**Nowy botnet Gameover Zeus rośnie w siłę**

**Nowe złośliwe oprogramowanie Gameover Zeus zainfekowało już ponad 10000 systemów.**

Cyberprzestępcy pracują nad przebudowaniem botnetu Gameover Zeus (GOZ), którego organy ścigania przejęły w czerwcu. Z najnowszych obserwacji wynika, że botnet osiąga już pewne sukcesy, szczególnie w Stanach Zjednoczonych.

Pierwsza wersja GOZ została zbudowana przy użyciu niesławnej wersji trojana Zeus, który został zaprojektowany do kradzieży danych uwierzytelniających do bankowości internetowej z zainfekowanych komputerów. Autorzy GOZ stworzyli odpowiednią infrastrukturę do zarządzania i kontroli o architekturze peer-to-peer, dzięki czemu botnet jest odporny na próby przejęcia.

Pomimo wyzwań technicznych amerykański Departament Sprawiedliwości, we współpracy z organem egzekwowania prawa zagranicznego oraz prywatnymi firmami zajmującymi się bezpieczeństwem na początku czerwca przejął kontrolę nad botnetem. Szacuje się, że zainfekowano od 0,5 do 1 mln komputerów, z czego 25% znajduje się w USA.

11 lipca naukowcy z firmy Malcovery Security zauważyli nowy wariant Gameover Zeus, który przestał używać infrastruktury peer-to-peer do zarządzania na rzecz nazwy domen.

Większość szkodliwego oprogramowania jest skonstruowana tak, że podłącza się do niezmiennej listy domen związanych z serwerami zarządzającymi. Jednak nowa wersja GOZ wykorzystuje algorytm generowania domeny (DGA), aby utworzyć listę setek albo tysięcy nowych przypadkowo wyglądających domen każdego dnia, a następnie próbuje się z nimi połączyć.

Wiedząc, w jaki sposób działa DGA, atakujący jest w stanie przewidzieć, z jaką domeną program będzie próbował skontaktować się w danym dniu. Dzięki tej wiedzy mogą zarejestrować się do jednej z domen, przypisać ją do serwera i czekać aż zainfekowane komputery połączą się w celu uzyskania nowych instrukcji.

To sprawia, że testerom bezpieczeństwa jest trudno przejąć kontrolę nad botnetem, ponieważ nowe domeny są generowane na stałe. Jednak jest na to pewien sposób - utworzenie algorytmu i zarejestrowanie kilku domen, które mogą czasowo wchodzić w interakcję z botnetem. Ten rodzaj operacji nosi nazwę sinkholing i może być stosowany do oceny liczby zakażonych układów, które są częścią botnetu.

Według zeszłotygodniowego raportu przygotowanego przez naukowców z firmy Bitdefender istnieją dwie nowe konfiguracje GOZ, które używają różnych algorytmów generacji nazwy domeny – jeden generuje 1000 nazw domen dziennie, a drugi generuje ich aż 10000. Bitdefender wyliczył, dzięki sinkholing, że pięć domen przez ponad pięć dni dla pierwszego z wariantów zaraziło 5907 komputerów z unikalnym adresem IP - prawie 84% z nich jest z USA. Drugi wariant GOZ zaraził 4316 adresów IP, z czego 70% było z Ukrainy i Białorusi.

Liczenie adresów IP nie jest dokładnym sposobem na ustalenie wielkości botnetu, ponieważ niektóre komputery otrzymują inne adresy IP od swojego dostawcy usług internetowych podczas każdego połączenia z Internetem. Jednak przy braku lepszej identyfikacji, można w ten sposób oszacować ich wstępną liczbę.

Naukowcy z Abor Networks również badali GOZ poprzez sinkholding nazw domen w lipcu, ale robili to, co cztery dni, w celu ustalenia, w jaki sposób zmienia się botnet wraz z upływem czasu. Spółka obserwuje, że liczba ofiar stopniowo wzrasta od 127 w dniu 14 lipca do 429 w dniu 21 lipca. Następnie 25 lipca po dużej kampanii spamowej, która rozprowadziła nową wersję GOZ ilość infekcji skoczyła do 8.494 ofiar, wiele z nich znajduje się w USA, Arbor Network w środę napisało na swoim blogu:

*„GOZ rośnie w siłę. W ciągu trzech tygodni, pięć naszych domen poprzez sinkholding znalazło 12353 unikalnych adresów IP z całego świata.”* - twierdzą naukowcy. Krajem najbardziej dotkniętym były Stany Zjednoczone, z 44% zakażeń.

Na razie twórcy nowego wariantu GOZ koncentrują się na przebudowie botnetu, a nie na kradzieży pieniędzy od użytkowników. Prawdopodobnie jest to tylko kwesta czasu, kiedy powrócą do swojego głównego celu.