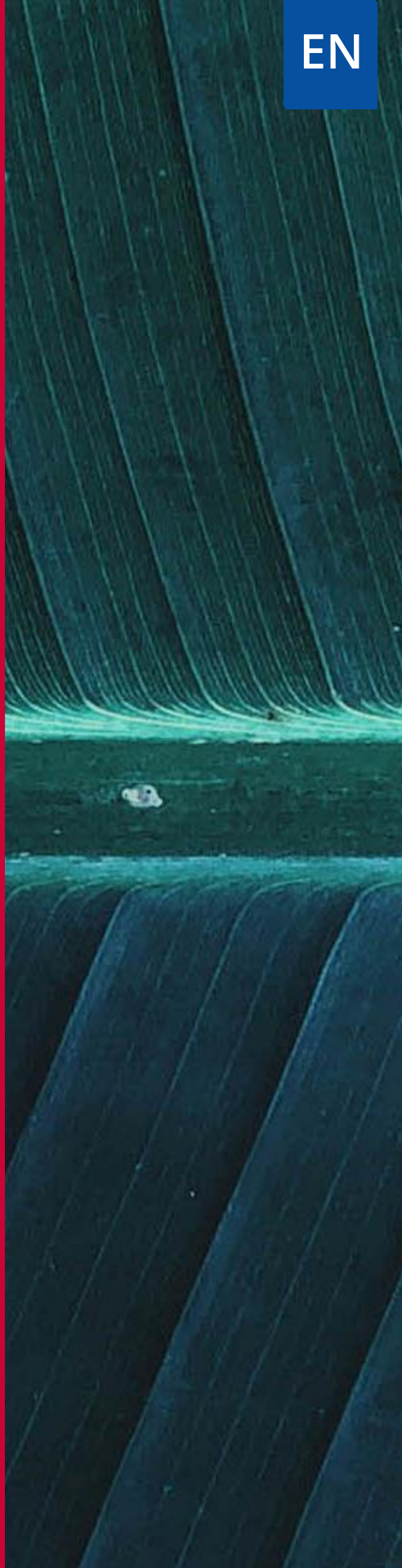
EN

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY



From January 2019 to April 2020

Spam

ENISA Threat Landscape

Overview

The first spam message was sent in 1978 by a marketing manager to 393 people via ARPANET. It was an advertising campaign for a new product from the company he worked for, the Digital Equipment Corporation. For those first 393 spammed people it was as annoying as it would be today, regardless of the novelty of the idea.[1] Receiving spam is an inconvenience, but it may also create an opportunity for a malicious actor to steal personal information or install malware.[2] Spam consists of sending unsolicited messages in bulk. It is considered a cybersecurity threat when used as an attack vector to distribute or enable other threats.

Another noteworthy aspect is how spam may sometimes be confused or misclassified as a phishing campaign. The main difference between the two is the fact that phishing is a targeted action using social engineering tactics, actively aiming to steal users' data. In contrast spam is a tactic for sending unsolicited e-mails to a bulk list. Phishing campaigns can use spam tactics to distribute messages while spam can link the user to a compromised website to install malware and steal personal data.

Spam campaigns, during these last 41 years have taken advantage of many popular global social and sports events such as UEFA Europa League Final, US Open, among others. Even so, nothing compared with the spam activity seen this year with the COVID-19 pandemic.[8]

Findings

85%_ **of all e-mails exchanged in April 2019 were spam, a 15-month high[1]**

14_ **million sextortion-related spam e-mails were detected in 2019[23]**

58.3%_ **of e-mail accounts in the mining industry were spammed[17]**

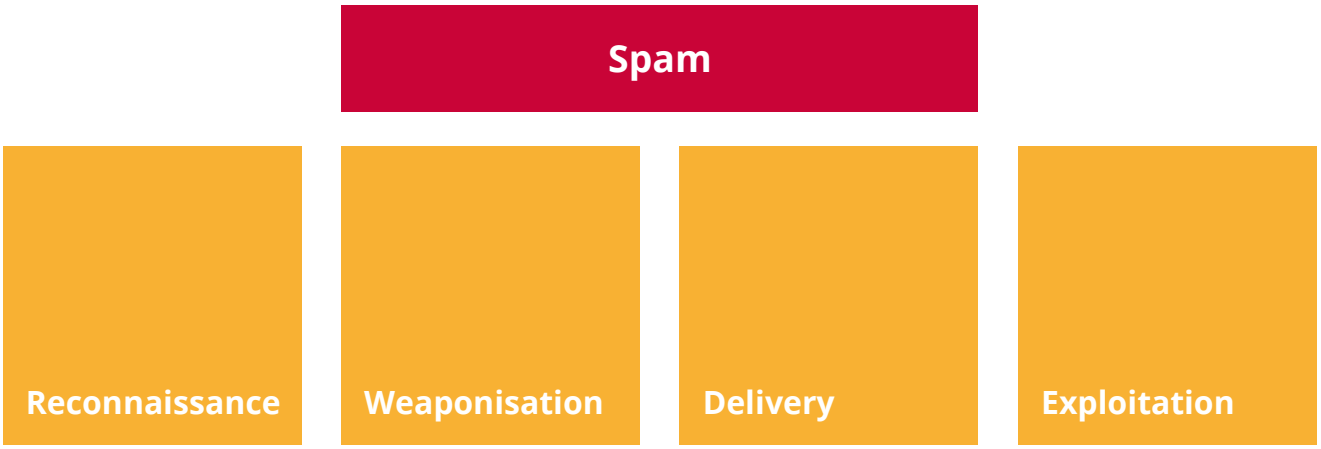
10%_ **of overall spam detections were targeting German e-mail accounts[2,3]**

13%_ **of data breaches were caused by malicious spam[16]**

83%_ **of companies were unprotected against e-mail-based brand impersonation[20]**

42%_ **of Chief Information Security Officers (CISOs) dealt with at least one spam-resulted security incident[1]**

Kill chain



Step of Attack Workflow

Width of Purpose

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

_Old head on young shoulders

After 41 years of existence, spam remains a notable security threat, despite all the others that are much more effective. However, once again in the reporting period, new target groups, new means and new spoils appeared in spamming campaigns. For instance, in August 2019, spam e-mails targeted multiple accounts encouraging their owners to share not only a scan of their identity but also a selfie so that they would 'win' a free smartphone device. In another spam campaign, users were asked to send a personal photo. The spammers' target group was then expanded to include the e-mail address used by the user, to activate paid TV or live broadcast services. Those accounts were spammed with fake licence expiry or renewal messages. The users were asked to reply and enter their bank account details and personal information to renew their registration.[2]

_Spamming to serve malware, ransomware and remote access trojans

In August 2019, spam e-mails containing malicious ISO disk image files were used to spread the LokiBot malware and to drop the remote access trojan (RAT) FlawedAmmyy. Spamming was also used to spread the TrickBot trojan, the Negasteal (also known as Agent Tesla) trojanspy, the Ave Maria (also known as Warzone) RAT and the notorious, since 2018, Pawload macro malware. Several ransomware families were also spread by spam messages, such as Dharma, Crysis and Ryuk, all of which were reported to be highly active in the reporting year.[15,21]

_Spam SMS

This year a SMS spam operation was carried out exposing more than 80 million users' personal data. A large number of phone numbers received messages containing certain phrases such as 'free money' or 'for real' and links to fake sites. From that point onwards, anyone that followed the link would be called on to sign up, giving away sensitive information. It was proved that the database used by the spammers was owned by the ApexSMScompany, the legitimacy of which is still unknown. Although security researchers accessed the database and tried to retrieve as much information as possible fearing that the operation would stop unexpectedly, it is still not known who and for what reason may access and use this data as it is still available.[4]

_Forms were the means

Spammers manipulated feedback forms on the websites of large companies used to ask questions, express wishes or subscribe to newsletters. However, in this reporting year, instead of spamming the company's linked mailboxes, the spammers exploited low levels of website security, bypassed any reCAPTCHA tests and registered multiple accounts with valid e-mail information. As a result, victims received a legitimate reply from the company, including the spammer's message.[2] In this way, even Google Forms was manipulated to retrieve user data and send commercial spam. A more aggressive case was the spam attack targeting company accounts, requesting that money be transferred to the attacker. To convince the victim, the spammers claimed to be able to send abusive messages in the victim's e-mail to more than 9 million e-mail addresses, blacklisting the company's e-mail address.[3]

Description

Chameleon spam

Various campaigns in 2019 used the same botnet system to distribute spam messages, although they used random headers and templates to format the content. For that reason, security researchers started studying these campaigns as one group under the alias 'Chameleon spam'.[5]

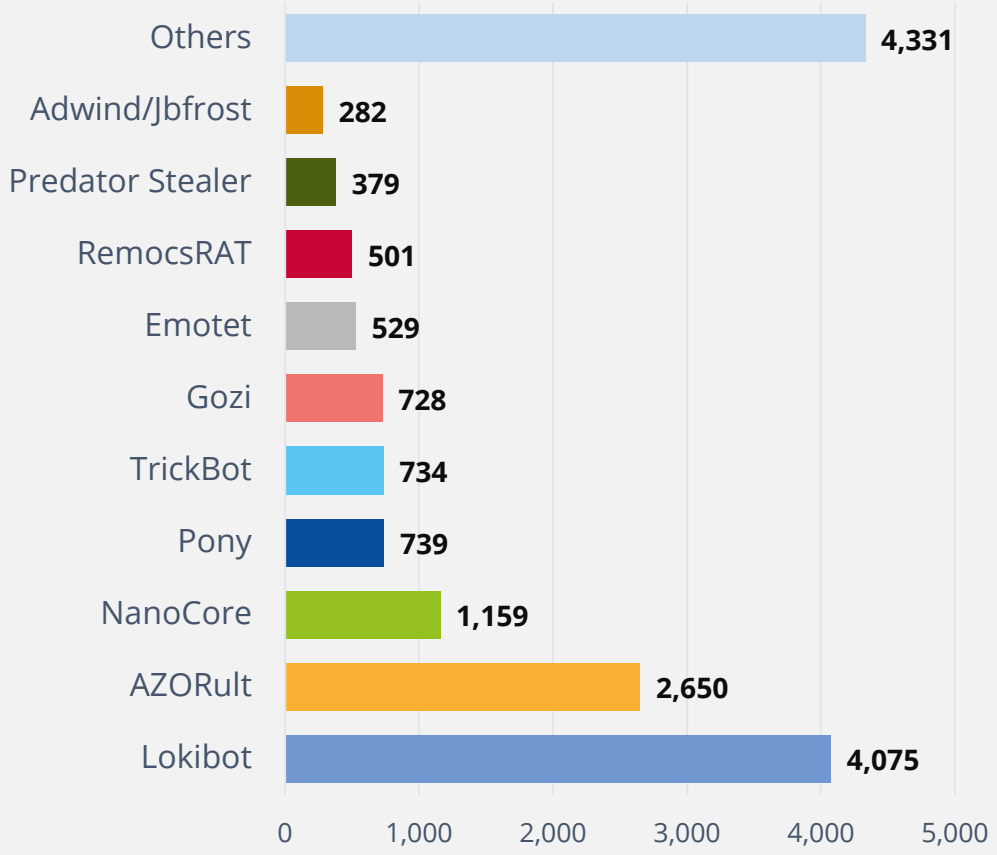
Chameleon spam messages originated from various countries and included fake links to fake job postings or job offers, airline ticket booking sites, special offers on purchasing products or even simple well-known services. These spam messages used a template similar to those used by valid companies such as Google, Qatar Airways, FedEx, LinkedIn or Microsoft so that the recipient would not notice the difference.[2]

As tough as old bots

In October 2019, e-mails using templates in English, German, Italian and Polish with the common subject 'Payment Remittance Advice' were widely distributed. These messages included an attached document containing a macro and recipients were asked to enable it upon opening the document. Once enabled, the macro could start the infection process by attempting to download the Emotet trojan.[13]

The Necurs spam botnet was very active during this period after a long time of little activity. The Gamut botnet was the third most active spam botnet in 2019. Gamut messages are mostly related to suggestions for dating or meeting people, offers of pharmaceutical products and job opportunities.[1]

_Number of botnets C2s associated with malware families

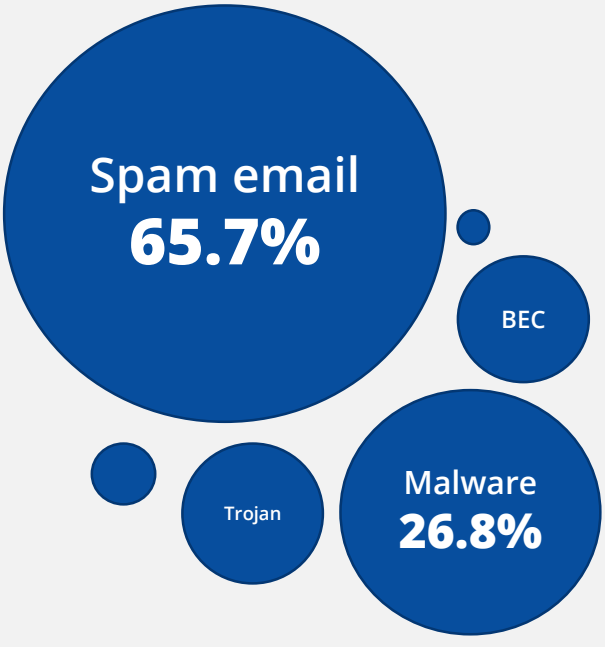


Source: Spamhaus [14]

Description

_ COVID-19 opened new doors

Soon after the start of the COVID-19 outbreak, phishing websites and malicious files delivered by e-mail appeared, using the terms coronavirus or COVID-19. A COVID-19 spamming campaign was reported to be spreading the Eeskiri-COVID.chm19, a disguised keyloggerfile. The name of the file may suggest that the campaign originated in Estonia (i.e. eeskirimeans 'rule' in Estonian).[11] In mid-February 2020 only a few hundred COVID-19 attacks per day were recorded, but by March 2020 more than 2.500 attacks were taking place every day, promising a hard year spam-wise.[12]



Threats leveraging from COVID-19 . Source: Trend Micro[11]

_ Examples

01_ The ApexSMS spam operation

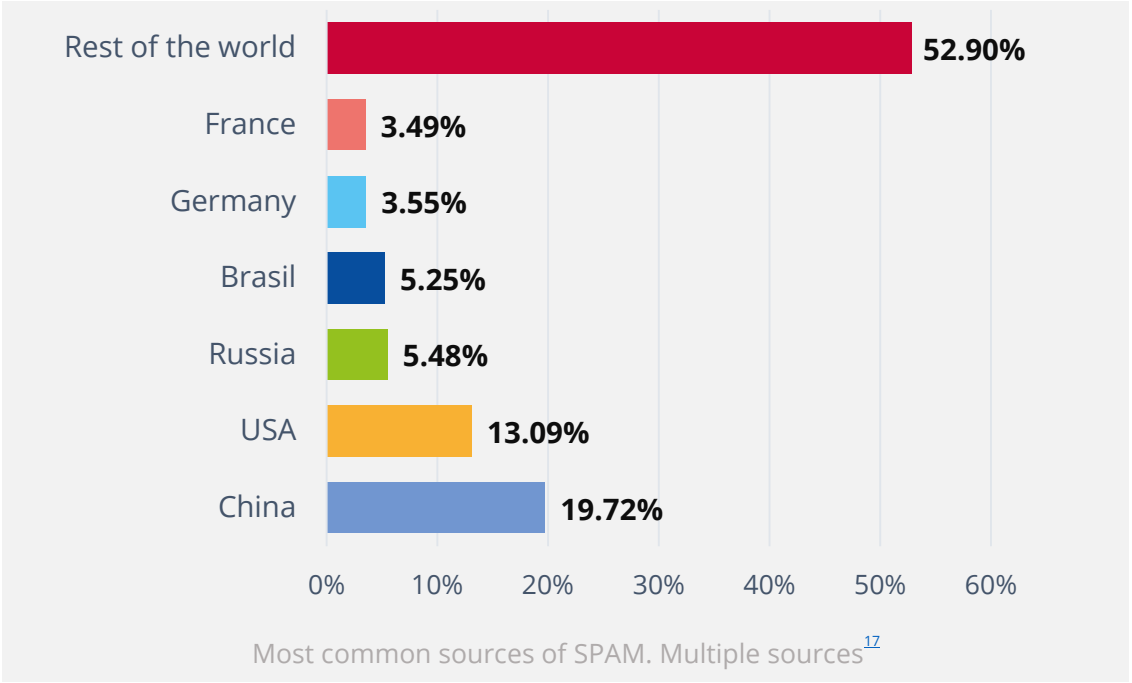
ApexSMS, an SMS marketing company suffered a data breach exposing the contact details of more than 80 million people.

02_ The Chameleon spam campaign

A persistent high-volume spam campaign emanated from a botnet system sending messages with randomized headers and often changing the template.

03_ Emotet spam distribution campaign

A spam campaign supporting the distribution of Emotet malware.



Most common sources of SPAM. Multiple sources[17]

Mitigation

Proposed actions

- Implement content filtering to locate unwanted attachments, mails with malicious content, spam and unwanted network traffic.
- Regular update the hardware, firmware, operating system and any drivers or software.
- Use multi-factor authentication to access e-mail accounts.
- Avoid money transfers to unverified bank accounts.
- Avoid logging into new links received in e-mails or SMS messages.
- Develop standard operating procedures and policies for handling sensitive data.
- Use a secure e-mail gateway with, if possible, regular and automated maintenance of filters (anti-spam, anti-malware, policy-based filtering).
- Disable automatic code execution, macro enabling and preloading of graphics and mailed links.
- Implement security techniques such as the sender policy framework (SPF), domain-based message authentication, reporting & conformance (DMARC), and the domain keys identified mail (DKIM).
- Regularly update whitelists, reputation filters and the real-time blackholeList (RBS).
- Use AI and machine learning for anomaly detection checks.

“Phishing campaigns can use spam tactics to distribute messages while spam can link the user to a compromised website to install malware to steal personal data.”

in ETL 2020

References

1. "Email: Click with Caution - How to protect against phishing, fraud, and other scams" June, 2019. Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf

2. "Spam and phishing in Q3 2019" November 26, 2019. Kaspersky. https://securelist.com/spam-report-q3-2019/95177/

3. "Spam and phishing in Q2 2019" August 28, 2019. Kaspersky. https://securelist.com/spam-and-phishing-in-q2-2019/92379/

4. "SMS Spammers Doxxed" May 9, 2019. Tech Crunch. https://techcrunch.com/2019/05/09/sms-spammers-doxxed/

5. "Tracking the Chameleon Spam Campaign" September 25, 2019. Trustwave. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/tracking-the-chameleon-spam-campaign/

6. "5 Biggest Cyberattacks of 2019 (So Far) and Lessons Learned" June 7, 2019. Gordon Flesch. https://www.gflesch.com/blog/biggest-cyberattacks-2019

7. "The world worst spammers". 2019. Spamhaus. https://www.spamhaus.org/statistics/spammers/

8. "Naming the coronavirus disease (COVID-19) and the virus that causes it". 2020. WHO. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it

9. "WHO Director-General's opening remarks at the media briefing on 2019 novel coronavirus" February 6, 2020. WHO. https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-2019-novel-coronavirus/

10. "COVID-19 situation update worldwide, as of 11 June 2020" 2020. ECDC. https://www.ecdc.europa.eu/en/geographical-distribution-2019-ncov-cases

11. "Developing Story: COVID-19 Used in Malicious Campaigns" April 24, 2020. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

12. "2019 Novel Coronavirus and COVID-19 Themed Attacks Dominate Threat Landscape" April 6, 2020. HIPAA Journal. https://www.hipaajournal.com/2019-novel-coronavirus-and-covid-19-themed-attacks-dominate-threat-landscape/

13. "Emotet is back: botnet springs back to life with new spam campaign" September 16, 2019. Malwarebytes Lab. https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/

14. "Spamhaus Botnet Threat Report 2019" January 28, 2020. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

15. "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

16. "Anticipating the Unknowns: 2019 Cisco CISO Benchmark Study" February 28, 2019. Cisco. https://blogs.cisco.com/security/anticipating-the-unknowns-2019-cisco-ciso-benchmark-study

17. "Internet Security Threat Report" Volume 24, Feburary 2019. Broadcom. https://docs.broadcom.com/doc/istr-24-2019-en

18. "Spam and phishing in Q1 2019" May 5, 2019. Kaspersky. https://securelist.com/spam-and-phishing-in-q1-2019/90795/

19. "Total Global Email & Spam Volume for May 2020" May, 2019. Talos. https://talosintelligence.com/reputation_center/email_rep#global-volume

20. "Q3 2019: Email Fraud and Identity Deception Trends" June, 2019. Agari. https://www.agari.com/insights/ebooks/2019-q3-report/

21. "The World's Most Abused TLDs" Spamhaus. https://www.spamhaus.org/statistics/tlds/

22. "Trend Micro Cloud App Security Report 2019" March 10, 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/trend-micro-cloud-app-security-report-2019

23. "The Sprawling Reach of Complex Threats". 2019. Trend Micro Research. https://documents.trendmicro.com/assets/rpt/rpt-the-sprawling-reach-of-complex-threats.pdf

24. "SONIC WALL Security Center Metrics". SONIC WALL. https://securitycenter.sonicwall.com/m/page/capture-labs-threat-metrics

Related

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.

READ THE REPORT

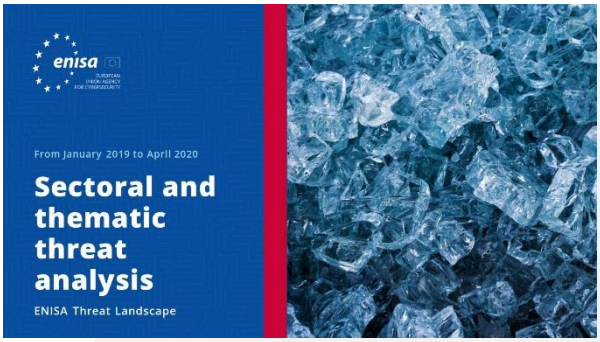
ENISA Threat Landscape Report
List of Top 15 Threats

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

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

Contextualised threat analysis 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

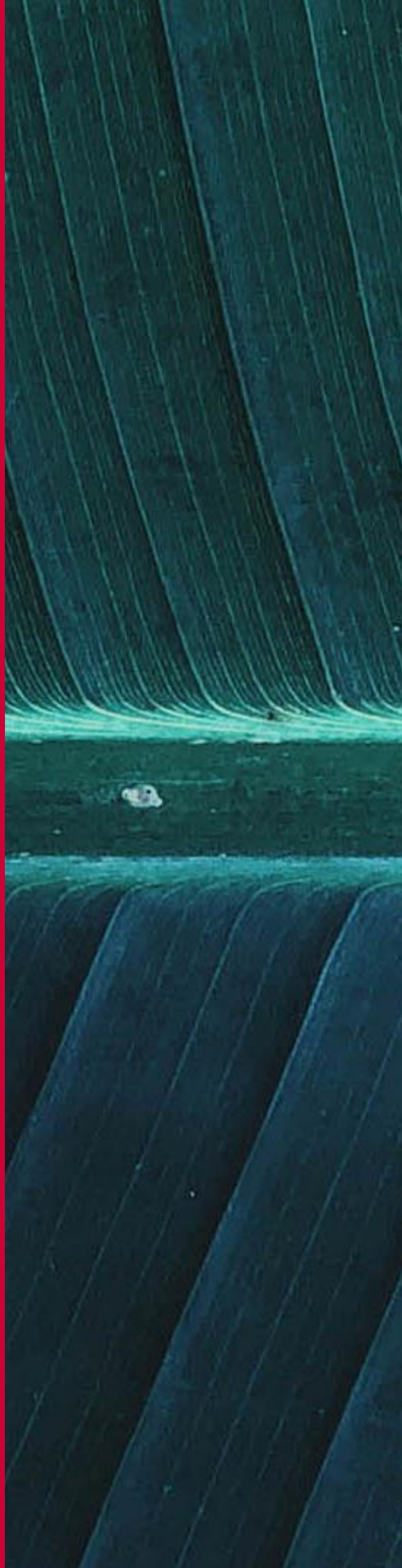
Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily 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