Cyberdefence 24

aut. Szymon Palczewski 28.05.2020

CHIŃSKI INTERNET ZDOMINOWANY PRZEZ ZŁOŚLIWEGO TROJANA. WIRUS „SZALEJE” W SIECI PAŃSTWA ŚRODKA

Użytkownicy chińskiego internetu od minimum trzech lat są nękani przez złośliwe oprogramowanie „szalejące” w sieci. Trojan funkcjonuje jedynie w granicach infrastruktury internetowej Państwa Środka. Lokalni giganci podjęli współpracę w celu zwalczenia problemu milionów użytkowników.

W ciągu ostatnich trzech lat trojan DoubleGuns był wykorzystywany przez hakerów do prowadzenia licznych złośliwych operacji wymierzonych w użytkowników chińskiego Internetu. Przez ten okres stał się jednym z największych botnetów szkodliwego oprogramowania w Państwie Środka – informuje serwis ZDNet.

DoubleGuns jest narzędziem hakerskim, które występuje wyłącznie w Chinach. Specjaliści Qihoo 360, producenta oprogramowania antywirusowego, podkreślają, że wirus zainfekował setki tysięcy użytkowników w Państwie Środka, przeprowadzając ponad milion infekcji w ciągu ostatnich lat.

Omawiane złośliwe oprogramowanie to odmiana trojana przeznaczonego na urządzenia z systemem Windows. Wirus działa w środowisku od lipca 2017 roku, kiedy to eksperci Qihoo 360 wykryli pierwsze jego próbki w sieci. Najczęściej jest rozpowszechniany za pomocą tzw. „aplikacji pułapek”, które są udostępniane na licznych chińskich stronach internetowych, głównie poświęconym pirackim grom oraz forach dla graczy.

DoubleGuns infekuje urządzenia ofiar poprzez instalowanie różnych złośliwych sterowników. Następnie umożliwia kradzież danych uwierzytelniających z aplikacji, ze szczególnym uwzględnieniem kont Steam – donosi ZDNet.

Co więcej, złośliwe oprogramowanie działa również jako moduł reklam i spamowania. Umieszcza witryny promocyjne na urządzeniach użytkowników, a także przejmuje konta komunikacyjne, aby rozpowszechniać reklamy wśród znajomych ofiary za pośrednictwem prywatnych wiadomości.

W obliczu problemu firma Qihoo 360 nawiązała współpracę z chińskim gigantem technologicznym Baidu, aby zakłócić działanie DoubleGuns, który – zadaniem ekspertów – „stał się zbyt duży, aby go ignorować”. Jednym z celów kooperacji jest zlikwidowanie części infrastruktury internetowej, która stanowi „zaplecze” dla trojana – wskazuje ZDNet.