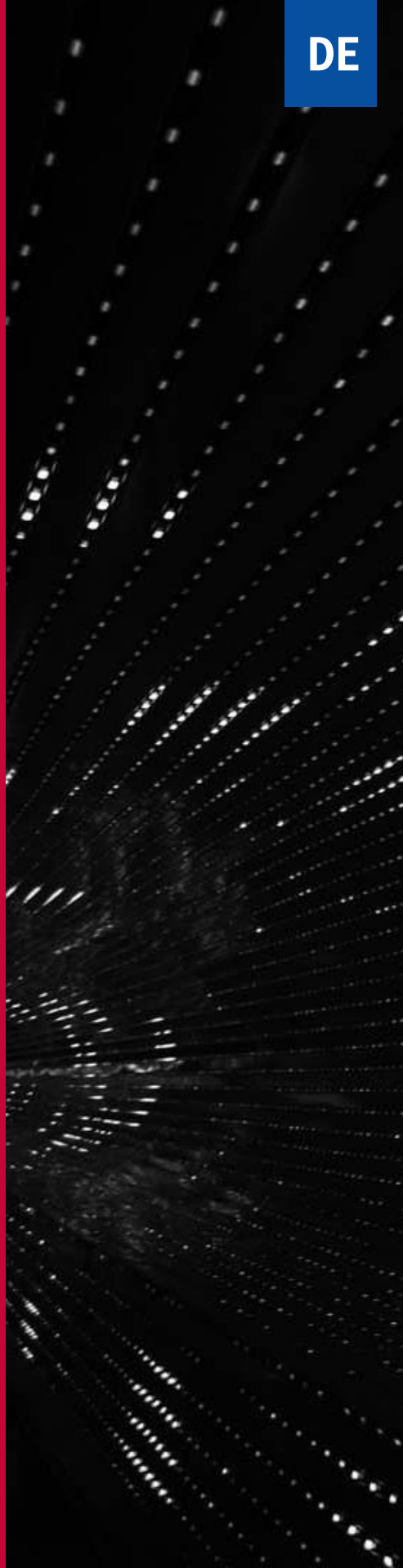
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

DE



Von Januar 2019 bis April 2020

Botnetz

ENISA Threat Landscape

Überblick

Ein Botnetz ist ein Netzwerk verbundener Geräte, die mit Bot-Malware infiziert sind. Diese Geräte werden normalerweise von böswilligen Akteuren verwendet, um DDoS-Angriffe (Distributed Denial of Service) durchzuführen. Botnetze werden in einem Peer-to-Peer-Modus (P2P)[1] oder von einem Command and Control (C2)[2] Center aus betrieben und von einem böswilligen Akteur ferngesteuert, um synchron zu arbeiten und ein bestimmtes Ergebnis zu erzielen.[3]

Der technologische Fortschritt bei verteilter Datenverarbeitung und Automatisierung hat böswilligen Akteuren die Möglichkeit geboten, neue Techniken zu erforschen und ihre Instrumente und Angriffsmethoden zu verbessern. Daher funktionieren Botnetze viel verteilter und automatisierter und sind bei Self-Service-Anbietern und Anbietern gebrauchsfertiger Lösungen erhältlich.

Schädliche Bots, die als „malicious bots" bezeichnet werden, entwickeln sich nicht nur ständig weiter, sondern die Fähigkeiten der Menschen und der Entwicklungsstand der Bots werden zunehmend auf bestimmte Anwendungen spezialisiert, z. B. auf Verteidigungsanbieter oder sogar Ausweichtechniken.[4] Aus einer anderen Perspektive bieten Botnetze Cyberkriminellen einen Vektor, um verschiedene Operationen vom E-Banking-Betrug über Ransomware bis hin zu Mining von Kryptowährungen und DDoS-Angriffen zu starten.[5]

Erkenntnisse

7,7_Millionen IoT-Geräte werden täglich mit dem Internet verbunden.

Von diesen befindet sich schätzungsweise 1 von 20 hinter einer Firewall oder einem ähnlichen Netzwerksicherheitsinstrument.[6]

57 %_Zunahme der Anzahl von entdeckten Mirai-Varianten im Jahr 2019

Obwohl bekannt ist, dass Mirai-Varianten Brute-Force-Versuche hauptsächlich zur Kompromittierung von IoT-Geräten verwenden, war 2019 sowohl bei Brute-Force-Versuchen (51 %) als auch bei Web-Exploitation-Versuchen (87 %) ein Anstieg zu verzeichnen.[7]

300.000_Meldungen des Emotet-Botnet-Verkehrs im Jahr 2019 beobachtet

Dies führte zu mehr als 100.000 Opferalarmen als im gleichen Zeitraum des Jahres 2018. Die Forscher gingen davon aus, dass die Anzahl der Emotet-Fälle im Vergleich zur zweiten Hälfte von 2018 und 2019 um 913 % gestiegen ist.[7]

60 %_der neuen konkurrierenden Botnetzaktivitäten sind mit dem Diebstahl von Anmeldedaten verbunden[9]

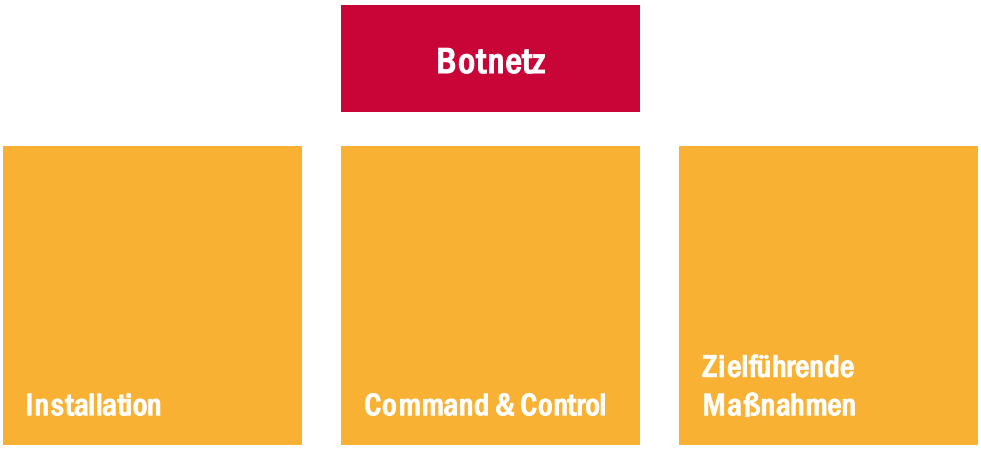
17.602_voll funktionsfähige Botnetz C2 Server im Jahr 2019 gefunden

71,5 % Zunahme im Vergleich zu 2018.[5]

Kill Chain

Schritt des Angriffs-Workflows

Umfang des Zwecks



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

_Bots sind das große Geld

Bots erleichtern Brute-Force-Fähigkeiten, indem sie Opfer dazu verleiten, Artikel in limitierter Auflage oder Artikel in Werbeangeboten zu kaufen und diese anschließend zu einem höheren Preis weiterzuverkaufen. Diese Tatsache wurde identifiziert, indem eine Stellenanzeige analysiert wurde, in der der Werbetreibende nach einem Softwareentwickler mit Erfahrung in der Umgehung von Sicherheitsmaßnahmen sowie in Bots mit Ausweichtechniken (z. B. Web-Scrapping, ReCAPTCHA-Bypass, Cookie-Generierung usw.) suchte und bereit war, 15.000 USD (ca. 12.750 EUR) für den richtigen Kandidaten zu bezahlen.[4]

_Der gemauerte Silexbot

Im Juni 2019 analysierte ein Sicherheitsforscher[17] ein neues Bot-Muster, das entwickelt wurde, um die Funktionen unsicherer IoT-Geräte zu stören. Mit anderen Worten wurde dieser Bot entwickelt, um bekannte/Standard-Anmeldedaten von IoT-Geräten zu verwenden, um sich anzumelden und das Gerät anschließend zu zerstören, indem Netzwerkkonfigurationen gelöscht und eine IP-Tabellenregel hinzugefügt wurde, um alle Verbindungen zu trennen. Ein interessanter Punkt neben den technischen Möglichkeiten war der Hinweis im Malware-Muster. Der Bedrohungsakteur entschuldigt sich für seine Aktivitäten und erklärt seine Maßnahmen als Mittel, um die Massenbetreibung unsicherer IoT-Geräte zum Aufbau von Botnetzen für böswillige Zwecke zu verhindern.

Echobot und sein wachsender Bedrohungsvektor

Im Juni 2019 identifizierte ein Sicherheitsforscher eine aktualisierte Version von Echobot. In dieser Analyse beobachtete der Forscher ein x86-kompiliertes Muster, das zu Angriffsvektoren führte, die von dieser Mirai-Variante in 26 verschiedenen Fällen verwendet wurden.[10] Im August stellte ein anderer Sicherheitsforscher eine Zunahme von Echobot fest, bei der 50 verschiedene Sicherheitslücken ausgehoben wurden, darunter die „Befehlsinjektion über HTTP“ (CPAI-2016-0658).[25,26] Im Dezember 2019 entdeckte ein anderes Team eine erweiterte Version von Echobot mit 71 Betreibungen (Exploits). Die neu hinzugefügten Exploits zielten auf alte und neue Schwachstellen ab und hatten eine erhebliche zusätzliche Fähigkeit, auf ICS-Geräte (Industrial Control System) zuzugreifen. Dazu gehörten Unternehmen und Geräte wie Mitsubishi, Citrix NetScaler-Steuerelemente für die App-Bereitstellung, die Barracuda-Webanwendungs-Firewall und Endpunktverwaltungstools.[27]

_Necurs im Rückzug, während Emotet wieder aufkommt

Im Januar 2019 wurde beobachtet, wie Necurs in eine Amateur-Spam-Kampagne überging, bei der die Forscher glauben sollten, dass die Fähigkeiten der dahinter stehenden böswilligen Akteure erheblich nachgelassen hätten.[20] Ganz im Gegenteil nahm jedoch die Aktivität von Emotet seit September 2019 erheblich zu und stieg gegen Ende 2019 weiter an. Dabei wurden eindeutige kompilierte Binärdateien, die dauerhafte Übermittlungsvektoren und Kommunikationsmechanismen darstellen, hinterlassen.[7] Eine Analyse ergab einen starken Anstieg der Verbreitung von Emotet per E-Mail.[22]

Entwicklungen

_Retadup, das Botnetz hinter Monero-Mining, ist gefallen

Retadup war hauptsächlich als Monero-Mining-Wurm aktiv, der polymorphe Fähigkeiten entwickelte.[23] Er hatte Windows-Computer in Lateinamerika infiziert. Dieser Bot verfügte über Funktionen, die vom Mining bis zur Bereitstellung von benutzerdefinierten Codes und heruntergeladenen Dateien auf den Computern der Opfer reichen (es wurde auch beobachtet, dass STOP Ransomware verteilt wurde[24]). Ein Sicherheitsforscher begann im März 2019 mit der Überwachung der Retadup-Aktivitäten und stellte fest, dass das C2-Protokoll auf einfache Weise entworfen wurde. Das Team identifizierte einen Fehler im Protokoll, der es ihnen ermöglichte, Infektionen vom Opfer zu entfernen, indem sie den C2-Server übernahmen. Die Infrastruktur für diese böswillige Aktivität befand sich hauptsächlich in Frankreich. Das Botnetz wurde in Zusammenarbeit mit der Nationalen Gendarmerie (Frankreich) entfernt, und rund 850 000 Computer wurden „desinfiziert".

_Mirai ist tot, lang lebe Mirai

Es könnte daran liegen, dass Mirai und seine Varianten aufgrund des Mangels an Fähigkeiten und Funktionen im ursprünglichen Code immer noch in den Botnetz-Familien dominieren, dass im ersten Halbjahr 2019 monatlich mehr als 20 000 Einzelmuster beobachtet wurden. Diese Varianten verwenden unterschiedliche Techniken zur Kompromittierung von IoTs, von Brute-Forcing-Standardkennwörtern mit festem Code bis hin zu Exploits.[6] Laut zwei Sicherheitsforschern gibt es auch eine große Vielfalt von Systemarchitekturen, auf die diese Varianten abzielen. Weitere Statistiken zur Emotet-Aktivität finden Sie in Abbildung 1.[7,18]

_Das P2P Roboto Botnetz

Robotos Aktivität wurde erstmals im August 2019 von einem Sicherheitsforschungsteam als P2P-Botnet-Programm beobachtet. Das erste erfasste Muster war eine verdächtige ELF-Datei. Im Oktober identifizierte das Forschungsteam einen weiteren Fall, eine ELF-Datei, die sich als Downloader des vorherigen Musters herausstelle. Bei weiteren Analysen stellte das Forschungsteam fest, dass das Roboto-Botnetz sieben Funktionen unterstützen kann, nämlich Reverse Shell, Selbstdeaktivierung, Sammeln von Prozess- und Netzwerkinformationen, Sammeln von Bot-Informationen, Ausführen von URL-angegebenen Dateien, DDoS-Angriffe und Ausführen von Systemangriffen. Interessanterweise scheint ein DDoS-Angriff laut dem Forscher nicht der Hauptanwendungsfall zu sein. Im Gegensatz zu anderen Botnetzen verbreitete sich dieser Bot, indem er die Sicherheitsanfälligkeit von Webmin RCE (CVE-2019-1507[28]) ausnutzte.[11]

_Mozi, ein anderes auf DHT basiertes Botnetz

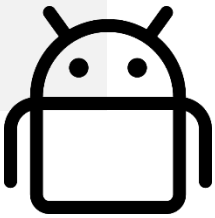
Mozi wurde nach seinem Propagierungsdateinamen benannt und als brandneues DHT-basiertes Botnetz identifiziert, das im September 2019 von einem Sicherheitsforscher beobachtet wurde. Eine erste Analyse des Musters, das von einem anderen Sicherheitsforscher[38] durchgeführt wurde, wurde als Gafgyt identifiziert. Dies lag jedoch daran, dass das Muster den Code von Gafgyt teilweise wiederverwendete. Dieses Botnetz verbreitet sich, indem es eine Handvoll Exploits und schwache Passwörter für Telnet verwendet. Die Analyse seiner Funktionen ergab, dass es in der Lage sein könnte, DDoS-Angriffe auszuführen, Informationen zu sammeln, Sample/Payload unter Verwendung einer bestimmten URL auszuführen und zu aktualisieren und Befehle auszuführen.[29, 30]

Entwicklungen

__Statistiken über Emotet-Aktivitäten

Erkenntnis	Statistik
Gesamtanzahl der erkannten ASn:	5 430
Gesamtanzahl der erkannten eindeutigen IPs:	120 764
Anzahl der teilnehmenden Länder:	193
Anzahl der versandten E-Mails:	10 935 346
Anzahl der verteilten URLs:	4 726
Bestimmte anvisierte RCPTs:	8 052 961

Abbildung 1: Quelle: Spamhaus[5]



„Der technologische Fortschritt bei verteilter Datenverarbeitung und Automatisierung hat böswilligen Akteuren die Möglichkeit geboten, neue Techniken zu erforschen und ihre Instrumente und Angriffsmethoden zu verbessern.“

In ETL 2020

Erkenntnisse

_Statistiken und andere relevante Zahlen

Laut einem Sicherheitsforscher sind **täglich 7,7 Millionen IoT-Geräte mit dem Internet verbunden**, und es wird geschätzt, dass sich nur 1 von 20 Geräten hinter einer Firewall oder einem ähnlichen Netzwerksicherheitsinstrument befindet.[6] Diese Schätzung zeigt, dass **IoT-Geräte immer noch beeinflussbar und anfällig für eine Ausbeutung** durch Cybersicherheitsbedrohungen wie Mirai sind.

- Im ersten Halbjahr 2019 nahmen die Botnetz-Aktivitäten und das Hosting von C2-Servern erheblich zu.[32] Dieser Anstieg entsprach 7 % aller Botnetz-Erkennungen und 1,8 % aller C2s weltweit. Finanzdienstleister und deren Kunden waren der am häufigsten angesprochene Sektor.
- Thailand war das Top-Land in Bezug auf das Hosting von C2-Servern, während Malaysia an zweiter Stelle lag, gefolgt von den Philippinen, Singapur und Indonesien.
- Basierend auf Interpol-Untersuchungen war das Andromeda-Botnetz das dominanteste in Bezug auf die Erkennung, obwohl es 2017 aufgelöst wurde.[33] Conficker[34] kam an zweiter Stelle, gefolgt von Necurs[35], Sality[36] und Gozi[37].

Im Jahr 2019 stieg die Anzahl der nachgewiesenen Mirai-Varianten im Vergleich zu 2018 um mehr als 57 %, wie in Abbildung 2 dargestellt.

Obwohl bekannt ist, dass Mirai-Varianten Brute-Force-Versuche hauptsächlich zur Kompromittierung von IoT-Geräten verwenden, war im Jahr 2019 sowohl bei Brute-Force-Versuchen (51 %) als auch bei Web-Exploitation-Versuchen (87 %) ein Anstieg zu verzeichnen.

Anzahl der Mirai-Muster

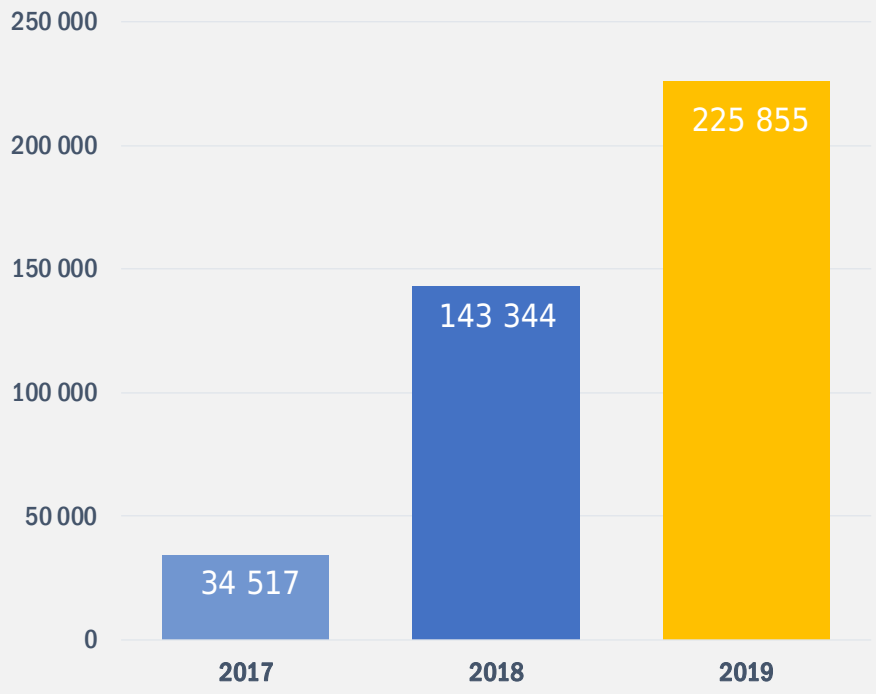


Abbildung 2 - Quelle: NETSCOUT[7]

Erkenntnisse

_Statistiken und andere relevante Zahlen

- Im Jahr 2019 beobachtete ein Sicherheitsforscher fast 300.000 weitere Benachrichtigungen über den Botnetz-Verkehr von Emotet im Vergleich zum gleichen Zeitraum im Jahr 2018, sowie über 100.000 weitere Meldungen über Opfer. Der Forscher glaubt, dass die Anzahl der Emotet-Fälle im Vergleich zur zweiten Hälfte von 2018 und 2019 um 913 % gestiegen ist.[7,22]
- Seit Roboto und Mozi aktiv wurden, nahm die P2P-Botnetzaktivität zu.[8]
- Linux-basierte Botnetze waren für fast 97,4 % der Angriffe verantwortlich.[8]
- Der höchste Anteil an Botnetzen wurde im vierten Quartal 2019 in den USA registriert (58,33 %). Während dies ein Anstieg gegenüber dem dritten Quartal 2019 ist (47,55 %), hat sich die Gesamtzahl der C2-Server fast halbiert. Das Vereinigte Königreich lag auf dem vierten Platz und sprang mit 14,29 % auf den zweiten Platz, während China mit 9,52 % die gleiche Position beibehielt. Der größte Rückgang bei C2-registrierten Servern war in den Niederlanden zu verzeichnen (von 45 % auf ~ 1 %). Weitere Informationen zur Verteilung der Botnetz C2-Server nach Ländern finden Sie in Abbildung 3.[8]
- Im Jahr 2019 blieb LokiBot mit einem Anstieg der Anzahl der C2-Aktivitäten um 74 % im Vergleich zu 2018 an der Spitze der Liste der Anmeldedaten stehlenden Bots. AZORult lag direkt hinter LokiBot auf dem zweiten Platz.[39]
- 17.602 Botnetz C2-Server waren 2019 in Betrieb, was einer Steigerung von 71,5 % gegenüber 2018 entspricht.[39]

Verteilung der Botnetz-C&C-Server auf Länder

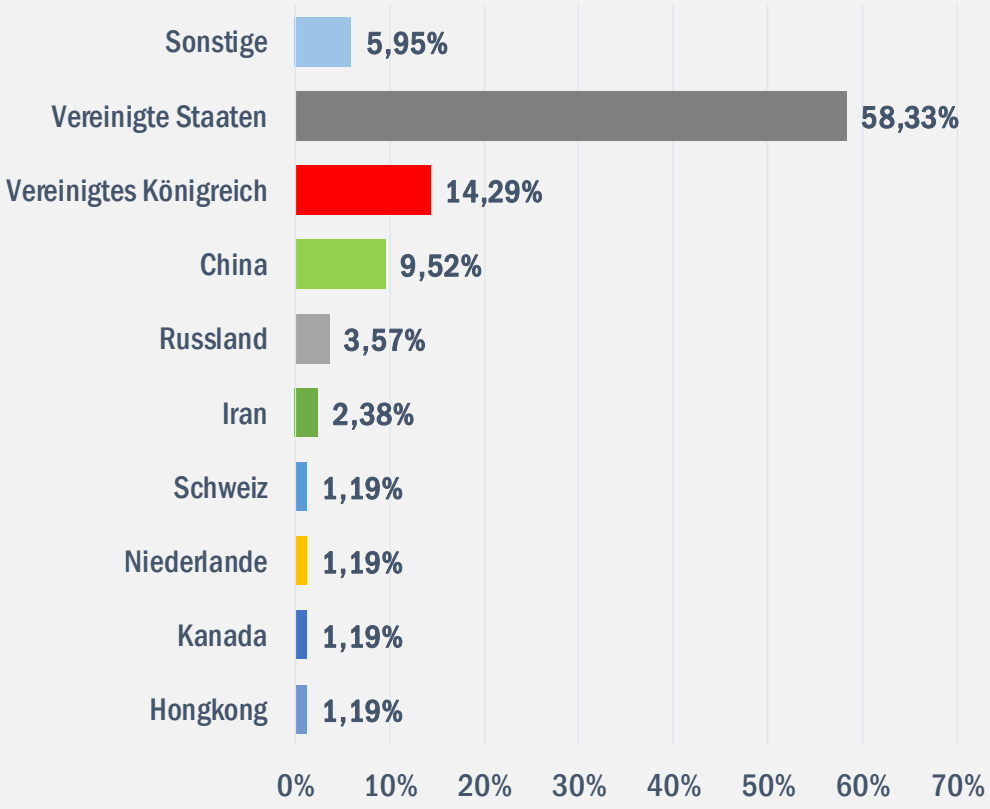


Abbildung 3 - Quelle: Kapersky[8]

Angriffsvektoren

_ Die Botnetz-Angriffe

Laut einem Sicherheitsforscher waren im Jahr 2019 fast 60 % der neuen konkurrierenden Botnetzaktivitäten mit dem **Diebstahl von Anmeldedaten** verbunden. Wie bereits erwähnt, ist LokiBot in diesem Bereich am aktivsten. Neben dem Diebstahl von Anmeldedaten sind **E-Banking und Finanzbetrug** weitere Bereiche, in denen Botnetz sehr präsent ist. Emotet und TrickBot sind erstklassige Beispiele für diese Aktivität mit einem aktualisierten Modell, das nicht nur E-Banking-Betrug, sondern auch Pay-per-Install (PPI) abdeckt.[9]

Darüber hinaus gehörten **RATs (Remote Access Trojaner)** zu den am häufigsten verwendeten Tools in Botnetz-C2-Aktivitäten. Während des Jahres 2018 waren die meisten dieser Aktivitäten mit Adwind verbunden, aber im Jahr 2019 wurde seine Aktivität reduziert und durch NanoCore ersetzt.[5]

In 2019 wurden **spezifische Angriffsvektoren übernommen**. Botnetze verwenden verschiedene Angriffsvektoren, um ihre Ziele zu erreichen. Infizierte Maschinen oder Zombienetzwerke werden durch Ausnutzen häufiger Sicherheitslücken mit Brute-Force- und anderen gängigen Infektionstechniken erstellt.[10,11,12] Anschließend kann der Botmaster eine Plattform für verschiedene Angriffe bereitstellen, wie zum Beispiel die weit verbreitete Spam- und Malware-Kampagne, das Stehlen und Wiederverwenden von Anmeldedaten, Crypto-Mining und DDoS.

Ein weiteres Beispiel für einen Angriffsvektor, der bei einem Botnetzangriff verwendet wird, ist der **„Triple Threat“.** Bei dieser Technik wird die Zielorganisation zunächst mit Emotet-Malware infiziert. Dann liefert die Emotet-Malware den TrickBot-Trojaner, der auf vertrauliche Informationen abzielt und diese verwendet. Wenn die Informationen gefunden wurden und die Zielumgebung/das Zielnetzwerk in der Liste des Angreifers enthalten ist, wird Ryuk-Ransomware bereitgestellt.[13]

Anzahl der beobachteten Botnetz-C2-Server zwischen 2014 und 2019

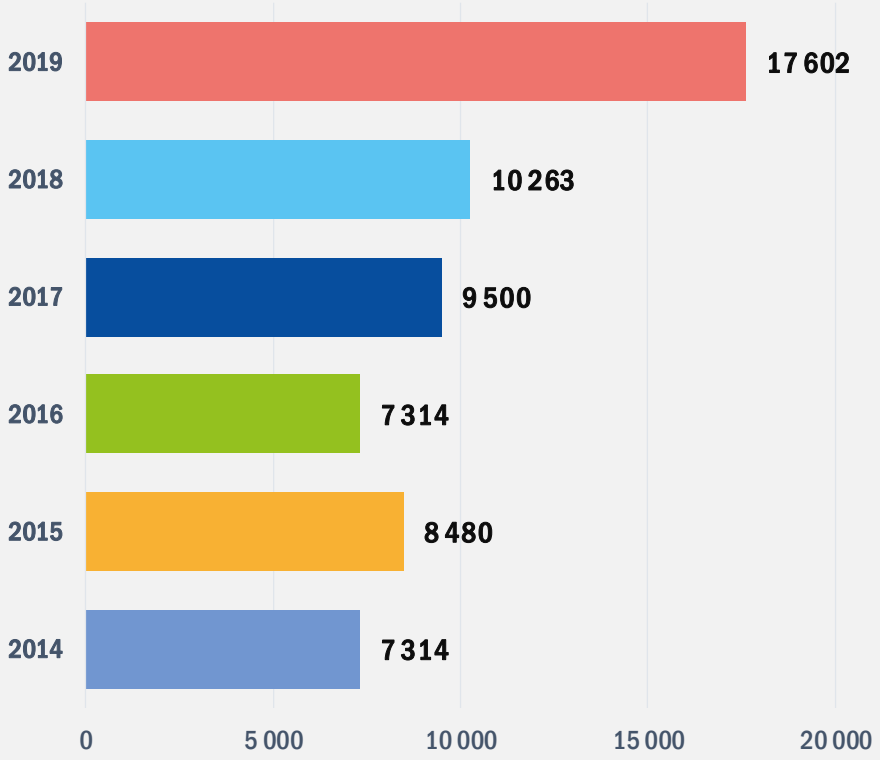


Abbildung 4 - Quelle: Spamhaus[5]

Abschwächung

_ Vorgeschlagene Aktionen

Ein wesentlicher Aspekt einer soliden Verteidigung ist das Konzept, das Umfeld zu kennen. Dies hilft dabei, böswillige Aktivitäten innerhalb des Datenverkehrs anhand der möglichen Baseline (d. h. Verhaltenserkennungen) zu identifizieren[14] und den Datenverkehr mithilfe eines Überwachungsinstrumentes zu messen.[4] In Anbetracht der Tatsache, dass mit der DDoS-Aktivität ein erheblicher Botnetz-Verkehr verbunden ist, gelten auch Abhilfemaßnahmen für DDoS-Bedrohungen.

- Stellen Sie Border-Gateway-Protokoll-Feeds mit der Fähigkeit bereit, nach dTLDs (dezentralen Domänen der obersten Ebene) zu suchen, um Verbindungen zu IP-Adressen zu blockieren, die mit der Botnetz-C2-Aktivität zusammenhängen.[8]
- Verstehen und Kategorisieren von Schwachstellen und Implementieren einer starken Patch- und Aktualisierungspraxis.[15,16]
- Beschränken oder blockieren Sie Kryptowährungs-Mining-Pools und überwachen Sie die Umgebung auf erforderliche Benutzer.[5]
- Stellen Sie herausfordernde Funktionen für erforderliche Websites bereit, um die Herkunft des Datenverkehrs zu überprüfen (d. h. reCAPTCHA).[16]
- Stellen Sie 2FA-Richtlinien (Strong Password and Authentication) auf öffentlich zugänglichen Servern oder Infrastrukturen bereit, um nicht Opfer einer Ausnutzung von schwachen Passwörtern/Authentifizierungen zu werden.[5]
- Bereitstellen und Konfigurieren von Netzwerk- und Anwendungsfirewalls.

"Die Komplexität der Bedrohungsfähigkeiten nahm 2019 zu, und viele Gegner nutzten Exploits, Diebstahl von Anmeldedaten und mehrstufige Angriffe."

In ETL 2020

Literaturangaben

1. "Peer-to-peer (P2P)." Malwarebytes Labs https://blog.malwarebytes.com/glossary/peer-to-peer/

2. Monnappa K A. "Learning Malware Analysis." Juni 2018 O'reilly. https://www.oreilly.com/library/view/learning-malware-analysis/9781788392501/17a1735d-9583-4d86-9d1e-8b2735af5168.xhtml

3. "ASEAN Cyberthreat Assessment 2020." 17. Februar 2020 Interpol https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-highlights-key-cyberthreats-in-Southeast-Asia

4. "State of The Internet Security - DDoS and Application Attacks Report: Band 5, Ausgabe 1." 2019. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-ddos-and-application-attacks-2019.pdf

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

6 "NETSCOUT Threat Intelligence Report: Powered by ATLAS - Findings from H1 2019." 2019.

7. "NETSCOUT Threat Intelligence Report - With key findings from the 15th Annual Worldwide Infrastructure Security Report (WISR) - Findings from H2 2019." 2019. NETSCOUT. https://www.netscout.com/threatreport

8. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. "DDoS attacks in Q4 2019." 13. Februar 2020. Kaspersky. https://securelist.com/ddos-report-q4-2019/96154/

9. Alina Dettmer. "What is Pay Per Install.?" 26. Oktober 2017. Aye Studios. https://www.ayetstudios.com/blog/mobile-advertising/mobile-campaign-types/pay-per-install

10. Larry Cashdollar. "Latest Echobot: 26 Infection Vectors." 13. Juni 2019. Akamai. https://blogs.akamai.com/sitr/2019/06/latest-echobot-26-infection-vectors.html

11. "The awaiting Roboto Botnet." 20. November 2019. Netlab. https://blog.netlab.360.com/the-awaiting-roboto-botnet-en/

12. Asher Davila. "Home & Small Office Wireless Routers Exploited to Attack Gaming Servers." 31. Oktober 2019. Paloalto. https://unit42.paloaltonetworks.com/home-small-office-wireless-routers-exploited-to-attack-gaming-servers/

13. "Triple Threat: Emotet deploys Trickbot to steal data & spread Ryuk." 2. April, 2019. Cybereason. https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware

14. "Bots." Imperva. https://www.imperva.com/learn/application-security/what-are-bots/

15. Rebecca Carter. "Bot Mitigation Best Practices." 19. Oktober 2018. DYN. https://dyn.com/blog/bot-mitigation-best-practices/

16. "What is a Botnet?" Veracode. https://www.veracode.com/security/botnet

17. "SIRT Advisory: Silexbot bricking systems with known default login credentials". 26. Juni 2019. Akamai.

18. "Mirai Botnet Continues to Plague IoT Space". 10. September, 2019. Reversing Labs. https://blog.reversinglabs.com/blog/mirai-botnet-continues-to-plague-iot-space

19. The Shadowserver Foundation. https://www.shadowserver.org/

20. "As Necurs Botnet Falls from Grace, Emotet Rises" January 27, 2020. Threat Post. https://threatpost.com/as-necurs-botnet-falls-from-grace-emotet-rises/152236/

21. "Mirai malware, attacks Home Routers". 14. Dezember 2016. ENISA https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers

22. "Estimating Emotet's size and reach". 12. Dezember 2019. SPAMHAUS. https://www.spamhaus.org/news/article/791/estimating-emotets-size-%20-and-reach

23. "Monero-Mining RETADUP Worm Goes Polymorphic, Gets an AutoHotKey Variant". 23. April, 2018. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-retadup-worm-goes-polymorphic-gets-an-autohotkey-variant/

24. "Meet Stop Ransomware: The Most Active Ransomware Nobody Talks About". 20. September, 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/meet-stop-ransomware-the-most-active-ransomware-nobody-talks-about/

25. "Command Injection Over HTTP". 26. Juli, 2016. Check Point. https://www.checkpoint.com/defense/advisories/public/2016/cpai-2016-0658.html/

26. "August 2019's Most Wanted Malware: Echobot Launches Widespread Attack Against IoT Devices". August 2019 Check Point. https://blog.checkpoint.com/2019/09/12/august-2019s-most-wanted-malware-echobot-launches-widespread-attack-against-iot-devices/

27. "Echobot Malware Now up to 71 Exploits, Targeting SCADA". 18. Dezember 2019. F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/echobot-malware-now-up-to-71-exploits--targeting-scada

28. "CVE-2019-15107 Detail". NIST. https://nvd.nist.gov/vuln/detail/CVE-2019-15107

29. "What is a distributed hash table?". EDPresso. https://www.educative.io/edpresso/what-is-a-distributed-hash-table

30. "A Look into the Gafgyt Botnet Trends from the Communication Traffic Log". 23. Juli, 2019. https://nsfocusglobal.com/look-gafgyt-botnet-trends-communication-traffic-log/

32. " ASEAN Cyberthreat Assessment 2020, Key Insights From The ASEAN Cybercrime Operations Desk" Interpol, 2020

33. "International team takes down virus-spewing Andromeda botnet". 5. Dezember 2017. The Register. https://www.theregister.com/2017/12/05/international_team_takes_down_virusspewing_andromeda_botnet/

34. "The odd, 8-year legacy of the Conficker worm". 21. November 2016 WeLiveSecurity. https://www.welivesecurity.com/2016/11/21/odd-8-year-legacy-conficker-worm/

35. "The Necurs Botnet: A Pandora's Box of Malicious Spam". 24. April 2017. https://securityintelligence.com/the-necurs-botnet-a-pandoras-box-of-malicious-spam/

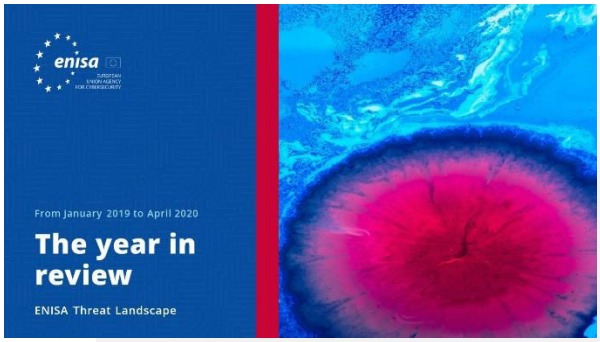
36. "WhitePaper: Sality: Story of a Peer to-Peer Viral Network". 10. Juni, 2011 Broadcom.

37. "Botnet C&C: Gozi". FortiGuard Labs. https://fortiguard.com/encyclopedia/botnet/7630489

38. Virustototal. https://www.virustotal.com

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

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**

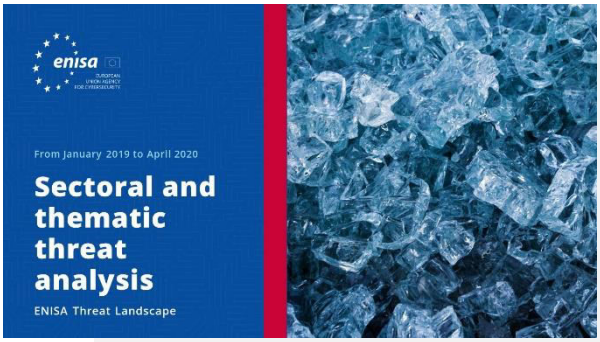
ENISAs-Liste der 15 größten Bedrohungen im Zeitraum zwischen Januar 2019 und April 2020.

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

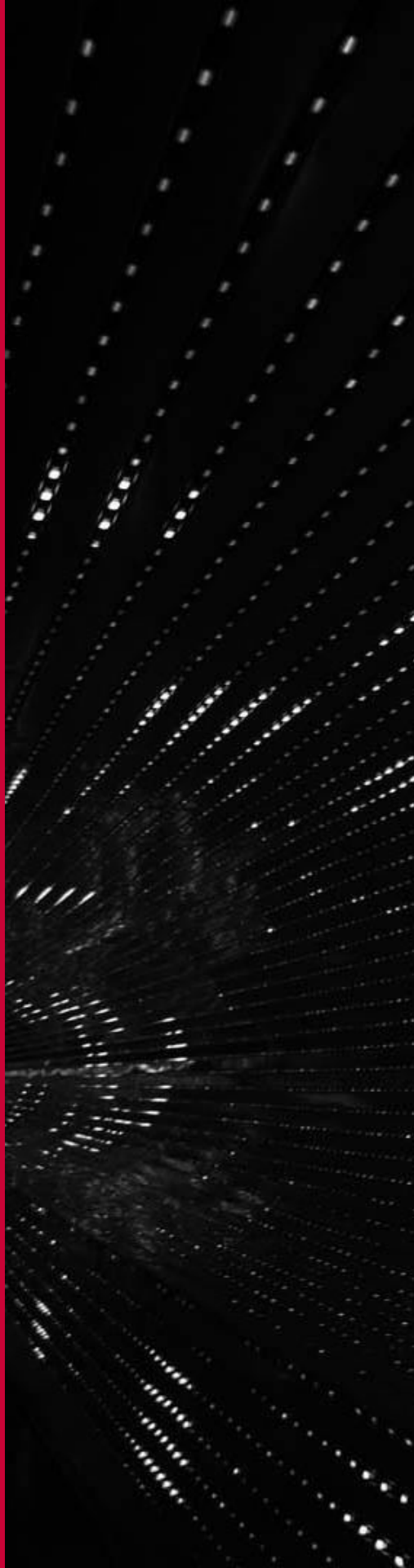
Sofern nichts anderes angegeben ist, gibt diese Veröffentlichung die Ansichten und Auslegungen der ENISA wieder. Diese Veröffentlichung ist nicht als eine Maßnahme der ENISA oder ihrer Gremien auszulegen, sofern sie nicht gemäß der Verordnung (EU) Nr. 526/2013 angenommen wurde. Diese Veröffentlichung 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