EN

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

From January 2019 to April 2020

Cyber espionage

ENISA Threat Landscape

Overview

Cyber espionage is considered both a threat and a motive in the cybersecurity playbook. It is defined as 'the use of computer networks to gain illicit access to confidential information, typically that held by a government or other organisation'.[1]

In 2019, many reports revealed that global organisations consider cyber espionage (or nation-state-sponsored espionage) a growing threat affecting industrial sectors, as well as critical and strategic infrastructures across the world, including government ministries, railways, telecommunication providers, energy companies, hospitals and banks. Cyber espionage focuses on driving geopolitics, and on stealing state and trade secrets, intellectual property rights and proprietary information in strategic fields. It also mobilises actors from the economy, industry and foreign intelligence services, as well as actors who work on their behalf. In a recent report, threat intelligence analysts were not surprised to learn that 71% of organisations are treating cyber espionage and other threats as a 'black box' and are still learning about them.

In 2019, **the number of nation-state-sponsored cyberattacks targeting the economy increased and it is likely to continue this way**. In detail, nation-state-sponsored and other adversary-driven attacks on the Industrial Internet of Things (IIoT) are increasing in the utilities, oil and natural gas (ONG), and manufacturing sectors. Furthermore, cyberattacks conducted by advanced persistent threat (APT) groups indicate that financial attacks are often motivated by espionage. Using tactics, techniques and procedures (TTPs) akin to those of their espionage counterparts, groups such as the Cobalt Group, Carbanak and FIN7 have allegedly been targeting large financial institutions and restaurant chains successfully.

- The European Parliament's Committee of Foreign Affairs called upon Member States to establish a cyber-defence unit and to work together on their common defence. It stated that 'the Union's strategic environment has been deteriorating … in order to face the multiple challenges that directly or indirectly affect the security of its Member States and its citizens; whereas issues that affect the security of EU citizens include: armed conflicts immediately to the east and south of the European continent and fragile states; terrorism – and in particular Jihadism –, cyberattacks and disinformation campaigns; foreign interference in European political and electoral processes'.[42]
- Threat actors motivated by financial, political, or ideological gain will increasingly focus attacks on supplier networks with weak cybersecurity programs. Cyber espionage adversaries have slowly shifted their attack patterns to exploiting third- and fourth-party supply chain partners.[1]

Data breaches motivated by cyber espionage[2]

20%

Malicious actors connected with nation-states

38%

Incidents motived by cyber espionage

11,2%

Cyber espionage incidents involving phishing

63%

Incidents

- South Korean's Ministry of National Defence announced that unknown hackers had compromised computer systems at the ministry's procurement office.[3]
- The United States Department of Justice announced a foreign state-sponsored operation with a botnet meant to disrupt by targeting companies in the media, aerospace, financial, and critical infrastructure sectors.[16]
- The Norwegian software firm Visma revealed that it had been targeted by hackers who were attempting to steal trade secrets from the firm's clients.[4]
- Individuals were caught in the early stages of gaining access to computer systems of several political parties and of the Australian Federal Parliament.[17]
- European aerospace company Airbus revealed that it was targeted by alleged nation-state sponsored hackers who stole personal and IT identification information of many employees.[19]
- Following an attack on Indian military forces in Kashmir, Pakistani hackers targeted almost 100 Indian government websites and critical systems.[5]
- Indonesia's National Election Commission reported that Chinese and Russian individuals had probed the voters' database ahead of presidential and legislative elections in the country.[20]
- Foreign hackers targeted several European government agencies ahead of EU elections in May.[21]
- The Australian Signal Directorate revealed that it had conducted cyberattacks against ISIS in the Middle East.[22]
- The Finish police probed a DoS attack against the web service used to publish the vote tallies from Finland's elections.[6]
- Amnesty International's Hong Kong Office announced that it had been the victim of an cyberattack.[23]
- The Israeli Defence Forces launched an airstrike on the Hamas after they unsuccessfully attempted to hack Israeli targets.[7]

- An Iranian network of websites and accounts was allegedly used to spread out false information about United Sates, Israel and Saudi Arabia.[24]
- Croatian government agencies were targeted in a series of attacks by unidentified state-sponsored hackers. The malware payloads were Empire backdoor and SilentTrinity, neither of which had been seen before.[26]
- Libya arrested two men who were accused of working with a Russian 'troll farm' to influence the elections in several African countries.[27]
- Several major German industrial firms including BASF, Siemens, and Henkel announced that they had been the victim of a state-sponsored hacking campaign.[28]
- A state-sponsored group allegedly conducted a series of cyberattacks against Egyptian journalists, academics, lawyers, human rights activists, and politicians.[8]
- A state-sponsored hacking group targeted diplomats and high-profile Russian speaking users in Eastern Europe using malware dubbed Attor.[29]
- An Israeli cybersecurity firm was found to have sold spyware used to target senior government and military officials in at least 20 countries by exploiting a vulnerability in WhatsApp.[32]
- A 7 year campaign by an unidentified Spanish-language espionage group was revealed to have resulted in the theft of sensitive mapping files from senior officials in the Venezuelan Army.[10]
- A state-sponsored cyberespionage group allegedly conducted a phishing campaign targeting Chinese government agencies and state-owned enterprises for information related to economic trade, defence issues, and foreign relations.[33]
- The Czech Foreign Ministry fell victim to a cyberattack by an unspecified foreign state.[34]
- A non-state actor targeted the British Labour party with a major DDoS attack that temporarily took the party's computer systems offline ahead of the national elections'.[36]

Incidents

_ The General Electric case

Xiaoqing Zheng, an American citizen of Chinese descent, was accused of spying against General Electric (GE). Mr. Zheng allegedly stole GE's turbine technology secrets and delivered them to a Chinese business man who allegedly, delivered them to a Chinese officials. Mr Zheng worked for GE between 2008 and 2018.[15]

The United Sates justice department accused the two men of stealing information to advance their own business interests in two turbine research and development companies - Liaoning Tianyi Aviation Technology Co Ltd and Nanjing Tianyi Avi Tech Co Ltd.[47]

The *modus operandi* of this inside threat actor included:

- copying secrets into a USB drive until GE blocked the use of these devices;
- encrypting the secrets and use steganography to hide data files in the binary code of digital photo files;
- plugging an iPhone to the work desktop computer to copy the image;
- sending the files to his personal e-mail address.

_ Mitigation measures

Because of the comprehensive nature of this threat, several of the mitigation measures recommended for other threats in this report could be employed as part of the following baseline mitigation controls[2]:

- Identify mission critical roles in the organisation and estimate their exposure to espionage risks. Evaluate such risks based on business information (i.e. business intelligence).
- Create security policies that accommodate human resource, business and operational security controls to cater for risk mitigation. These should include rules and practices for awareness raising, corporate governance and security operations.
- Establish corporate practices to communicate, train staff in the rules developed.
- Develop an evaluation criteria (KPIs) to benchmark the operation and adapt it to upcoming changes.
- Create a Whitelist for critical application services depending on the risk level assessed.
- Assess vulnerabilities and patch the software regularly, especially for systems that are on the perimeter.
- Implement the need-to-know principle for defining access rights and establish controls to monitor misuse of privileged profiles.
- Establish content filtering for all inbound and outbound channels (e.g. e-mail, web, network traffic).

References

1. “Cyber Threatscape Report. 2019.” IDefense - Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

2. “Data Breach Investigations Report 2020” DBR & Verizon. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report-emea.pdf

3. Catalin Cimpanu**.**“Hackers breach and steal data from South Korea's Defense Ministry” January 16, 2019. ZDNet. https://www.zdnet.com/article/hackers-breach-and-steal-data-from-south-koreas-defense-ministry/

4. Jack Stubbs.“China hacked Norway's Visma to steal client secrets: investigators” February 6, 2019. Reuters. https://www.reuters.com/article/us-china-cyber-norway-visma/china-hacked-norways-visma-to-steal-client-secrets-investigators-idUSKCN1PV141

5. Kate Fazzini. “In India-Pakistan conflict, there’s a long-simmering online war, and some very good hackers on both sides”. February 28, 2019. CNBC . ttps://www.cnbc.com/2019/02/27/india-pakistan-online-war-includes-hacks-social-media.html

6. Kati Pohjanpalo. “Finland Detects Cyber Attack on Online Election-Results Service”. April 10, 2019. Bloomberg.

https://www.bloomberg.com/news/articles/2019-04-10/finland-detects-cyber-attack-on-online-election-results-service

7. Lily Hay Newman “What Israel's Strike on Hamas Hackers Means For Cyberwar” June 5, 2019. Wired. https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/

8.”Egypt Is Using Apps to Track and Target Its Citizens, Report Says” October 3, 2019. The New York Times. https://www.nytimes.com/2019/10/03/world/middleeast/egypt-cyber-attack-phones.html

9. Colin Lencher.“Huawei accuses the US of ‘launching cyber attacks’ against the company“ September 4, 2019.The Verge. https://www.theverge.com/2019/9/4/20849092/huawei-cyberattacks-us-government-netowrks-employee-harassment

10. Catalin Cimpanu “A cyber-espionage group has been stealing files from the Venezuelan military” August 5, 2019. ZDNet. https://www.zdnet.com/article/a-cyber-espionage-group-has-been-stealing-files-from-the-venezuelan-military/

11. Catalin Cimpanu. “Croatian government targeted by mysterious hackers” July 5, 2019. ZDNet. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

12. Michael McGowan. “China behind massive Australian National University hack, intelligence officials say” June 6, 2019. The Guardian. https://www.theguardian.com/australia-news/2019/jun/06/china-behind-massive-australian-national-university-hack-intelligence-officials-say

13. “General election 2019: Labour Party hit by second cyber-attack” November 12, 2019. BBC. https://www.bbc.com/news/election-2019-50388879

14. Nicole Perlroth, Matthew Rosenberg**.** “Russians Hacked Ukrainian Gas Company at Center of Impeachment” January 13, 2020. The New York Times. https://www.nytimes.com/2020/01/13/us/politics/russian-hackers-burisma-ukraine.html

15. Danny Bradbury . “GE Engineer Charged for Novel Data Theft” April 24, 2019. Info Security. https://www.infosecurity-magazine.com/infosec/ge-engineer-charged-data-theft-1/

16. “U.S. announces disruption of ‘Joanap’ botnet linked with North Korea”. January 30, 2019. CyberScoop. https://www.cyberscoop.com/joanap-botnet-north-korea-department-of-justice/

17. “The cyber attack on Parliament was done by a 'state actor' — here's how experts figure that out”. February 20, 2019. ABC News. https://www.abc.net.au/news/2019-02-20/cyber-activists-or-state-actor-attack-how-experts-tell/10825466

18. “While Trump was meeting with Kim Jong Un in Vietnam, North Korean hackers reportedly attacked targets in the US”. March 5, 2019. Business Insider. https://www.businessinsider.com/north-korean-hackers-trump-kim-meeting-mcafee-2019-3

19. “Airbus hit by series of cyber attacks on suppliers”. September 26, 2019. France 24. https://www.france24.com/en/20190926-airbus-hit-by-series-of-cyber-attacks-on-suppliers

20. “Indonesia Says Election Under Attack From Chinese, Russian Hackers”. March 12, 2019. Bloomberg. https://www.bloomberg.com/news/articles/2019-03-12/indonesia-says-poll-under-attack-from-chinese-russian-hackers

21. “Cyber-espionage warning: Russian hacking groups step up attacks ahead of European elections”. March 21, 2019. ZDNet. https://www.zdnet.com/article/cyber-espionage-warning-russian-hacking-groups-step-up-attacks-ahead-of-european-elections/

22. “Australian cyber soldiers hacked Islamic State and crippled its propaganda unit – here's what we know”. December 18, 2019. ABC News. https://www.abc.net.au/news/2019-12-18/inside-the-secret-hack-on-islamic-state-propaganda-network/11809426

23. “State-sponsored hackers target Amnesty International Hong Kong with sophisticated cyber-attack”. April 25, 2019. Amnesty International. https://www.amnesty.org/en/latest/news/2019/04/state-sponsored-cyber-attack-hong-kong/

24. “New Report Shows How a Pro-Iran Group Spread Fake News Online”. Mary 14, 2019. The New York Times. https://www.nytimes.com/2019/05/14/world/middleeast/iran-fake-news-report.html

25. “China behind massive Australian National University hack, intelligence officials say”. June 6, 2019. The Guardian. https://www.theguardian.com/australia-news/2019/jun/06/china-behind-massive-australian-national-university-hack-intelligence-officials-say

26. “Croatian government targeted by mysterious hackers”. July 5, 2019. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

27. “Two Russians accused of election interference arrested in Libya”. July 8, 2019. Cyber Scout. https://cyberscout.com/en/blog/two-russians-accused-of-election-interference-arrested-in-libya

28. “BASF, Siemens, Henkel, Roche target of cyber attacks”. July 24, 2019. Reuters. https://www.reuters.com/article/us-germany-cyber/basf-siemens-henkel-roche-target-of-cyber-attacks-idUSKCN1UJ147

29. “New espionage malware found targeting Russian-speaking users in Eastern Europe” October 10, 2019. ZDNet. https://www.zdnet.com/article/new-espionage-malware-found-targeting-russian-speaking-users-in-eastern-europe/

30. “Advanced Israeli spyware is targeting Moroccan human rights activists”. November 2019. TheNextWeb. https://thenextweb.com/security/2019/10/14/advanced-israeli-spyware-is-targeting-moroccan-human-rights-activists/

31. “Hacking the hackers: Russian group hijacked Iranian spying operation, officials say”. October 21, 2019. Reuters. https://www.reuters.com/article/us-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUSKBN1X00AK

32. “Israeli spyware allegedly used to target Pakistani officials' phones”. December 19, 2019. The Guardian. https://www.theguardian.com/world/2019/dec/19/israeli-spyware-allegedly-used-to-target-pakistani-officials-phones

33. “A phishing campaign with nation-state hallmarks is targeting Chinese government agencies”. August 8, 2019.Cyber Scoop. https://www.cyberscoop.com/china-phishing-anomali-nation-state-apt/

34. “Foreign power was behind cyber attack on Czech ministry: Senate”. August 13, 2019. Reuters. https://www.france24.com/en/20190926-airbus-hit-by-series-of-cyber-attacks-on-suppliers

35. “Huawei technicians helped government officials in two African countries track political rivals and access encrypted communications.”. August 15, 2019. The Wall Street Journal. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017

36. “Labour suffers second cyber-attack in two days” November 12, 2019. The Guardian. https://www.theguardian.com/politics/2019/nov/12/labour-reveals-large-scale-cyber-attack-on-digital-platforms

37. “Extensive hacking operation discovered in Kazakhstan”. November 23, 2019. ZDNet. https://www.zdnet.com/article/extensive-hacking-operation-discovered-in-kazakhstan/

References

38. “A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems”. November 20, 2019. Wired. https://www.wired.com/story/iran-apt33-industrial-control-systems/

39. “Russian 'Gamaredon' Hackers Back at Targeting Ukraine Officials”. December 6, 2019. Security Week. https://www.securityweek.com/russian-gamaredon-hackers-back-targeting-ukraine-officials

40. “Iran announced it foiled ‘really massive’ foreign cyber attack”. December 11, 2019. Security Affairs. https://securityaffairs.co/wordpress/94981/cyber-warfare-2/iran-foreign-cyber-attack.html

41. “Croatian government targeted by mysterious hackers”. July 5, 2019. ZDNet. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

42. “Report on the implementation of the common foreign and security policy – annual report” December 18, 2019. EU Parliament. https://www.europarl.europa.eu/doceo/document/A-9-2019-0054_EN.html

43. “Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent”. September 26, 2012. Krebs on Security. https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information

44. “Energy Manufacturer Also Victimized by IE Zero Day in Watering Hole Attack”. January 2, 2013. The Threat Post. https://threatpost.com/energy-manufacturer-also-victimized-ie-zero-day-watering-hole-attack-010213/77359/

45. “The French Connection: French Aerospace-Focused CVE-2014-0322 Attack Shares Similarities with 2012 Capstone Turbine Activity”. February 25, 2014. CrowdStrike Blog. https://www.crowdstrike.com/blog/french-connection-french-aerospace-focused-cve-2014-0322-attack-shares-similarities-2012/

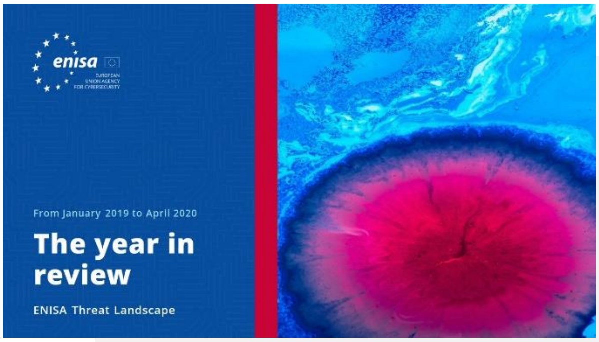
46. “Advanced Persistent Threat Groups”. Fireeye. https://www.fireeye.com/current-threats/apt-groups.html

47. “U.S. accuses pair of stealing secrets, spying on GE to aid China”. April 23, 2019. Reuters. https://www.reuters.com/article/us-usa-justice-ge/us-accuses-pair-of-stealing-secrets-spying-on-ge-to-aid-china-idUSKCN1RZ24O

“The number of nation-state sponsored cyberattacks targeting the economy increased during 2019.”

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

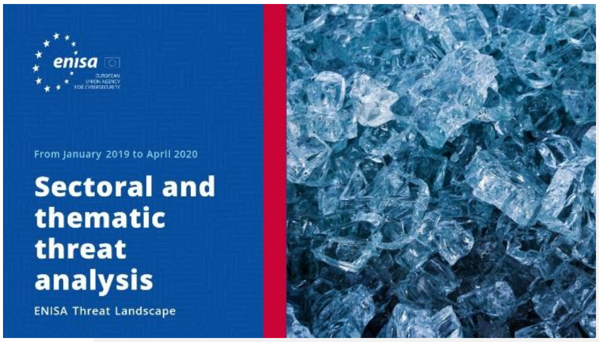
Research topics

ENISA Threat Landscape

READ THE REPORT

ENISA Threat Landscape Report **Research topics**

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


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.

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.

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 cyber threat 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