DE

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Von Januar 2019 bis April 2020

Crypto-jacking

ENISA Threat Landscape

Überblick

Cryptojacking (auch als Cryptomining bezeichnet) ist die unbefugte Verwendung der Ressourcen eines Geräts, um nach Online-Geld (Kryptowährung) zu schürfen oder zu „minen“. Zu den Zielen gehören alle angeschlossenen Geräte wie Computer und Mobiltelefone. Cyberkriminelle zielen jedoch zunehmend auf Cloud-Infrastrukturen ab.[1] Diese Art von Angriff hat bei den Strafverfolgungsbehörden nicht viel Aufmerksamkeit erregt und ihr Missbrauch wird selten gemeldet[2], vor allem, weil es relativ wenig negative Folgen mit sich bringt. Dennoch können Unternehmen höhere IT-Kosten, verschlechterte Computerkomponenten, erhöhten Stromverbrauch und verringerte Mitarbeiterproduktivität feststellen, die durch langsamere Arbeitsplätze verursacht werden.[3]

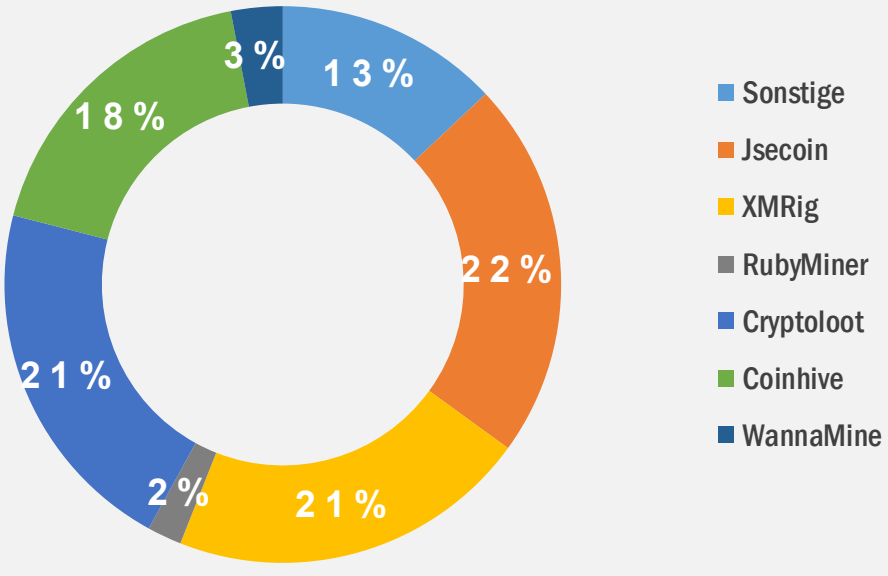


Abbildung 1: Top Cryptomining Malware weltweit. Quelle: Check Point[9]

Erkenntnisse

64,1_Millionen Cryptojacking-Fälle bis Ende 2019

78 %_Rückgang der Cryptojacking-Aktivitäten in der zweiten Hälfte des Jahres 2019 im Vergleich zur ersten Hälfte

Die Aktivitäten nahmen im ersten Halbjahr 2019 gegenüber den vorangegangenen 6 Monaten des Jahres 2018 um 9 % zu.[4,5]

65 %_der 120 beliebtesten Börsen im dritten Quartal 2019 wiesen schwache oder durchlässige KYC-Prozesse (Know Your Customer) auf

32 % der Börsen handelten mit Privacy Coins.[6]

39,3 %_der Crypto-Mining-Infektionen im Jahr 2019 betrafen Japan.

20,8 % der Crypto-Mining-Infektionen betrafen Indien und 14,2 % Taiwan. Abbildung 1 zeigt die fünf Länder mit den am häufigsten erkannten Malware-Infektionsversuchen von Cryptocurrency Miner für die Jahre 2018 und 2019.[7]

13 %_der Cryptojacking-Vorfälle werden auf trojan.Win32.Miner.bbb zurückgeführt

Im Zeitraum von November 2018 bis Oktober 2019 waren die am nächsten aktiven Miner Trojan.Win32.Miner.ays (11,35 %) und Trojan.JS.Miner.m (11,12 %).[6]

Kill chain

Cryptojacking

Ausspähung	Wappnung	Lieferung	Betreibung

Schritt des Angriffs-Workflows

Umfang des Zwecks

Cryptojacking

Installation	Command & Control	Zielführende Maßnahmen

Das Cyber Kill Chain® Framework wurde von Lockheed Martin entwickelt und basiert auf einem militärischen Konzept, das mit der Struktur eines Angriffs zusammenhängt. Um einen bestimmten Angriffsvektor zu untersuchen, verwenden Sie dieses Kill-Chain-Diagramm, um jeden Schritt des Prozesses sowie die vom Angreifer verwendeten Hilfsmittel, Techniken und Verfahren festzuhalten.

WEITERE INFORMATIONEN

Entwicklungen

_Beliebter Cryptomining-Service Coinhive geschlossen

Coinhive startete im September 2017 und bewarb sich als alternative Einnahmequelle für Webentwickler anstelle von Bannerwerbung.[24] Es wurden JavaScript-Bibliotheken verwendet, die auf Websites installiert werden konnten, sowie die Verarbeitungsleistung des Besuchers, um die Kryptowährung legitim abzubauen. Bis zu seiner Schließung im März 2019 wurde es von Bedrohungsakteuren, die Code in gehackte Websites injizierten, um die Monero-Kryptowährung abzubauen und Gelder in ihre eigenen Taschen umzuleiten, in hohem Maße missbraucht. Nach seiner Schließung ging das Volumen der webbasierten Cryptojacking-Treffer in der zweiten Jahreshälfte 2019 um 78 % zurück.[4] Infolge dieses Rückgangs konzentrierten sich Cyberkriminelle auf höherwertige Ziele wie leistungsstarke Server[9] und Cloud-Infrastrukturen.[1] Coinhives Platz an der Spitze wurde seitdem von Jsecoin (22 %), XMRig (21 %) und Cryptoloot (21 %) eingenommen. Die weltweite Verbreitung von Top-Cryptomining-Malware ist in Abbildung 1 dargestellt.

_Weitere Angriffe auf Cloud-Infrastrukturen

In der ersten Jahreshälfte 2019 war ein zunehmender Trend in Bezug auf Vorfälle von Kryptowährung-Mining-Angriffen auf die Cloud zu beobachten.[15,25] Cloud-Umgebungen verwenden normalerweise Mechanismen, die Ressourcen bei Bedarf anpassen und daher lukrative Ziele für die Ausführung von Mining-Software sind. Dies geht jedoch zu Lasten der Website-Eigentümer, die wiederum höhere Rechnungen für die Überschreitung von Quoten bezahlen müssen.[15] Im ersten Halbjahr 2019 nahmen die Sicherheitslücken in Cloud-Container-Software gegenüber dem Vorjahreszeitraum um 46 % zu.[26] Angreifer nutzten erfolgreich Anwendungsprogrammierschnittstellen (APIs) und Containerverwaltungsplattformen, um schädliche Images (z. B. Docker und Kubernetes) zu installieren und Kryptowährungen abzubauen.[25]

Störfälle

April 2019_ **Die Cryptojacking-Kampagne namens Beapy nutzte die Sicherheitslücke von EternalBlue aus und infizierte Unternehmen in China**[3]

Mai 2019_ **Die Monero-Mining-Malware PCASTLE zielte hauptsächlich auf Systeme in China ab, indem es die Technik der dateilosen Eingänge einsetzte**[19]

Es wurde festgestellt, dass mehr als 50.000 Server von Unternehmen aus den Bereichen Gesundheitswesen, Telekommunikation, Medien und IT durch Malware infiziert waren, die die TurtleCoin (TRTL)-Kryptowährung abbauen.[20]
Eine neue Malware-Familie namens BlackSquid nutzte acht bekannte Exploits, darunter EternalBlue und DoublePulsar, und verbreitete sich anschließend auf Webservern in Thailand und den USA, um Monero-Mining-Skripte bereitzustellen.[17,21]

August 2019_ **Cryptojacking-Malware in 11 RubyGem-Sprachablagen, die Tausende von Benutzern dem Cryptomining-Code aussetzen**[22]

Entwicklungen

Verschiebung hin zu dateibasiertem Cryptomining

Im Jahr 2019 wurde ein Rückgang des browserbasierten Cryptojacking zugunsten des dateibasierten Cryptomining festgestellt. Dateibasierte Cryptomining[27]-Angriffe verbreiteten sich über Malware und nutzten bereits vorhandene Exploits auf nicht gepatchten Betriebssystemen wie EternalBlue und anderen Sicherheitslücken mit hohem Risiko. Faktoren, die zu dieser Verschiebung beigetragen haben, waren die Schließung des beliebten webbasierten Mining-Anbieters Coinhive[1] und der Rückgang der Kryptowährungswerte.[10] Ein weiterer Faktor ist, dass dateibasiertes Cryptomining schon immer effizienter war als webbasiertes Mining und 25 Mal rentabler.[3] Bedrohungsakteure haben ihre Malware mit zusätzlichen Tools angepasst, um vertrauliche Informationen vom Computer des Opfers zu extrahieren.

Weltweit gehen Cryptojacking-Angriffe zurück

Im Jahr 2019 war ein Abwärtstrend[5] im Hinblick auf Cryptojacking-Angriffe festzustellen, der hauptsächlich auf die Schließung von Coinhive[6], die koordinierten Bemühungen der Strafverfolgungsbehörden sowie die Abwertung der Monero-Kryptowährung zurückzuführen war. Da jedoch bekannt ist, dass Cryptojacking-Angriffe den Kryptowährungswerten folgen, kann ein Coinhive-ähnlicher Dienst entstehen und einen neuen Anstieg auslösen. Frühe Statistiken für 2020 zeigen einen Anstieg von 30 % gegenüber dem Vorjahr im März.

_Monero blieb die Kryptowährung der ersten Wahl

Ähnlich wie bei früheren Trends war Monero (XMR) die Kryptowährung der Wahl für Cryptojacking-Aktivitäten im Jahr 2019. Der Grund ist zweifach: Erstens konzentriert sich Monero auf Datenschutz und Anonymität, weshalb die Transaktionen nicht zurückverfolgt werden können. Zweitens wurde der Proof-of-Work-Algorithmus entwickelt, um das Mining mit einer Standard-CPU im Gegensatz zu spezieller Hardware rentabel zu machen. Im dritten Quartal 2019 handelten 32 % der Börsen mit Datenschutzmünzen wie Monero. In Erwartung neuer Vorschriften zur Bekämpfung der Geldwäsche entschieden sich viele Börsen jedoch dafür, Datenschutzmünzen zu dekotieren.

_Die am häufigsten betroffenen Zielländer

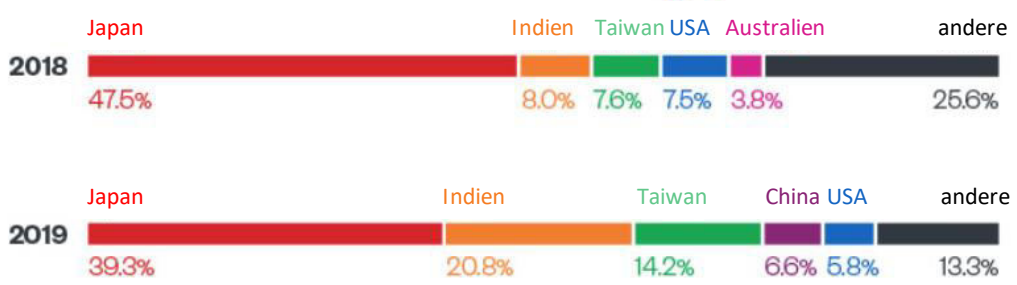


Abbildung 2: Die am häufigsten von Cryptojacking betroffenen Länder Quelle: Trend Micro[7]

Angriffsvektoren

_Techniken

Cyberkriminelle verwendeten die folgenden Techniken, um Krypto-Miner auszuführen oder bereitzustellen:

- durch Integration von Cryptojacking-Funktionen in vorhandene Malware;[10]
- durch Kompromittierung von Websites;[11]
- durch anhaltende Drive-by-Angriffe;[12]
- durch die Nutzung sozialer Netzwerke;[13]
- durch die Nutzung mobiler Apps und App-Stores;[14]
- durch die Verwendung von Exploit-Kits;[15]
- durch die Nutzung von Werbenetzwerken und Malvertising;[16]
- durch die Nutzung von Wechselmedien;[17]
- und durch die Verwendung von „wurmfähigen“ Crypto-Minern.[18]

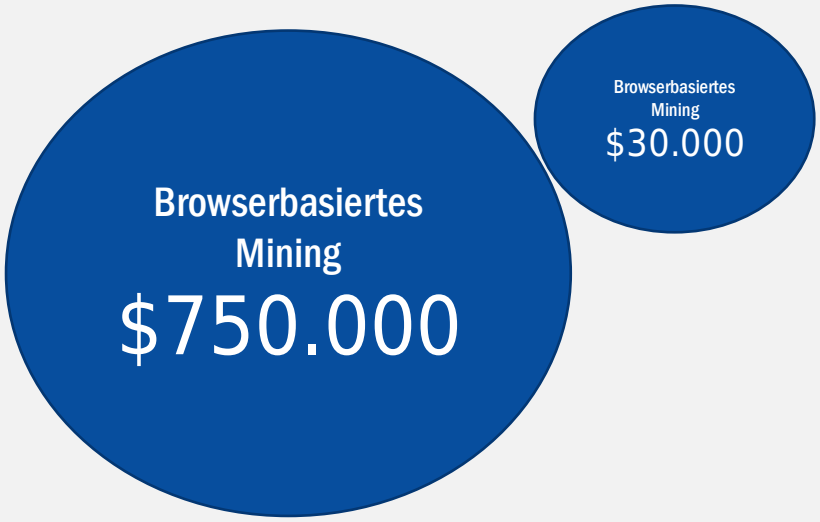


Abbildung 3: Wie viel kann ein Münz-Mining-Botnetz in 30 Tagen verdienen? Quelle: Broadcom[3]

Vorgeschlagene Aktionen

- Überwachen Sie den Batterieverbrauch auf den Geräten der Benutzer und suchen Sie bei verdächtigen Spitzen in der CPU-Auslastung nach dem Vorhandensein dateibasierter Miner.
- Implementieren Sie die Inhaltsfilterung, um unerwünschte Anhänge, E-Mails mit schädlichem Inhalt und Spam herauszufiltern.
- Implementieren Sie die Filterung des Stratum-Mining-Protokolls sowie die Blacklisting der IP-Adressen und Domänen beliebter Mining-Pools.
- Installieren Sie den Endpunktschutz mithilfe von Antivirenprogrammen oder Cryptominer, die Browser-Plug-Ins blockieren.
- Führen Sie regelmäßige Sicherheitsüberprüfungen durch, um Netzwerkanomalien zu erkennen.
- Implementieren Sie ein robustes Schwachstellen- und Patch-Management.
- Verwenden Sie die Whitelist, um zu verhindern, dass unbekannte ausführbare Dateien an den Endpunkten ausgeführt werden.
- Investieren Sie in die Sensibilisierung der Benutzer für Crytojacking, insbesondere im Hinblick auf ein sicheres Surfverhalten.
- Implementieren Sie Patches und Fixes für bekannte Exploits wie Eternal Blue auf weniger offensichtlichen Zielen wie Warteschleifenmanagementsystemen, POS-Terminals und sogar Verkaufsautomaten.
- Überwachung und Führung von schwarzen Listen gängiger ausführbarer Cryptomining-Dateien.

Literaturangaben

1. Sergiu Gatlan. "Cryptominers Still Top Threat In March Despite Coinhive Demise." 9. April, 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/cryptominers-still-top-threat-in-march-despite-coinhive-demise/

2. "Internet Organised Crime Threat Assessment (IOCTA)." 2019. EUROPOL. https://www.europol.europa.eu/iocta-report

3. "Beapy: Cryptojacking Worm Hits Enterprises in China." 24. April 2019. BROADCOM. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/beapy-cryptojacking-worm-china

4. Bill Conner. "SONICWALL Cyber Threat Report." 2020. SONICWALL https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/

5. Yessi Bello Perez. "Unsuspecting victims were cryptojacked 52.7 million times in the first half of 2019." 24. Juli, 2019. TheNextWeb – HARD FORK. https://thenextweb.com/hardfork/2019/07/24/cryptojacking-cryptocurrency-million-hits-first-half-2019/

6 Ben Noble. "A Third of Cryptocurrency Exchanges Still Host Privacy Coins Despite Fears of Impending FATF Travel Rule." 27. November 2019. CIPHERTRACE https://ciphertrace.com/ciphertrace-q3-2019-caml-press-release/

7. "Defending Systems Against Cryptocurrency Miner Malware." 28. Oktober , 2019. Trend Micro. https://www.trendmicro.com/vinfo/be/security/news/cybercrime-and-digital-threats/defending-systems-against-cryptocurrency-miner-malware

8. "Kaspersky Security Bulletin '19 Statistics." 2009. Kaspersky. https://go.kaspersky.com/rs/802-IJN-240/images/KSB_2019_Statistics_EN.pdf

9. "CYBER SECURITY REPORT." 2020. Check Point Research cp<r>. https://www.checkpoint.com/downloads/resources/cyber-security-report-2020.pdf

10. Ionut Ilascu. "Eternal Blue Exploit Serves Beapy Cryptojacking Campaign." 25. April, 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/eternalblue-exploit-serves-beapy-cryptojacking-campaign/

11. "New mining worm PsMiner uses multiple high-risk vulnerabilities to spread." 12. März 2019. 360 Total Security. https://blog.360totalsecurity.com/en/new-mining-worm-psminer-uses-multiple-high-risk-vulnerabilities-to-spread/

12. Dan Thorp-Lancaster. "New drive-by cryptocurrency mining scheme persists after you exit your browser window." 9. November, 2017 Windows Central. https://www.windowscentral.com/new-drive-cryptocurrency-mining-scheme-persists-even-after-you-exit-your-browser-window

13. Dr. Michaeal McGuire. "Social Media Platforms and the Cybercrime Economy." 2019. Bromium. https://www.bromium.com/wp-content/uploads/2019/02/Bromium-Web-of-Profit-Social-Platforms-Report.pdf

14. Axelle Apvrille. "Abusing cryptocurrencies on Android smartphones." 2019. Fortinet. https://fortinetweb.s3.amazonaws.com/fortiguard/research/currency-insomnihack19.pdf

15. "2019 Midyear Security Roundup Evasive Treats Pervasive Effects." 2019. TrendMicro https://documents.trendmicro.com/assets/rpt/rpt-evasive-threats-pervasive-effects.pdf

16. Margi Murphy. "YouTube shuts down hidden cryptojacking adverts." 29. Januar, 2018. The Telegraph https://www.telegraph.co.uk/technology/2018/01/29/youtube-shuts-hidden-crypto-jacking-adverts/

17. Matthew Beedham. "New cryptocurrency mining malware is spreading across Thailand and the US." 4. Juni, 2019 TheNextWeb – HARD FORK. https://thenextweb.com/hardfork/2019/06/04/security-crypto-jacking-mining-malware/

18. Sean Lyngaas. "BlueKeep is back. For now, attackers are just using it for cryptomining." 4. November, 2019 CyberScoop. https://www.cyberscoop.com/bluekeep-exploited-cryptomining/

19. Janus Agcaoili. "Monero-Mining Malware PCASTLE Zeroes Back In on China, Now Uses Multilayered Fileless Arrival Techniques." 5. Juni, 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-malware-pcastle-zeroes-back-in-on-china-now-uses-multilayered-fileless-arrival-techniques/

20. Marie Huillet. "Researchers Say 50,000 Servers Worldwide Infected With Privacy Coin Cryptojacking Malware." 29. Mai, 2019. Cointelegraph. https://cointelegraph.com/news/researchers-say-50-000-servers-worldwide-infected-with-privacy-coin-cryptojacking-malware

21. Johnlery Triunfante, Mark Vicente. "BlackSquid Slithers Into Servers and Drives With 8 Notorious Exploits to Drop XMRig Miner." 27. August, 2019 Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/blacksquid-slithers-into-servers-and-drives-with-8-notorious-exploits-to-drop-xmrig-miner/

22. "Malicious cryptojacking code found in 11 Ruby libraries." 2. August, 2019 https://decrypt.co/8602/malicious-cryptjacking-code-found-in-11-ruby-libraries

23. Brook Chelmo. "Cryptojacking in 2019: Cryptocurrency Value Keeping Attack Vector in Play." 6. August, 2019. SonicWall. https://blog.sonicwall.com/en-us/2019/08/cryptojacking-in-2019-cryptocurrency-value-keeping-attack-vector-in-play/

24. Catalin Cimpanu. "Coinhive cryptojacking service to shut down in March 2019". 27. Februar, 2019 ZD Net. https://www.zdnet.com/article/coinhive-cryptojacking-service-to-shut-down-in-march-2019/

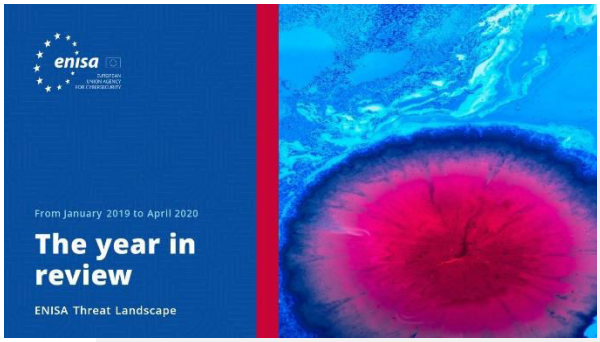
25. Tom Hegel. "Making it Rain - Cryptocurrency Mining Attacks in the Cloud". 14. März 2019. AT&T Business. https://cybersecurity.att.com/blogs/labs-research/making-it-rain-cryptocurrency-mining-attacks-in-the-cloud/

26. "How a Prominent Cryptomining Botnet is Paving the Way for a Lucrative and Illicit Revenue Model". August 2019 Carbon Black. https://www.carbonblack.com/resources/access-mining/

27. "Cryptojacking Attacks: Who's Mining on Your Coin?". 5. April, 2019. Security Intelligence. https://securityintelligence.com/cryptojacking-attacks-whos-mining-on-your-coin/

28. "Malware Creates Cryptominer Botnet Using EternalBlue and Mimikatz'. 12. April, 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/malware-creates-cryptominer-botnet-using-eternalblue-and-mimikatz/

Themenbezogen



ENISA Threat Landscape Bericht **Das Berichtsjahr**

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

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht **Liste der 15 größten Bedrohungen**

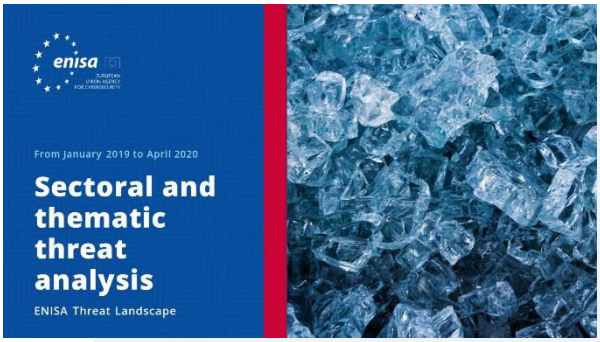
ENISAs-Liste der 15 größten Bedrohungen im Zeitraum zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht **Forschungsthemen**

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

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.

LESEN SIE DEN BERICHT

Über

_ 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, -Diensten und -Prozessen durch Programme für die Cybersicherheitszertifizierung, sie 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 Information 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.

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

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu