

## Brytyjska policja prowadzi fałszywe witryny DDoS w celu zbierania informacji o cyberprzestępcach

28.03.2023

Brytyjska Narodowa Agencja ds. Przestępczości (NCA) ujawniła, że stworzyła szereg witryn udających usługi „DDoS-for-hire” lub „booter”. Dzięki temu użytkowników Internetu chcących zaszkodzić stronom internetowym może spotkać niemiła niespodzianka: zamiast zatrudnić cyberprzestępców do bombardowania witryny niepożądanym ruchem lub wyrzucania rywali z gry wideo, mogą przekazać swoje dane bezpośrednio policji.

Wiadomości o honeypotach „DDoS-for-hire” wyszły na jaw po tym, jak NCA zdecydowała się zmienić stronę docelową jednej z witryn typu „DDoS-for-hire”, aby ogłosić, że została ona zawieszona, a użytkownicy mogą spodziewać się kontaktu ze strony organów ścigania.

**Operacja PowerOFF – Brytyjska policja prowadzi fałszywe**  
Brytyjska policja prowadzi fałszywe witryny DDoS w celu zbierania informacji o cyberprzestępcach **Bitdefender®**

## witryny DDoS

Narodowa Agencja ds. Przestępczości współpracowała w ramach operacji PowerOFF, aby atakować użytkowników przestępczych usług DDoS.

„NCA zebrała istotne dane od osób, które uzyskały dostęp do naszej domeny” – powiedział Alan Merrett z National Cyber Crime Unit NCA. – „Udostępnimy te dane międzynarodowym organom ścigania w celu podjęcia działań śledczych. Organy ścigania skontaktują się z osobami w Wielkiej Brytanii, które korzystały z tej witryny”.

Operacja PowerOFF doprowadziła już do aresztowania wielu osób, a NCA zapewnia, że pociągnie winnych użytkowników do odpowiedzialności za ich działalność przestępczą.

„Tradycyjne usuwanie witryn i aresztowania to kluczowe elementy reakcji organów ścigania na zagrożenie atakami DDoS. Jednak dzięki operacji PowerOFF rozszerzyliśmy nasze możliwości, jednocześnie podważając zaufanie do rynku przestępczego” – wyjaśnił Alan Merrett z National Cyber Crime Unit NCA. – „Nie ujawnimy, ile mamy witryn ani w jaki sposób będziemy zbierać dane o internautach szukających usług cyberprzestępców. Ludzie, którzy chcą korzystać z tych stron, nie mogą być pewni, kto tak naprawdę za nimi stoi.”

Organy ścigania na całym świecie często przyglądają się stronom, które umożliwiają przeprowadzenie ataku DDoS. Na przykład pięć lat temu

Brytyjska policja prowadzi fałszywe witryny DDoS w celu zbierania informacji o cyberprzestępcach

**Bitdefender**

policja aresztowała administratora platformy webstresser.org i przejęła kontrolę nad jej serwerami oraz bazą danych ponad 136 000 użytkowników. W rezultacie tej policyjnej akcji wielu podejrzanych klientów Webstresser stanęło w obliczu aresztowania i postawienia zarzutów karnych .

## **Młodociani cyberprzestępcy**

Jak wcześniej zauważył rzecznik prasowy NCA, osoby korzystające z witryn DDoS do wynajęcia to często bardzo młodzi internauci. Zwrócił także uwagę, że liczba ataków przeprowadzonych na systemy szkolne wzrosła ponad dwukrotnie w latach 2019-2020.

Według NCA średni wiek osób korzystających z usługi rozruchowej DDoS wynosi zaledwie piętnaście lat, a najmłodszy „kryminalista” zarejestrowany w aktach policyjnych ma zaledwie dziewięć lat.

„Skala ataków DDoS w ostatnich latach znacząco wzrosła. Szczególnie niepokojące jest to, że osoby odpowiedzialne za incydenty tego typu są coraz młodsze, a cele ataków bardziej bezmyślne. Do niedawna większość ataków DDoS była skierowana przeciwko stronom rządowym, stronom podmiotów infrastruktury krytycznej, placówek medycznych i portali informacyjnych. Celem takich działań było zastraszenie opinii publicznej i wprowadzenie zamętu medialnego w obliczu wojen i innych ważnych wydarzeń. Niestety coraz częściej ataki DDoS są przeprowadzane przez uczniów strojących sobie żarty w formie wyłączania stron internetowych swoich szkół. Musimy pamiętać, że takie

działania są nielegalne w większości krajów, a ich skutki mogą być nie tylko bardzo kosztowne dla rodziców młodocianych hakerów, lecz także mogą zakończyć się odsiadką w zakładzie karnym” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Ten niebezpieczny trend sprawił, że NCA zorganizował kampanię Cyber Choices, która za pomocą specjalnych komunikatów umieszczanych w wyszukiwarkach uświadamia młodym ludziom konsekwencje popełnienia cyberprzestępstwa.

Miejmy nadzieję, że do internautów dotrze wiadomość, że policja inwestuje środki w dochodzenie w sprawie klientów usług „DDoS-for-hire” i jest gotowa postawić ich przed wymiarem sprawiedliwości.

Źródło: <https://bitdefender.pl/policja-prowadzi-falszywe-witryny-ddos/>

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 28.03.2023

Z pozdrowieniami Piotr Rozmiarok

E-mail: [piotr.r@marken.com.pl](mailto:piotr.r@marken.com.pl) | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender

Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie Brytyjska policja prowadzi fałszywe witryny DDoS w celu **Bitdefender** zbierania informacji o cyberprzestępcach

dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.