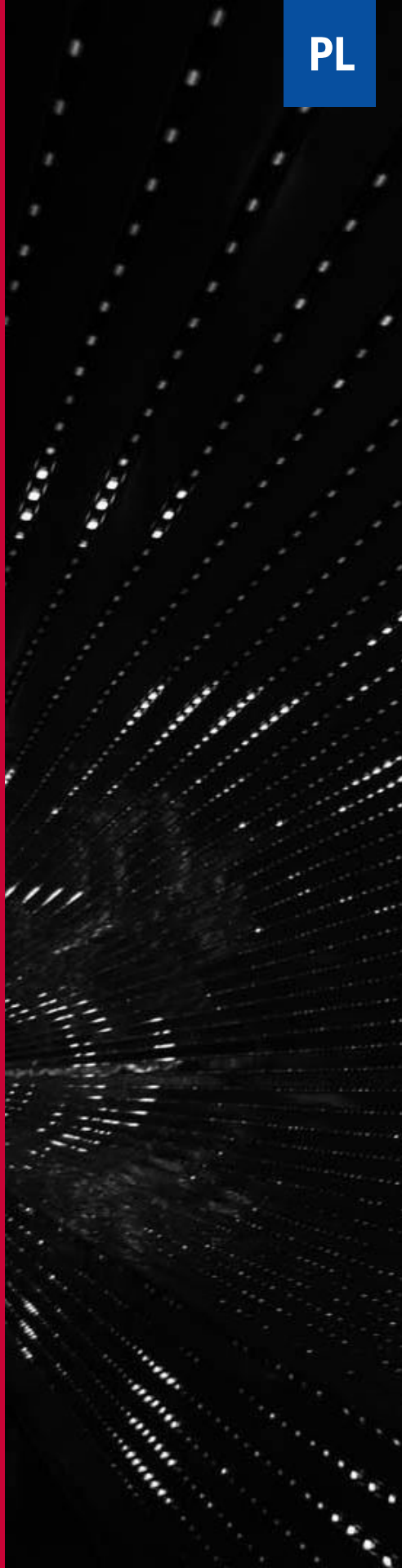
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

PL



Od stycznia 2019 r. do kwietnia 2020 r.

Botnet

Krajobraz zagrożeń wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)

Informacje ogólne

Botnet to sieć połączonych urządzeń zarażonych złośliwym oprogramowaniem – botami. Urządzenia te zazwyczaj są wykorzystywane przez sprawców szkodliwych działań do przeprowadzania rozproszonych ataków typu „odmowa usługi" (Distributed Denial of Service, DDoS). Botnety, działające w trybie peer-to-peer (P2P)[1] lub w trybie dowodzenia i kontroli (Command and Control, C2)[2], są zdalnie sterowane przez sprawcę szkodliwych działań tak, by działały w sposób zsynchronizowany celem uzyskania określonego rezultatu[3].

Postęp technologiczny w zakresie przetwarzania rozproszonego i automatyzacji umożliwił sprawcom szkodliwych działań wykorzystywanie nowych technik i ulepszanie narzędzi oraz metod ataku. Dzięki temu botnety operują w sposób znacznie bardziej rozproszony i zautomatyzowany. Można je nabyć w trybie samoobsługowym, gotowe do użytku.

Tak zwane „złośliwe boty" stale ewoluują, a na dodatek umiejętności ludzi i rozwój botów stają się coraz bardziej wyspecjalizowane w pewnych zastosowaniach, takich jak dostarczanie systemów obronnych lub nawet techniki unikania ataku[4]. Patrząc na to z innej perspektywy, botnety stanowią wektor, przez który cyberprzestępcy mogą przeprowadzać różnego rodzaju operacje, od ataków na elektroniczne usługi bankowe po oprogramowanie typu ransomware, wydobywanie kryptowalut i ataki typu DDoS[5].

Wnioski

7,7_miliona urządzeń IoT jest każdego dnia podłączanych do internetu

Jedno na 20 spośród nich jest chronionych przez zaporę sieciową lub podobne narzędzia z zakresu bezpieczeństwa sieci[6].

57%_wzrost liczby wariantów Mirai wykrytych w roku 2019

Wprawdzie warianty Mirai wykorzystują przede wszystkim metody ataków siłowych na urządzenia IoT, jednak w 2019 r. zaobserwowano zwiększenie liczby prób zarówno ataku siłowego (51%), jak i ataku przez stronę internetową (87%)[7].

300 000_powiadomień o ruchu generowanym przez botnet Emotet w roku 2019

W porównaniu z tym samym okresem 2018 r. skutkowało to o ponad 100 000 większą liczbą alertów o padnięciu ofiarą ataku. Analitycy sądzą, że w drugiej połowie 2019 r. liczba wystąpień Emotet wzrosła o 913% w porównaniu z drugą połową 2018 r.[7]

60%_aktywności nowych, konkurencyjnych botnetów wiąże się z kradzieżą danych uwierzytelniających[9]

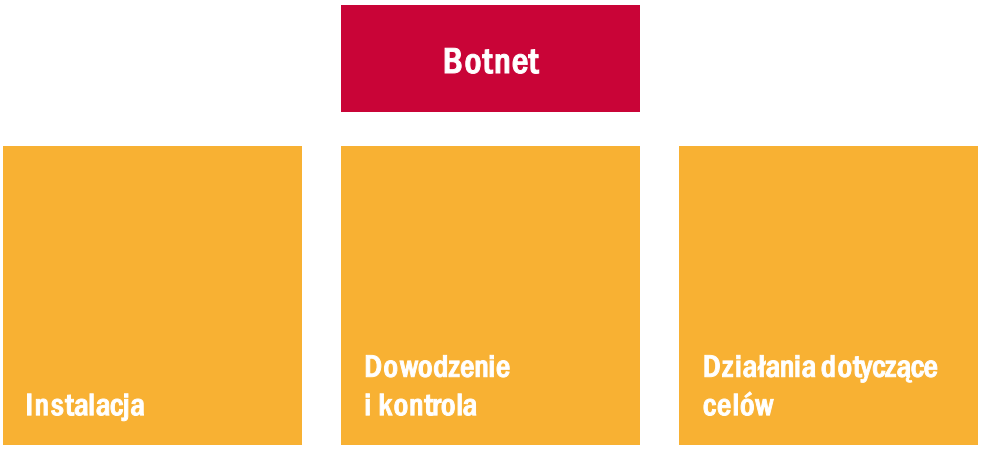
17 602_w pełni funkcjonalnych serwerów C2 botnetów w roku 2019

Wzrost o 71,5% w porównaniu z 2018 r.[5]

Kill chain

Proces etapów ataku

Zakres działania



Rozwiązanie Cyber Kill Chain® zostało opracowane przez Lockheed Martin na podstawie wojskowej koncepcji związanej ze strukturą ataku. Aby zbadać określony wektor ataku, należy użyć poniższego schematu Cyber Kill Chain w celu stworzenia mapy każdego etapu procesu i określić narzędzia, techniki i procedury, z jakich skorzystał atakujący.

WIĘCEJ INFORMACJI

Trendy

_Boty to lukratywny biznes

Boty umożliwiają dokonywanie ataków siłowych typu brute force poprzez wabienie ofiar ofertami zakupu przedmiotów z edycji limitowanych lub przedmiotów w cenach promocyjnych, a następnie ich odsprzedaży za wyższą cenę. Wykryto to, analizując ogłoszenie o pracę, w którym szukano programisty z doświadczeniem w unikaniu mechanizmów zabezpieczających i tworzeniu botów posługujących się technikami unikania (tj. gromadzących dane ze stron internetowych (web scraping), obchodzących reCAPTCHA, generujących pliki cookie itp.). Odpowiedniemu kandydatowi oferowano zarobki rzędu 15 000 USD (ok. 12 750 EUR)[4].

_Silexbot – zmieniający urządzenia w głaz

W czerwcu 2019 r. analityk bezpieczeństwa[17] zbadał nowego bota, opracowanego do zaburzania funkcjonowania niezabezpieczonych urządzeń IoT. Innymi słowy, bot ten był zaprojektowany tak, by przy użyciu znanych/domyślnych danych uwierzytelniających logować się na urządzenia IoT, a następnie je unieruchamiać poprzez kasowanie konfiguracji sieci i dodawanie do tabel numerów IP reguły odrzucania wszystkich połączeń. Oprócz tych możliwości technicznych bot zawierał także ciekawą notatkę.[7] Osoba wysyłająca groźbę przeprasza za swoje działania i wyjaśnia, że mają one na celu zapobieżenie masowemu wykorzystaniu niezabezpieczonych urządzeń IoT w celu budowania botnetów do szkodliwych zastosowań.

_Echobot i nasilający się wektor zagrożenia

W czerwcu 2019 r. analityk bezpieczeństwa zidentyfikował nową wersję programu Echobot. W ramach analizy badacz zaobserwował, że skompilowany na x86 program dał w efekcie wektory ataku wykorzystane przez ten wariant programu Mirai w 26 różnych incydentach[10]. W sierpniu inny analityk bezpieczeństwa zaobserwował zwiększenie częstości występowania Echobota atakującego 50 różnych luk w zabezpieczeniach, w tym „wstrzyknięcie polecenia przez HTTP" (CPAI-2016-0658)[25,26]. W grudniu 2019 r. inny zespół wykrył ulepszoną wersję Echobota obejmującą 71 exploitów. Nowo dodane exploity wykorzystywały stare i nowe luki w zabezpieczeniach, a ponadto miały dodaną istotną opcję pozwalającą na atakowanie urządzeń należących do systemów automatyki przemysłowej (Industrial Control System, ICS). Obejmuje to firmy i urządzenia takie jak Mitsubishi, mechanizmy kontroli działania aplikacji Citrix NetScaler, zaporę dla aplikacji sieciowych Barracuda oraz narzędzia administracyjne w punktach końcowych[27].

_Popularność Necurs spada, a Emotetu ponownie rośnie

W styczniu 2019 r. odnotowano, że sieć Necurs zmienia profil w kierunku amatorskich kampanii rozsyłania spamu, co sugerowało, że stojący za tym botnetem sprawcy szkodliwych działań mają aktualnie znacznie mniejsze umiejętności niż kiedyś[20]. Z kolei aktywność botów Emotet znacznie wzrosła od września 2019 r. i trend wzrostowy utrzymał się do końca 2019, przy czym można było odnaleźć unikatowe, skompilowane kody maszynowe reprezentujące trwałe wektory dostarczania i mechanizmy komunikacyjne[7]. W wyniku analizy wykryto znaczne zwiększenie dystrybucji oprogramowania Emotet za pośrednictwem e-maila[22].

Trendy

_Upadek Retadup – botnetu stojącego za operacją wydobywania kryptowaluty Monero

Retadup to botnet działający przede wszystkim jako robak kopiący walutę Monero, który miał zdolność modyfikacji własnego kodu[23]. Infekował on maszyny Windows w Ameryce Łacińskiej. Bot ten miał wiele funkcji, od wydobywania kryptowaluty po uruchamianie indywidualnego kodu i pobieranie plików na komputery ofiar (odnotowano również rozprowadzanie oprogramowania typu ransomware STOP[24]). Analityk bezpieczeństwa rozpoczął monitorowanie aktywności botnetu Retadup w marcu 2019 r. i zauważył, że protokół C2 zaprojektowano w prosty sposób. Zespół zidentyfikował w tym protokole podatność, dzięki której można było usunąć infekcję z urządzenia ofiary, przejmując serwer C2. Infrastruktura obsługująca tę szkodliwą działalność znajdowała się w większości we Francji. Botnet zlikwidowano przy współpracy żandarmerii francuskiej. Oprogramowanie usunięto z około 850 000 komputerów.

_Umarła Mirai, niech żyje Mirai

Być może to dzięki niedoborowi możliwości i funkcji w pierwotnym kodzie Mirai i jej warianty wciąż dominują wśród rodzin botnetów – w pierwszej połowie 2019 r. odnotowano ponad 20 000 unikatowych przypadków. W wariantach tych wykorzystane są różne techniki atakowania urządzeń IoT – od siłowego ataku typu brute force na domyślne, ustalone hasła po exploity[6]. Warianty te, jak twierdzą dwaj analitycy bezpieczeństwa, atakują szeroki wachlarz architektur systemowych. Więcej statystyk dotyczących aktywności botnetu Emotet przedstawiono na Rysunku 1[7,18].

_Botnet P2P Roboto

W sierpniu 2019 r. zespół analityków bezpieczeństwa po raz pierwszy odnotował aktywność Roboto jako botnetu P2P.Pierwszą przechwyconą próbką był budzący podejrzenia plik ELF. W październiku zespół badawczy zidentyfikował kolejną próbkę (plik ELF), która okazała się być programem do pobierania wyżej wymienionego pliku. W wyniku dalszej analizy zespół badawczy stwierdził, że botnet Roboto ma siedem funkcji: powłoka odwrotna, samoczynna dezaktywacja, gromadzenie informacji dotyczących procesu i sieci, gromadzenie informacji dotyczących botów, wykonywanie plików wskazanych w adresach URL, ataki typu DDoS oraz ataki na systemy. Co ciekawe, według analityka ataki DDoS nie są głównym zastosowaniem tego botnetu. W przeciwieństwie do innych botnetów, ten rozprzestrzeniał się poprzez wykorzystywanie podatności Webmin RCE (CVE-2019-1507[28])[11].

_Mozi – kolejny botnet oparty na DHT

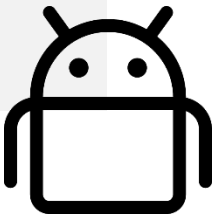
Mozi, nazwany tak od pliku propagacji, został odnotowany przez analityka bezpieczeństwa we wrześniu 2019 r. jako zupełnie nowy botnet oparty na DHT. Wstępna analiza próbki przeprowadzona przez innego analityka bezpieczeństwa[38] wskazała, że jest to program Gafgyt. Taki wynik wziął się jednak stąd, że w badanym programie częściowo wykorzystano kod z Gafgyt. Botnet ten rozprzestrzenia się poprzez kilka exploitów oraz wykorzystanie słabych haseł do protokołu telnet. Analiza funkcji wykazała, że przy użyciu tego botnetu można przeprowadzać ataki typu DDoS, gromadzić dane, wykonywać i aktualizować dany program / oprogramowanie docelowe przy użyciu określonego adresu URL oraz wykonywanych poleceń[29, 30].

Trendy

Statystyka aktywności botnetu Emotet

Aktywność	Liczby
Łączna liczba wykrytych ASn:	5430
Łączna liczba wykrytych unikatowych numerów IP:	120 764
Uczestniczące kraje ogółem:	193
Łączna liczba wysłanych e-maili:	10 935 346
Łączna liczba dystrybucyjnych adresów URL:	4726
Liczba unikalnych odbiorców:	8 052 961

Rysunek 1: Źródło: Spamhaus[5]



„Postęp technologiczny w zakresie przetwarzania rozproszonego i automatyzacji umożliwił sprawcom szkodliwych działań wykorzystywanie nowych technik i ulepszanie narzędzi oraz metod ataku.”

w: ETL 2020

Wnioski

_Statystyki oraz istotne liczby

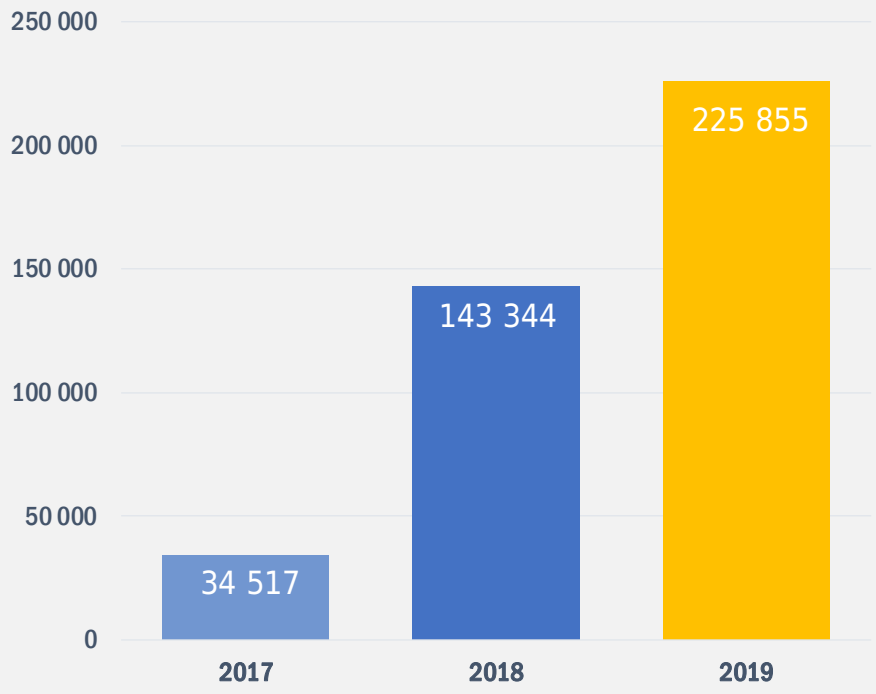
Jak twierdzi jeden z analityków bezpieczeństwa, codziennie do internetu podłączonych jest **7,7 miliona urządzeń IoT** i szacuje się, że tylko 1 na 20 znajduje się za zaporą sieciową lub jest chronione tego rodzaju zabezpieczeniem sieciowym[6]. Oznacza to, że **urządzenia IoT są nadal podatne na** zagrożenia cyberbezpieczeństwa, takie jak botnet Mirai.

- W pierwszej połowie 2019 r. aktywność botnetów i hostingu serwerów C2 znacznie się zwiększyła[32]. Wzrost ten odpowiada za 7% wszystkich zgłoszeń o botnetach i 1,8% zgłoszeń o C2 na świecie. Najczęściej celem ataków były serwisy finansowe i ich klienci.
- W zakresie hostingu serwerów C2 palmę pierwszeństwa wśród krajów dzierży Tajlandia, po niej zaś są Malezja, Filipiny, Singapur i Indonezja.
- Z analiz Interpolu wynika, że w zakresie zgłoszeń wykrycia dominował botnet Andromeda, jakkolwiek został on zdezaktywowany w 2017 r.[33]. Na drugim miejscu znalazł się botnet Conficker[34], a w dalszej kolejności Necurs[35], Sality[36] i Gozi[37].

W 2019 r. liczba wykrytych wariantów Mirai wzrosła o ponad 57% w porównaniu z rokiem 2018 (rysunek 2).

Wprawdzie warianty Mirai wykorzystują przede wszystkim metody ataków siłowych na urządzenia IoT, jednak w 2019 r. zaobserwowano zwiększenie liczby prób zarówno ataku siłowego (51%), jak i ataku przez stronę internetową (87%).

Liczba próbek Mirai



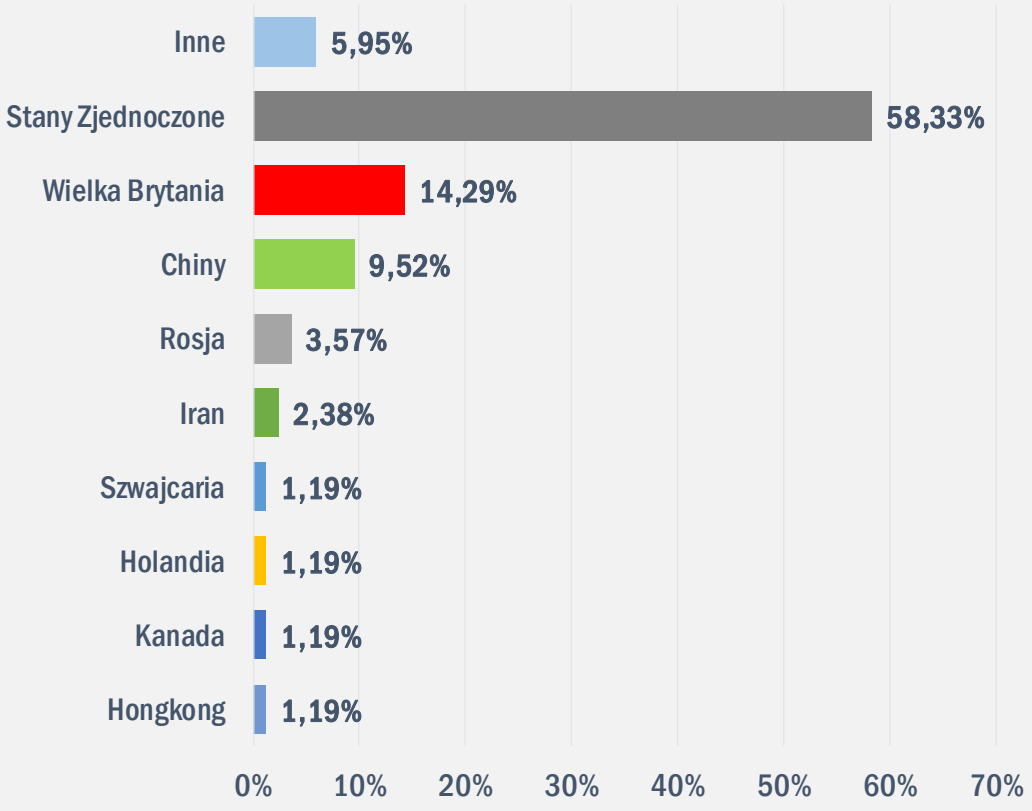
Rysunek 2 – źródło: NETSCOUT[7]

Wnioski

_Statystyki oraz istotne liczby

- W 2019 r. analityk bezpieczeństwa odnotował niemal 300 000 więcej zgłoszeń o ruchu botnetu Emotet i ponad 100 000 więcej zgłoszeń o ofiarach w porównaniu z tym samym okresem w 2018 r. Analityk sądzi, że w drugiej połowie 2019 r. liczba wystąpień Emotet wzrosła o 913% w porównaniu z drugą połową 2018 r.[7,22]
- Aktywność botnetów P2P wzrosła od czasu, gdy zaczęły działać Roboto i Mozi[8].
- Za niemal 97,4% ataków odpowiedzialne były botnety oparte na Linuksie[8].
- Najwięcej botnetów odnotowano w USA (58,33%) w IV kwartale 2019 r. Jest to więcej, niż w III kwartale 2019 r. (47,55%), jednak łączna liczba serwerów C2 zmniejszyła się niemal o połowę. Wielka Brytania z czwartego miejsca wskoczyła na drugie z wynikiem 14,29%, zaś Chiny utrzymały swoje miejsce udziałem 9,52%. Najbardziej znaczący spadek liczby zarejestrowanych serwerów C2 nastąpił w Holandii (z 45% do ~1%). Więcej informacji na temat rozkładu serwerów C2 botnetów w poszczególnych krajach przedstawiono na Rysunku 3[8].
- W 2019 r. na pierwszym miejscu listy botów kradnących dane uwierzytelniające pozostawał LokiBot – aktywność jego serwerów C2 wzrosła o 74% w porównaniu z rokiem 2018. Tuż za LokiBotem, na drugim miejscu, znalazł się AZORult[39].
- W 2019 r. aktywnych było 17 602 serwerów C2 botnetów, co stanowi wzrost o 71,5% w porównaniu z rokiem 2018[39].

Rozkład serwerów C&C botnetów w poszczególnych krajach



Rysunek 3 – źródło: Kaspersky[8]

Wektory ataku

Ataki botnetów

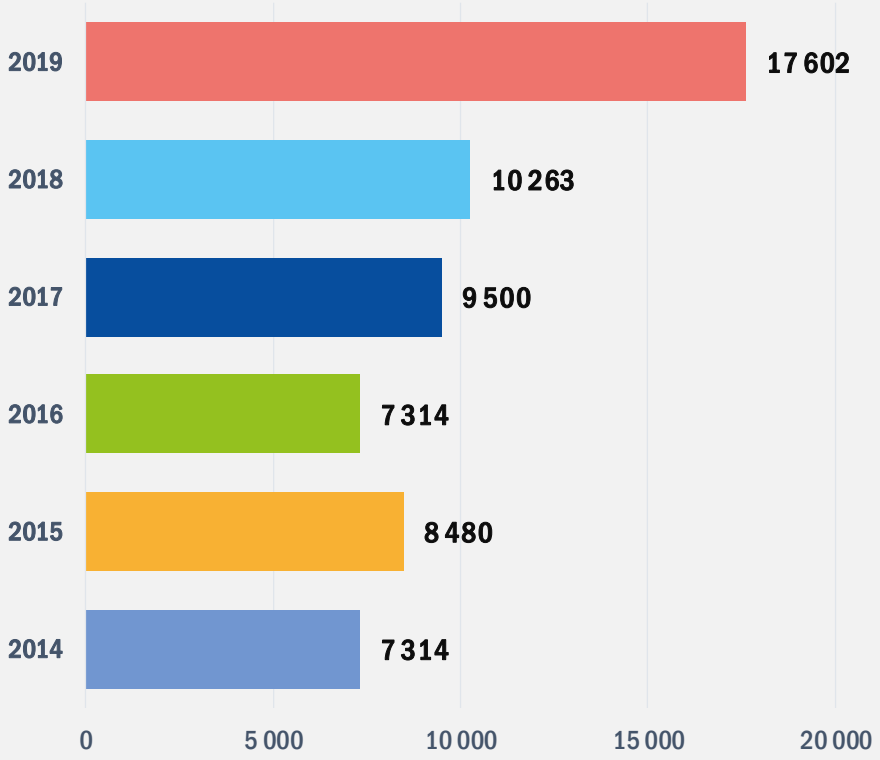
Jak twierdzi analityk bezpieczeństwa, w 2019 r. niemal 60% aktywności nowych, konkurencyjnych botnetów związana była z **kradzieżą danych uwierzytelniających**. Jak już wspomniano, najbardziej aktywny w tym obszarze jest LokiBot. Oprócz aktywności związanej z kradzieżą danych uwierzytelniających botnet ten działa również na dużą skalę w dziedzinie **bankowości elektronicznej i oszustw finansowych**. Główne przykłady tej działalności to Emotet i TrickBot, w których stosowany jest nowszy model obejmujący nie tylko oszustwa związane z bankowością elektroniczną, ale też płatności za instalację (pay-per-install, PPI)[9].

Ponadto wśród najczęściej wykorzystywanych narzędzi w sterowaniu botnetami znalazły się **trojany dostępu zdalnego (Remote Access Trojans, RAT)**. W 2018 r. większość tej aktywności związana była z programem Adwind, jednak w 2019 r. jego aktywność spadła na rzecz NanoCore[5].

W 2019 r. pojawiły się szczególne wektory ataku. Botnety wykorzystują różne wektory ataku, aby osiągnąć cele. Zainfekowane maszyny lub sieci zombie powstają w taki sposób, że powszechnie występujące podatności atakowane są siłowo i innymi często spotykanymi technikami infekcji[10,11,12]. Zarządzający botami może następnie udostępnić platformę dla różnych ataków, w tym szeroko zakrojonych akcji wysyłania spamu i złośliwego oprogramowania, kradzieży i ponownego wykorzystywania danych uwierzytelniających, wydobywania kryptowalut i ataków DDoS.

Innym przykładem wektora ataku wykorzystywanego przez botnety jest mechanizm **„potrójnego zagrożenia"**. Polega to na tym, że atakowana organizacja zostaje najpierw zainfekowana złośliwym oprogramowaniem Emotet. Następnie oprogramowanie Emotet umieszcza w sieci trojana TrickBot, którego działanie ukierunkowane jest na zdobywanie i badanie informacji wrażliwych. W razie znalezienia takich informacji, jeśli dane środowisko/sieć znajduje się na liście atakującego, instalowane jest oprogramowanie wymuszające okup Ryuk[13].

Liczba odnotowanych serwerów C2 botnetów w latach 2014–2019



Rysunek 4 – źródło: Spamhaus[5]

Ograniczenie ryzyka

_ Proponowane działania

Jednym z kluczowych aspektów mocnej ochrony jest koncepcja znajomości środowiska. Pomoże to w zidentyfikowaniu szkodliwej aktywności na podstawie pomiaru różnic w ruchu sieciowym w porównaniu z ewentualnym poziomem bazowym (tj. analiza behawioralna)[14] przy użyciu narzędzia do monitorowania sieci[4]. Znaczna część ruchu sieciowego botnetów wiąże się z atakami typu DDoS; mają zatem zastosowanie również techniki przeciwdziałania tym atakom.

- Wdrożenie kanałów protokołów bram sieciowych wyszukujących dTLD (decentralised top-level domains – zdecentralizowane domeny najwyższego poziomu) mających na celu blokowanie połączeń z adresami IP związanymi z aktywnością C2 botnetów.[8].
- Zrozumienie i kategoryzacja słabych punktów oraz wdrożenie zdecydowanych zasad instalowania łatek bezpieczeństwa i aktualizacji[15,16].
- Ograniczenie lub blokada infrastruktury wydobywania kryptowalut i monitorowanie środowiska dla użytkowników, dla których jest to wymagane[5].
- Wdrożenie testów odpowiedzi na wyzwanie w witrynach, w których jest to wymagane, w celu sprawdzenia pochodzenia ruchu (np. reCAPTCHA)[16].
- Wdrożenie zasad stosowania mocnych haseł i uwierzytelniania (2FA) na serwerach i infrastrukturze, które są dostępne publicznie, aby uniknąć padnięcia ofiarą wykorzystania słabych haseł / słabego uwierzytelniania[5].
- Wdrożenie i konfiguracja zapór w sieci i w aplikacjach.

„Rok 2019 przyniósł wzrost wyrafinowania potencjalnych zagrożeń w związku z używaniem przez wielu cyberprzestępców exploitów, kradzieży poświadczeń i ataków wieloetapowych”.

w: ETL 2020

Bibliografia

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

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

3. „ASEAN Cyberthreat Assessment 2020". 17 lutego 2020 r. 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: Volume 5, Issue 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 stycznia 2020 r. 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. NETS. https://www.netscout.com/threatreport

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

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

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

11. „The awaiting Roboto Botnet". 20 listopada 2019 r. 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 października 2019 r. 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 kwietnia 2019 r. 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 października 2018 r. 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 czerwca 2019 r. Akamai.

18. „Mirai Botnet Continues to Plague IoT Space". 10 września 2019 r. 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" 27 stycznia 2020 r. Threat Post. https://threatpost.com/as-necurs-botnet-falls-from-grace-emotet-rises/152236/

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

22. „Estimating Emotet's size and reach". 12 grudnia 2019 r. 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 kwietnia 2018 r. 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 września 2019 r. Bleeping Computer. https://www.bleepingcomputer.com/news/security/meet-stop-ransomware-the-most-active-ransomware-nobody-talks-about/

25. „Command Injection Over HTTP". 26 lipca 2016 r. 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". Sierpień 2019 r. 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 grudnia 2019 r. 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 lipca 2019 r. 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 grudnia 2017 r. 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 listopada 2016 r. 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 kwietnia 2017 r. https://securityintelligence.com/the-necurs-botnet-a-pandoras-box-of-malicious-spam/

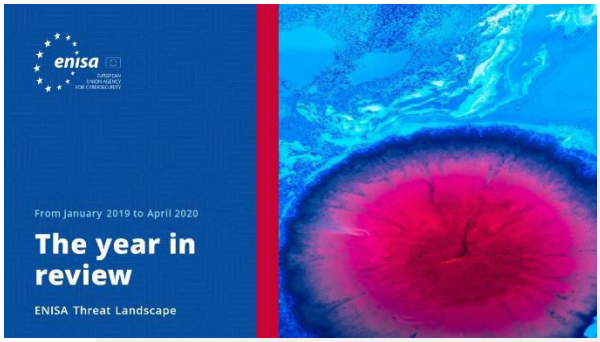
36. „WhitePaper: Sality: Story of a Peer to-Peer Viral Network". 10 czerwca 2011 r. Broadcom.

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

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

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

Powiązany



Raport ENISA o krajobrazie zagrożeń **Przegląd roku**

Zestawienie trendów w cyberbezpieczeństwie w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Wykaz piętnastu największych zagrożeń

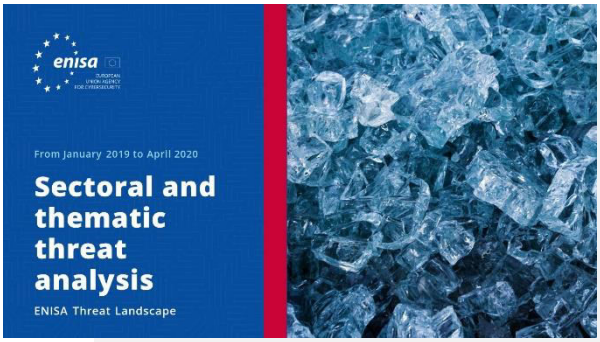
Agencja ENISA: wykaz piętnastu największych zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Tematyka badań

Zalecenia dotyczące tematów badawczych z różnych kwadrantów w dziedzinie cyberbezpieczeństwa i rozpoznawania zagrożeń cybernetycznych.

PRZECZYTAJ RAPORT



Raport ENISA o krajobrazie zagrożeń
Sektorowa i tematyczna analiza zagrożeń

Kontekstualna analiza zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Nowe trendy

Główne trendy w cyberbezpieczeństwie w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Omówienie kwestii rozpoznawania cyberzagrożeń

Aktualny stan wywiadu dotyczącego cyberzagrożeń w UE.

PRZECZYTAJ RAPORT

Informacje o agencji

_ Agencja

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) jest unijną agencją działającą na rzecz osiągnięcia wysokiego ogólnego poziomu cyberbezpieczeństwa w całej Europie. Utworzona w roku 2004 i wzmocniona przez Akt o cyberbezpieczeństwie Agencja Unii Europejskiej ds. Cyberbezpieczeństwa wnosi wkład w politykę cybernetyczną UE; zwiększa wiarygodność produktów, usług i procesów informacyjno-komunikacyjnych dzięki systemom certyfikacji cyberbezpieczeństwa; współpracuje z państwami członkowskimi i organami UE oraz pomaga przygotować Europę na przyszłe wyzwania cybernetyczne. Poprzez wymianę informacji, budowanie zdolności i pogłębianie wiedzy Agencja współdziała z kluczowymi zainteresowanymi stronami, aby zwiększać zaufanie do gospodarki opartej na łączności i odporność unijnej infrastruktury oraz w efekcie zapewnić cyfrowe bezpieczeństwo społeczeństwa i mieszkańców Europy. Więcej informacji na temat ENISA i jej działalności można znaleźć na stronie www.enisa.europa.eu.

Współautorzy

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) oraz *wszyscy członkowie 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) i Thomas Hemker.

Wydawcy

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

Dane kontaktowe

Zapytania dotyczące tego dokumentu można kierować na adres enisa.threat.information@enisa.europa.eu.

Zapytania prasowe dotyczące tego dokumentu można kierować na adres press@enisa.europa.eu.

Chcielibyśmy poznać opinie czytelników na temat tego raportu!
Poświęć chwilę, by wypełnić kwestionariusz. Aby uzyskać dostęp do formularza, kliknij tutaj.

Zastrzeżenia prawne

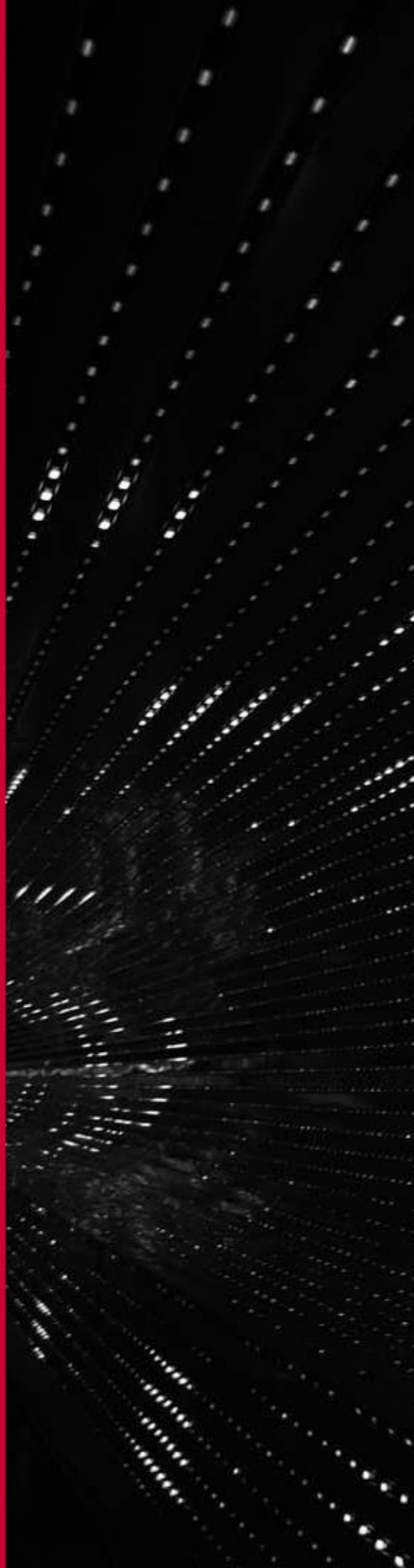
Informujemy, że niniejsza publikacja przedstawia poglądy i interpretacje ENISA, o ile nie stwierdzono inaczej. Niniejsza publikacja nie powinna być interpretowana jako działanie prawne ENISA ani organów ENISA, chyba że została przyjęta zgodnie z rozporządzeniem (UE) nr 526/2013. Niniejsza publikacja nie musi przedstawiać aktualnego stanu wiedzy i ENISA może ją okresowo aktualizować.

Źródła zewnętrzne zostały odpowiednio zacytowane. ENISA nie ponosi odpowiedzialności za treść źródeł zewnętrznych, w tym zewnętrznych stron internetowych, do których odniesienia znajdują się w niniejszej publikacji.

Niniejsza publikacja ma charakter wyłącznie informacyjny. Musi ona być dostępna nieodpłatnie. Ani ENISA, ani żadna osoba działająca w jej imieniu nie ponoszą odpowiedzialności za wykorzystanie informacji zawartych w niniejszym sprawozdaniu.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

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