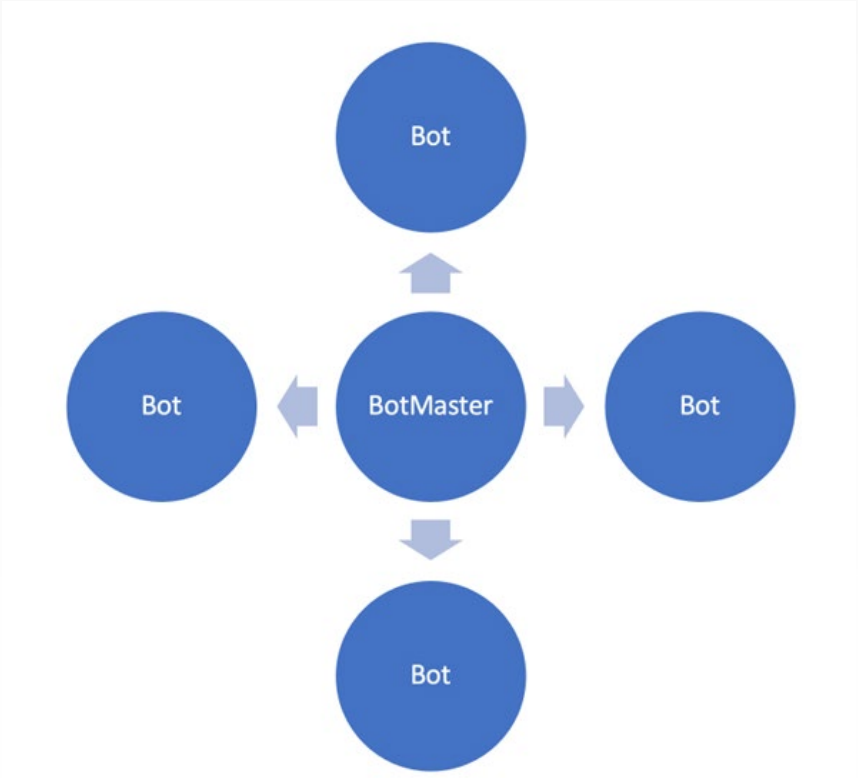
fundacja instytut
CYBERBEZPIECZEŃSTWA

Botnety

- zagrożenia i przeciwdziałanie

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

Botnet to sieć komputerów, nad którymi została przejęta kontrola poprzez zainfekowanie ich złośliwym oprogramowaniem. Haker zarządzający siecią ma kontrolę nad innymi urządzeniami elektronicznymi i może je wykorzystywać do różnych celów w sposób niezauważony i bez ponoszenia większych kosztów. Kluczowe dla cyberprzestępcy w przypadku botnetów jest, aby ofiara jak najdłużej pozostawała nieświadoma, że jej sprzęt został zainfekowany. Każdy botnet jest kontrolowany przez BotMastera, który zarządza całą siecią i wydaje polecenia zainfekowanym komputerom.



Do czego są wykorzystywane?

Botnety mogą być wykorzystywane przez przestępców do różnych celów, takich jak rozsyłanie spamu czy rozprzestrzenianie wirusów. Duża liczba kontrolowanych komputerów może być używana także do ataków DDoS (Distributed Denial of Service), czyli rozproszonej odmowy usługi, które są wymierzone w systemy komputerowe bądź usługi sieciowe1. Celem DDoS jest zakłócenie działania usług i doprowadzenie do przerwania ciągłości działań operacyjnych systemu, co osiąga się przez przeprowadzenie ataku równocześnie z wielu komputerów. Haker zatem, nie posiadając dużej liczby komputerów, może zainfekować inne komputery, stworzyć tym samym botnet i za jego pomocą przeprowadzić atak DDoS.

Coraz częstszym przykładem wykorzystania botnetów jest także cryptojacking, czyli złośliwe wydobywanie kryptowalut. Polega ono na zainstalowaniu na cudzych komputerach złośliwego oprogramowania, które wykorzystuje ich zasoby do kopania kryptowalut, czyli rozwiązywania skomplikowanych działań matematycznych. Wydobywanie kryptowalut zużywa ogromne ilości energii elektrycznej i eksploatuje wykorzystywany do tego sprzęt2. Ze względu na wysokie ceny energii staje się to coraz droższe i mniej opłacalne. Jeśli jednak haker dysponuje siecią zainfekowanych komputerów, które zdalnie kontroluje, może wykorzystać je do kopania kryptowalut i osiągać w związku z tym duże zyski. Im większą liczbą komputerów dysponuje haker, tym lepsze wyniki może osiągać. Osoby, których komputery zostały zainfekowane, będą ponosić większe koszty energii, a ich sprzęt może się szybciej zużyć.

1 *Botnet Definition: What Is a Botnet and How Does It Work?*, Radware, https://www.radware.com/cyberpedia/bot-management/botnet/ [dostęp: 26.06.2023].

2 L. Klusaitė, *Co to jest cryptojacking i jak się przed nim bronić?*, NordVPN, 29.03.2023 r., https://nordvpn.com/pl/blog/co-to-jest-cryptojacking/ [dostęp: 26.06.2023].

Przykłady botnetów

Przykładem popularnego botnetu był Emonet, który po raz pierwszy został zauważony w 2014 roku, gdy złośliwe oprogramowanie zaatakowało klientów niemieckich i austriackich banków3. W kolejnych latach Emonet rozszerzał swoje działania i stwarzał coraz większe zagrożenie. Oferował m.in. usługę dla cyberprzestępców, którzy po dokonaniu opłaty mogli zainstalować inne złośliwe oprogramowanie na urządzeniach zainfekowanych już przez Emonet. Stworzył także takie złośliwe oprogramowania jak Qbot, TrickBot oraz ransomware Ryuk. Wirusy dystrybuowano przede wszystkim drogą mailową poprzez złośliwe dokumenty. Twórcy Emoneta byli w stanie zarazić duże sieci korporacyjne po tym, jak zainfekowali zaledwie kilka urządzeń danej sieci. W styczniu 2021 roku dzięki międzynarodowej operacji organów ścigania przejęto kontrolę nad infrastrukturą Emonetu4. W działania były zaangażowane służby z różnych państw, takich jak Holandia, Niemcy, USA, Wielka Brytania czy Francja, a operację koordynowały Europol i Eurojust5. Nie zlikwidowała ona jednak całkowicie Emonetu, który powrócił i rozpoczął nową kampanię dystrybucji złośliwego oprogramowania. W raporcie Any Run Emonet został uznany za drugą największą sieć rozprzestrzeniającą złośliwe oprogramowania6.

Innym przykładem botnetu jest botnet Mirai, stworzony przez Josiaha White'a, Parasa Jha i Daltona Normana. Początkowo jego celem było wyłączenie serwerów Minecraft za pomocą ataków DDoS, ale szybko rozprzestrzenił się, infekując tysiące urządzeń internetu rzeczy (Internet of Things, IoT) i zaczął przeprowadzać ataki na dużą skalę. Pierwszy z nich miał miejsce w 2016 roku i był wymierzony we francuską firmę technologiczną OVH. Do ataku wykorzystano wówczas około 145 tys. urządzeń7. W 2017 roku jeden z twórców tego botnetu opublikował kod źródłowy na popularnym forum

3 *World's most dangerous malware EMOTET disrupted through global action*, Europol, 27.01.2021 r., https://www.europol.europa.eu/media-press/newsroom/news/world's-most-dangerous-malware-emotet-disrupted-through-global-action [dostęp: 26.06.2023].

4 J. Bielaszewski, *Duży cios Europolu w botnet Emotet – przejęli jego infrastrukturę*, Sekurak, 27.01.2021 r., https://sekurak.pl/duzy-cios-europolu-w-botnet-emotet-przejeli-jego-infrastrukture-wymusili-rowniez-automatyczna-dezinstalacje-z-zainfekowanych-komputerow-25-marca-2021/ [dostęp: 26.06.2023].

5 S. Palczewski, *Sukces Europolu. Potężny botnet „na kolanach"*, CyberDefence24, 28.01.2021 r., https://cyberdefence24.pl/armia-i-sluzby/sukces-europolu-potezny-botnet-na-kolanach [dostęp: 26.06.2023].

6 *Annual Report 2022*, AnyRun, https://any.run/cybersecurity-blog/annual-report-2022/ [dostęp: 26.06.2023].

7 *The Mirai Botnet – Threats and Mitigations*, CIS, https://www.cisecurity.org/insights/blog/the-mirai-botnet-threats-and-mitigations [dostęp: 26.06.2023].

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości

hakerskim i ogłosił, że rezygnuje z hakowania. Celem tej deklaracji było prawdopodobnie ukrycie swojej tożsamości i uniknięcie odpowiedzialności za popełnione przestępstwa. Publikacja kodu doprowadziła jednak do tego, że inni zaczęli wykorzystywać Mirai do własnych złośliwych celów.

Jak rozpoznać, czy mamy złośliwe oprogramowanie na komputerze?

Cyberprzestępcom wykorzystującym botnet zależy na tym, aby ofiara jak najdłużej pozostała nieświadoma, że jej komputer został zainfekowany. Złośliwe oprogramowanie działa w tle i jest trudne do zidentyfikowania. Najlepszy sposób na jego wykrycie to instalacja programu antywirusowego i przeprowadzenie skanowania w poszukiwaniu podejrzanych treści. Dobrze wykonywać tego typu weryfikację regularnie. Może zdarzyć się tak, że darmowy program antywirusowy nie wykryje wirusa, więc jeżeli istnieją podejrzenia, że komputer został zaatakowany przez cyberprzestępców, warto przeprowadzić weryfikację bardziej zaawansowanymi programami antywirusowymi. W ostateczności można także przywrócić ustawienia fabryczne, co powinno usunąć większość wirusów. Warto także zwracać uwagę na pracę komputera, ponieważ zainfekowany sprzęt może pracować wolniej lub szybciej się przegrzewać, gdyż hakerzy zarządzający botnetami używają go do innych aktywności. Jest to widoczne zwłaszcza wtedy, gdy hakerzy wykorzystują go do kopania kryptowalut, co w dużym stopniu eksploatuje dane urządzenie. Jednocześnie należy pamiętać, że spowolniona praca komputera nie musi do razu świadczyć o tym, że został on zainfekowany. Gorsza jakość pracy urządzenia może wynikać także z innych czynników, takich jak zbyt mała pojemność pamięci RAM, kończące się wolne miejsce na dysku czy nieaktualny system operacyjny.

Jak chronić się przed złośliwym oprogramowaniem?

Kluczowym aspektem ochrony przed złośliwym oprogramowaniem jest stosowanie dobrego programu antywirusowego. Taki program skanuje, wykrywa, rozpoznaje i usuwa złośliwe oprogramowanie z komputera. Proces przeszukiwania może odbywać się na żądanie, co polega na uruchomieniu przeszukiwania komputera ręcznie przez użytkownika, albo w czasie rzeczywistym – np. w czasie pobierania plików program automatycznie sprawdza poziom bezpieczeństwa pliku i gdy wykryje złośliwe oprogramowanie, natychmiast reaguje i proponuje usunięcie lub zablokowanie pliku.

Antywirus może skutecznie przeciwdziałać złośliwym oprogramowaniom, ale nie daje stuprocentowej gwarancji, dlatego istotne jest zachowanie ostrożności w internecie. Nie należy pobierać podejrzanych programów ani plików. W szczególności powinno się zwracać uwagę na możliwe ataki phishingowe, bazujące na inżynierii społecznej. Polega ona na tym, że cyberprzestępcy próbują spowodować podjęcie przez ofiarę działań zgodnych z ich zamierzeniami. Może to być np. otworzenie linku wysłanego mailowo, który po kliknięciu instaluje złośliwe oprogramowanie. Należy także uważać na otwierane przez nas załączniki. Mogą być one rozsyłane przez przestępców w mailach phishingowych. Takie załączniki zaatakują komputer, gdy zostaną pobrane. Wirus może też zostać ściągnięty na urządzenie po otworzeniu zainfekowanej strony internetowej.

Bardo ważnym elementem ochrony przez wirusami jest także regularne aktualizowanie oprogramowania komputera. Aktualizacje te zawierają często naprawę luk w bezpieczeństwie, które są wykorzystywane przez hakerów do ataków na urządzenia. Warto też regularnie aktualizować swój program antywirusowy oraz przeglądarki internetowe, a także inne programy lub aplikacje. Dzięki temu znacznie zwiększymy bezpieczeństwo danego sprzętu.

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości

Podsumowanie

Botnety stanowią duże zagrożenie i są wykorzystywane do różnych celów. Za pomocą sieci zainfekowanych komputerów hakerzy mogą dokonywać ataków na dużą skalę, wyrządzających poważne szkody. Zagrożenia w cyberprzestrzeni rosną, dlatego należy stosować odpowiednie środki bezpieczeństwa, aby chronić się przed złośliwym oprogramowaniem. Kluczową rolę odgrywają w tym kontekście programy antywirusowe oraz ostrożne korzystanie z internetu.

Bibliografia:

1. *Annual Report 2022*, AnyRun, https://any.run/cybersecurity-blog/annual-report-2022/ [dostęp: 26.06.2023].
2. *Botnet Definition: What Is a Botnet and How Does It Work?*, Radware, https://www.radware.com/cyberpedia/bot-management/botnet/ [dostęp: 26.06.2023].
3. Bielaszewski J., *Duży cios Europolu w botnet Emotet – przejęli jego infrastrukturę*, Sekurak, 27.01.2021 r., https://sekurak.pl/duzy-cios-europolu-w-botnet-emotet-przejeli-jego-infrastrukture--wymusili-rowniez-automatyczna-dezinstalacje--z-zainfekowanych-komputerow-25-marca-2021/ [dostęp: 26.06.2023].
4. Klusaitė L., *Co to jest cryptojacking i jak się przed nim bronić?*, NordVPN, 29.03.2023 r., https://nordvpn.com/pl/blog/co-to-jest-cryptojacking/ [dostęp: 26.06.2023].
5. Palczewski S., *Sukces Europolu. Potężny botnet „na kolanach”*, CyberDefence24, 28.01.2021 r., https://cyberdefence24.pl/armia-i-sluzby/sukces-europolu-potezny-botnet-na-kolanach [dostęp: 26.06.2023].
6. *The Mirai Botnet – Threats and Mitigations*, CIS, https://www.cisecurity.org/insights/blog/the-mirai-botnet-threats-and-mitigations [dostęp: 26.06.2023].
7. *World’s most dangerous malware EMOTET disrupted through global action*, Europol, 27.01.2021 r., https://www.europol.europa.eu/media-press/newsroom/news/world’s-most-dangerous-malware-emotet-disrupted-through-global-action [dostęp: 26.06.2023].

www.instytutcyber.pl

fundacja instytut
CYBERBEZPIECZEŃSTWA

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości