**Bitdefender: Botnet, który zainfekował ponad 90 000 urządzeń rośnie w siłę**

**30 kwietnia, badacze Bitdefender dowiedzieli się o nowej wersji bota Hide and Seek, który udokumentowaliśmy na początku tego roku. Botnet, pierwszy na świecie, który komunikuje się za pośrednictwem niestandardowego protokołu peer to peer, stał się także pierwszym, który uzyskał trwałość, czyli możliwość „przeżycia” ponownego uruchomienia.**

Historycznie botnet infekował blisko 90 000 unikalnych urządzeń od chwili odkrycia do dzisiaj, z różnym skutkiem po każdej aktualizacji.

Botnet to geograficznie rozproszona sieć zainfekowanych komputerów w tym wypadku również urządzeń spełniających koncepcję Internet of Things, pozwalająca jego twórcy na sprawowanie kontroli nad wszystkimi zainfekowanymi jednostkami. Autor botneta może wykorzystać zainfekowane urządzenia do przeprowadzenia ataków sieciowych, inwigilacji, rozsyłania SPAMU czy kradzieży poufałych informacji.

„Istnieją dwa aspekty tych ataków, jeden to zdobycie dostępu do urządzenia, drugim z nich jest informacja, jakie miejsce dane urządzenie zajmuje w sieci. Użytkownicy takich jednostek bardzo często nie są świadomi, że padli ofiarą botneta, ponieważ jego aktywność jest trudna do wykrycia z wykorzystaniem zwykłych metod. Jeżeli sieć zainfekowanych urządzeń poszerzy się o serwer szansa zarażenia następnych jednostek gwałtownie wzrasta.”, komentuje Mariusz Politowicz, inżynier techniczny Bitdefender z firmy Marken.

Nowe próbki zidentyfikowane pod koniec kwietnia zawierają teraz kod służący wykorzystaniu dwóch nowych luk, aby umożliwić złośliwemu oprogramowaniu zagnieżdżenie w większej liczbie modeli kamer IPTV. Oprócz luk w zabezpieczeniach, bot może również zidentyfikować dwa nowe typy urządzeń i przekazać ich domyślną nazwę użytkownika i hasła.

Odkryta próbka dotyczy również kilku urządzeń generycznych. Zainfekowane ofiary skanują sąsiadów w poszukiwaniu usługi telnet. Natychmiast po znalezieniu usługi telnet zainfekowane urządzenie usiłuje zaimportować dostęp. Jeśli logowanie zakończy się sukcesem, złośliwe oprogramowanie ogranicza dostęp do portu 23, aby potencjalnie uniemożliwić konkurencyjnemu botowi przejęcie urządzenia.

Ten atak skierowany jest do szerokiej gamy urządzeń. Badania Bitdefendera pokazują, że bot ma 10 różnych plików binarnych skompilowanych dla różnych platform, w tym x86, x64, ARM (Little Endian i Big Endian), SuperH, PPC i tak dalej.

Po pomyślnym zainfekowaniu szkodliwe oprogramowanie kopiuje się w folderze /etc/init.d/ i dodaje się do systemu operacyjnego. Aby osiągnąć trwałość, infekcja musi odbywać się za pośrednictwem usługi Telnet, ponieważ uprawnienia administratora są wymagane do skopiowania pliku binarnego do katalogu init.d.

Następnie otwarty zostaje losowy port UDP, który jest propagowany do sąsiednich botów. Ten port będzie wykorzystywany przez cyberprzestępców do skontaktowania się z urządzeniem.

Obsługiwana lista poleceń nie zmieniła się znacząco od poprzedniej wersji bota. Wciąż nie ma wsparcia dla ataków DDoS (jednej z najczęściej spotykanych cech botów), co automatycznie nie pozwala na zarobek poprzez botnety. Jednak sam bot może nadal eksfiltrować pliki za pomocą metody Hide ‘N Seek.

Bazując na dostępnych dowodach, zakładamy, że botnet znajduje się w fazie wzrostu, ponieważ operatorzy starają się przechwycić jak najwięcej urządzeń, zanim dodadzą bardziej agresywne funkcje do pliku binarnego.