



Von Januar 2019 bis April 2020

Liste der 15 größten Bedrohungen

ENISA Threat Landscape



Die größten Bedrohungen



ENISA Threat Landscape Bericht

Nr. 1 Malware

Analyse und Trends der Malware-Bedrohung zwischen Januar 2019 und April 2020. Malware belegte in der Bedrohungslandschaft den 1. Platz und behält diese Position seit 2018 bei.

LESEN SIEDENBERICHT



ENISA Threat Landscape Bericht

Nr. 2 Webbasierte Angriffe

Trendanalyse webbasierter Angriffe zwischen Januar 2019 und April 2020. Webbasierte Angriffe belegten in der Bedrohungslandschaft den 2. Platz und behielten diese Position seit 2018 bei.

LESEN SIEDENBERICHT



ENISA Threat Landscape Bericht

Nr. 3 Phishing

Trendanalyse der Bedrohung durch Phishing zwischen Januar 2019 und April 2020. Phishing-Angriffe belegten in der Bedrohungslandschaft den 3. Platz und stiegen somit vom im Jahr 2018 belegten 4. Platz auf.

LESEN SIEDENBERICHT





ENISA Threat Landscape Bericht **Nr. 4** Angriffe über Webanwendungen

Analyse und Trends in Bezug auf Webanwendungsangriffe zwischen Januar 2019 und April 2020. Angriffe über Webanwendungen belegten in der Bedrohungslandschaft den 4. Platz und stiegen somit vom im Jahr 2018 belegten 3. Platz ab.

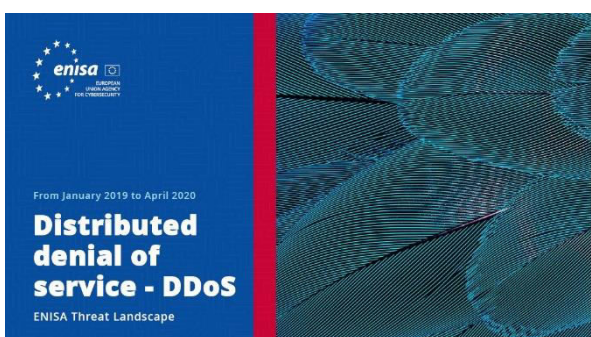
LESEN SIEDENBERICHT



ENISA Threat Landscape Bericht **Nr. 5** Spam

Trendanalyse von Spam-Angriffen zwischen Januar 2019 und April 2020. Spam belegte in der Bedrohungslandschaft den 5. Platz und stieg somit vom im Jahr 2018 belegten 6. Platz auf.

LESEN SIEDENBERICHT



ENISA Threat Landscape Bericht **Nr. 6** DDoS

Trendanalyse von DDoS-Angriffen zwischen Januar 2019 und April 2020. DDoS-Angriffe belegten in der Bedrohungslandschaft den 6. Platz und stiegen somit vom im Jahr 2018 belegten 5. Platz ab.

LESEN SIEDENBERICHT

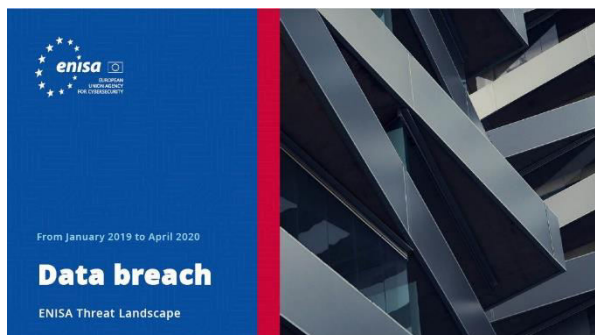
Die größten Bedrohungen



LESEN SIEDENBERICHT

ENISA Threat Landscape Bericht **Nr. 7** Identitätsdiebstahl

Analyse und Trends des Identitätsdiebstahls zwischen Januar 2019 und April 2020. Identitätsdiebstahl belegte in der Bedrohungslandschaft den 7. Platz und stieg somit vom im Jahr 2018 belegten 13. Platz auf.



LESEN SIEDENBERICHT

ENISA Threat Landscape Bericht **Nr. 8** Datenschutzverletzung

Trendanalyse von Datenschutzverletzungen zwischen Januar 2019 und April 2020. Datenschutzverletzungen belegten in der Bedrohungslandschaft den 8. Platz und behielten diese Position seit 2018 bei.

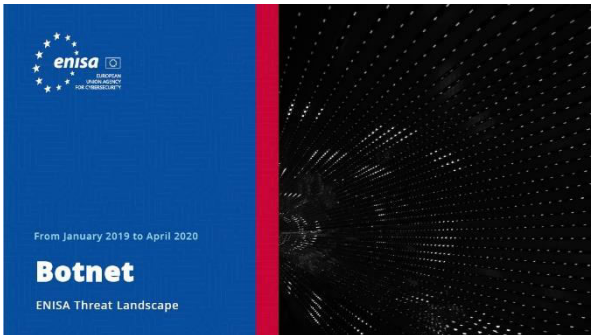


LESEN SIEDENBERICHT

ENISA Threat Landscape Bericht **Nr. 9** Insiderbedrohung

Trendanalyse der Insiderbedrohung zwischen Januar 2019 und April 2020. Insiderbedrohungen belegten in der Bedrohungslandschaft den 9. Platz und behielten diese Position seit 2018 bei.





LESEN SIE DEN BERICHT



ENISA Threat Landscape Bericht

Nr. 10 Botnetze

Analyse und Trends in Bezug auf Botnetz-Angriffe zwischen Januar 2019 und April 2020. Botnetz-Angriffe belegten in der Bedrohungslandschaft den 10. Platz und stiegen somit vom im Jahr 2018 belegten 7. Platz ab.



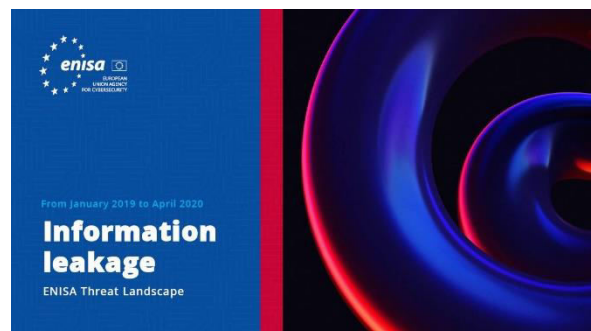
LESEN SIE DEN BERICHT



ENISA Threat Landscape Bericht

Nr. 11 Physische Manipulation, Beschädigung, Diebstahl und Verlust

Physische Manipulation, Beschädigung, Diebstahl und Verlust belegten in der Bedrohungslandschaft den 11. Platz und stiegen somit vom im Jahr 2018 belegten 10. Platz ab.



LESEN SIE DEN BERICHT



ENISA Threat Landscape Bericht

Nr. 12 Informationslecks

Trendanalyse über Informationslecks zwischen Januar 2019 und April 2020. Angriffe über Informationslecks belegten in der Bedrohungslandschaft den 12. Platz und stiegen somit vom im Jahr 2018 belegten 11. Platz ab.

Die größten Bedrohungen



ENISA Threat Landscape Bericht **Nr. 13** Ransomware

Analyse und Trends in Bezug auf Ransomware zwischen Januar 2019 und April 2020. Ransomware belegte in der Bedrohungslandschaft den 13. Platz und stieg somit vom im Jahr 2018 belegten 14. Platz auf.

LESEN SIEDENBERICHT



ENISA Threat Landscape Bericht **Nr. 14** Cyberespionage

Trendanalyse von Cyberespionage zwischen Januar 2019 und April 2020. Cyberespionage belegte in der Bedrohungslandschaft den 14. Platz und stieg somit vom im Jahr 2018 belegten 15. Platz auf.

LESEN SIEDENBERICHT



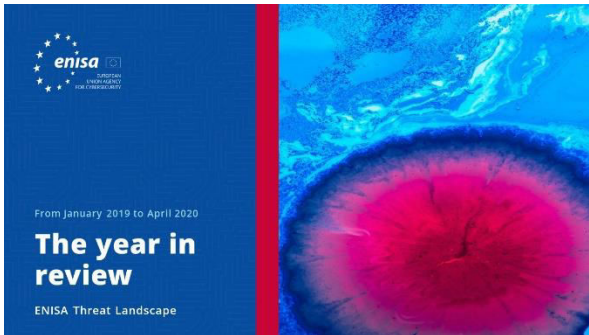
ENISA Threat Landscape Bericht **Nr. 15** Cryptojacking

Trendanalyse von Cryptojacking zwischen Januar 2019 und April 2020. Cryptojacking-Angriffe belegten in der Bedrohungslandschaft den 15. Platz und stiegen somit vom im Jahr 2018 belegten 13. Platz ab.

LESEN SIEDENBERICHT

„Im nächsten Jahrzehnt werden Cybersicherheitsrisiken aufgrund der zunehmenden Komplexität der Bedrohungslandschaft, des kontroversen Ökosystems und der Erweiterung der Angriffsfläche schwieriger zu bewerten und zu interpretieren sein.“

Themenbezogen



ENISA Threat Landscape Bericht Das Berichtsjahr

Eine Zusammenfassung der Cybersicherheitstrends für den Zeitraum zwischen Januar 2019 und April 2020.

[LESENSIEDENBERICHT](#)



ENISA Threat Landscape-Bericht Hauptvorfälle in der EU und weltweit

Die bedeutendsten Cybersicherheitsvorfälle zwischen Januar 2019 und April 2020.

[LESENSIEDENBERICHT](#)

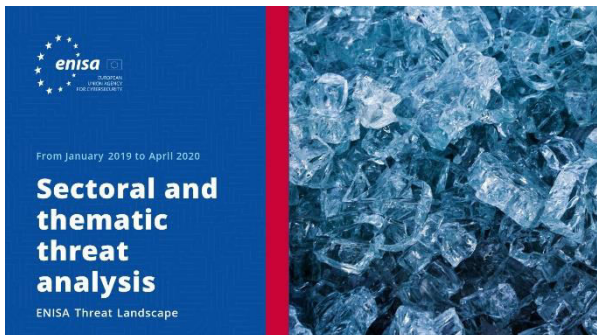


ENISA Threat Landscape Bericht Forschungsthemen

Empfehlungen zu Forschungsthemen aus verschiedenen Quadranten der Cybersicherheit und Cyber Threat Intelligence.

[LESENSIEDENBERICHT](#)





LESEN SIE DEN BERICHT



ENISA Threat Landscape-Bericht Sektorale und thematische Bedrohungsanalyse

Kontextualisierte Bedrohungsanalyse zwischen Januar 2019 und April 2020.



LESEN SIE DEN BERICHT



ENISA Threat Landscape Bericht Aufkommende Trends

Die bedeutendsten Cybersicherheitstrends, die zwischen Januar 2019 und April 2020 beobachtet wurden.



LESEN SIE DEN BERICHT



ENISA Threat Landscape Bericht Übersicht über Cyber Threat Intelligence

Der aktuelle Stand der Cyber Threat Intelligence in der EU.

Die Agentur

Die Agentur der Europäischen Union für Cybersicherheit, ENISA, hat die Aufgabe, zu einer hohen Cybersicherheit innerhalb der Union beizutragen. Die Agentur der Europäischen Union für Cybersicherheit wurde 2004 gegründet und durch das EU-Gesetz zur Cybersicherheit gestärkt. Sie trägt zur Unionspolitik im Bereich der Cybersicherheit bei, erhöht die Vertrauenswürdigkeit von ICT-Produkten, -Dienstleistungen und -Prozessen durch Programme für die Cybersicherheitszertifizierung, kooperiert mit den Mitgliedstaaten und Organen der EU und unterstützt Europa dabei, sich den künftigen Herausforderungen im Bereich der Cybersicherheit zu stellen. Durch Wissensaustausch, Aufbau von Fähigkeiten und Sensibilisierung in Bezug auf Cybersicherheit arbeitet die Agentur gemeinsam mit ihren wichtigsten Interessenträgern darauf hin, das Vertrauen in die vernetzte Wirtschaft zu stärken, die Infrastruktur der Union abwehrfähiger zu machen und schließlich ein sicheres digitales Umfeld für die Gesellschaft und die Bürger Europas zu gewährleisten. Weitere Informationen über die ENISA und ihre Arbeit finden Sie unter www.enisa.europa.eu.

Mitwirkende

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) und *alle Mitglieder der ENISA CTI Interessenvertreter*: Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) und Thomas Hemker.

Herausgeber

Marco Barros Lourenço (ENISA) und Louis Marinos (ENISA).

Kontaktangaben

Für Fragen über dieses Dokument, verwenden Sie bitte enisa.threat.information@enisa.europa.eu.

Für Medienanfragen zu dieser Stellungnahme verwenden Sie bitte die folgenden Kontaktangaben: press@enisa.europa.eu.



Wir würden gerne Ihr Feedback zu diesem Bericht erhalten!

Bitte nehmen Sie sich einen Moment Zeit, um den Fragebogen auszufüllen. Um das Formular zu öffnen, können Sie [hier](#) klicken.



Impressum/Rechtshinweise

Sofern nichts anderes angegeben ist, gibt diese Veröffentlichung die Ansichten und Auslegungen der ENISA wieder. Diese Veröffentlichung ist nicht als eine Maßnahme der ENISA oder ihrer Gremien auszulegen, sofern sie nicht gemäß der Verordnung (EU) Nr. 526/2013 angenommen wurde. Diese Veröffentlichung entspricht nicht unbedingt dem neuesten Stand und kann in angemessenen Abständen aktualisiert werden.

Quellen von Dritten werden zitiert, sofern erforderlich. Die ENISA haftet nicht für den Inhalt der externen Quellen, einschließlich externer Websites, auf die in dieser Veröffentlichung verwiesen wird.

Die vorliegende Veröffentlichung ist nur für Informationszwecke gedacht. Sie muss kostenlos zugänglich sein. Weder die ENISA noch in deren Namen oder Auftrag tätige Personen können für die Nutzung der in dieser Veröffentlichung enthaltenen Informationen haftbar gemacht werden.

Hinweis zum Copyright

© European Union Agency for Cybersecurity (ENISA), 2020 Die Vervielfältigung ist gestattet, sofern die Quelle angegeben ist.

Copyright für das Bild auf dem Cover: © Wedia. Bei Verwendung oder Wiedergabe von Fotos oder sonstigem Material, das nicht dem Urheberrecht der ENISA unterliegt, muss die Zustimmung direkt bei den Urheberrechtsinhabern eingeholt werden.

ISBN: 978-92-9204-354-4

DOI: 10.2824/552242



Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Griechenland

Tel.: +30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu



Alle Rechte vorbehalten. Copyright ENISA 2020.

<https://www.enisa.europa.eu>

