source. GitHub. https://github.com/000JustMe/PewCrypt

48. “Are the REvil, GranCrab Ransomware Families Related?” September 25, 2019. MSSP Alert. https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/revil-gandcrab-related/

49. “Threat Landscape Report”, Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q3-2019.pdf

50. “Sodin Ransomware includes exploit for Windows CVE-2018-8453 bug“. July 4, 2019. Security Affairs. https://securityaffairs.co/wordpress/87944/malware/sodin-ransomware-cve-2018-8453.html

51. “Threat Landscape Report” 2019. Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q2-2019.pdf

52. “Emsisoft Decryptor for Aurora” 2019. Emsisoft. https://www.emsisoft.com/ransomware-decryption-tools/aurora

53. “Emsisoft Decryptor for Muhstik” 2019. Emsisoft. https://www.emsisoft.com/ransomware-decryption-tools/muhstik

54. “Caution! Ryuk Ransomware decryptor damages larger files, even if you pay”. December 9, 2019. Emsisoft. https://blog.emsisoft.com/en/35023/bug-in-latest-ryuk-decryptor-may-cause-data-loss/

55. “RakhniDecryptor tool for defending against Trojan-Ransom.Win32.Rakhni ransomware”. Kaspersky. https://support.kaspersky.com/10556

56. “Another two bite the dust: Kaspersky updates decryption tool to fight ransomware pair”. September 27, 2019. The Online Citizen. https://www.theonlinecitizen.com/2019/09/27/another-two-bite-the-dust-kaspersky-updates-decryption-tool-to-fight-ransomware-pair/

57. “Mira Ransomware Decryptor” April 1, 2019. F-Secure. https://blog.f-secure.com/mira-ransomware-decryptor/

58. “Nemty update: decryptors for Nemty 1.5 and 1.6” Tesorion. https://www.tesorion.nl/nemty-update-decryptors-for-nemty-1-5-and-1-6/

59. “McAfee Labs Threats Report”, August, 2019. McAfee, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

60. “The 10 biggest ransomware attacks of 2019” CRN. https://www.crn.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/2

61. “The 10 biggest ransomware attacks of 2019” CRN. https://www.crn.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/3

62. “The 10 biggest ransomware attacks of 2019” CRN. https://www.crn.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/6

63. “The 10 biggest ransomware attacks of 2019” CRN. https://www.crn.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/7

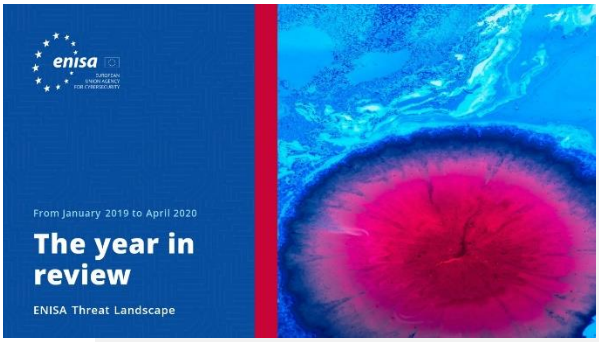
64. “The 10 biggest ransomware attacks of 2019” CRN. https://www.crn.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/11

65. https://www.nomoreransom.org/

“CTI has been firmly established in the cybersecurity domain as an essential tool for enhancing agility and efficiency in defending cyberattacks.”

in ETL 2020

Related



From January 2019 to April 2020

The year in review

ENISA Threat Landscape

READ THE REPORT

ENISA Threat Landscape Report **The year in review**

A summary on the cybersecurity trends for the period between January 2019 and April 2020.

From January 2019 to April 2020

ENISAs' list of top 15 threats

ENISA Threat Landscape

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.

From January 2019 to April 2020

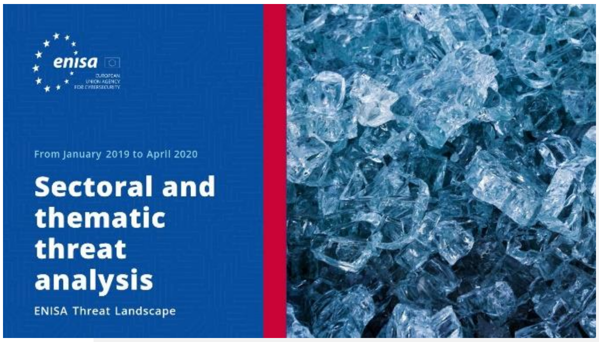
Research topics

ENISA Threat Landscape

READ THE REPORT

ENISA Threat Landscape Report **Research topics**

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



enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

From January 2019 to April 2020

Sectoral and thematic threat analysis

ENISA Threat Landscape

READ THE REPORT

ENISA Threat Landscape Report **Sectoral and thematic threat analysis**

Contextualised threat analysis between January 2019 and April 2020.

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

From January 2019 to April 2020

Emerging trends

ENISA Threat Landscape

READ THE REPORT

ENISA Threat Landscape Report **Emerging trends**

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

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

From January 2019 to April 2020

Cyberthreat intelligence overview

ENISA Threat Landscape

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.

Copyright Notice

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