Bitdefender

Dark Frost Botnet atakuje branżę gier

02.06.2023

Eksperci do spraw cyberbezpieczeństwa zidentyfikowali botnet o nazwie Dark Frost Botnet, który bezpośrednio atakuje deweloperów gier komputerowych. Złośliwe oprogramowanie, które zagraża branży elektronicznej rozrywki, składa się z kodu skradzionego z podobnych projektów hakerskich, takich jak Mirai i Qbot. Szczególnie interesujące w tym wypadku jest zachowanie hakera odpowiedzialnego za ataki, który zamiast ukryć swoją tożsamość, prowadzi transmisję online ze swojej przestępczej działalności.

Dark Frost Botnet – geneza

„Botnet to duża sieć botów, czyli komputerów zainfekowanych przez złośliwe oprogramowanie typu malware. Na skutek cyberataku kontrolę nad tymi urządzeniami przejmuje haker, który może je wykorzystać do dalszej dystrybucji złośliwego oprogramowania, przeprowadzania ataków DDoS i tworzenia kampanii phishingowych. Aktualnie botnety są jednym z największych zagrożeń w nowoczesnym Internecie” – mówi

Mariusz Politowicz z firmy Marken, polskiego dystrybutora oprogramowania Bitdefender.

Botnety takie jak Mirai często przyciągają uwagę mediów, ale świat online jest pełen mniejszych projektów tworzonych przez cyberprzestępców. Haker, który przeprowadził niedawne ataki na deweloperów gier komputerowych, wziął kod z kilku znanych fragmentów złośliwego oprogramowania (Gafgyt, Qbot, Mirai) i stworzył swoją własną wersję botnetu.

Cyberprzestępca, który stoi za stworzeniem Dark Frost Botnet, celował w źle skonfigurowane serwery Hadoop YARN, które umożliwiłyby mu wdrożenie tego zagrożenia poprzez zdalne wykonanie kodu.

„Wykorzystanie tej błędnej konfiguracji serwerów YARN staje się ostatnio coraz bardziej popularne, ponieważ nie przypisano jej CVE i pozwala ona cyberprzestępcom nakłonić serwer do pobrania i uruchomienia złośliwego pliku binarnego" — wyjaśniają badacze bezpieczeństwa Akamai. – „Należy jednak zauważyć, że ta luka istnieje od 2014 r., co czyni ją daleką od nowatorskiej techniki".

Cybercelebryta

Tym co czyni ten Dark Frost Botnet jeszcze bardziej interesującym, jest to, że jego autor nie tylko nie próbuje ukryć swojej tożsamości, ale wręcz bierze na siebie odpowiedzialność za ataki i chwali się możliwościami oprogramowania.

„Haker rozpoczął ataki DDoS na firmy zajmujące się grami, dostawców hostingu serwerów gier, streamerów online, a nawet na innych członków społeczności graczy, z którymi miał bezpośrednią interakcję” – dodali badacze. – „Cyberprzestępca stojący za tymi atakami opublikował nagrania z ich przebiegu, aby wszyscy mogli je zobaczyć”.

Ataki DDoS powstałe dzięki Dark Frost Botnetowi osiągają szczytową prędkość 629,28 Gb/s – wystarczającą do naruszenia usług online nawet dla dużych firm.

Przestępca zaatakował serwery ze starym problemem bezpieczeństwa, ale mimo to naruszył setki z nich. Nawet niedoświadczony haker może wyrządzić znaczne szkody, więc wyobraźmy sobie, co może osiągnąć dobrze finansowana grupa.

Źródło: https://bitdefender.pl/dark-frost-botnet-atakuje-branze-gier/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 02.06.2023
Z pozdrowieniami Piotr Rozmiarek
E-mail: 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

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.