**Rosyjski haker dostaje 35 lat więzienia. Wykorzystał luki w programach antywirusowych**

**Obywatel byłego ZSRR, który mieszkał w Rydze na Łotwie, otrzymał trzy zarzuty związane z działalnością "Scan4you" - usługi antywirusowej online. Serwis pomagał hakerom uniknąć rozwiązań anty-malware, ogłosił amerykański Departament Sprawiedliwości.**

Akta sądowe ujawniają, że w latach 2009-2015, 37-letni Ruslans Bondars korzystał ze Scan4you. Usługa pozwalała twórcom złośliwego oprogramowania wykorzystać luki bezpieczeństwa w oprogramowaniu antywirusowym, chroniącym miliony systemów, należących do największych amerykańskich przedsiębiorców, instytucji finansowych i agencji rządowych.

Przykładem skutków działalności Scan4you jest przypadek, w którym wspomniany serwis pomógł dokonać kradzieży 40 milionów numerów kart kredytowych i debetowych, a także około 70 milionów adresów, numerów telefonów oraz innych danych osobowych obywateli USA. Jedna z poszkodowanych firm wyliczyła wtedy straty na wartość 290 milionów USD.

Sprawcy, kryjący swój wirus pod nazwą Citadel, zainfekowali złośliwym kodem ponad 11 milionów komputerów na całym świecie. Oni również korzystali z usługi Scan4you do złamania zabezpieczeń i ukrycia swojego programu. Twórcy Citadel spowodowali, że ich ofiary zostały poszkodowane na około 500 milionów dolarów.

„Konie trojańskie takie jak Citadel działają w ukryciu i przejmują kontrolę nad maszyną ofiary. Mogą wysyłać do swojego stwórcy dane, przechwycone hasła oraz pliki zgromadzone na dysku.”, komentuje Mariusz Politowicz, inżynier techniczny Bitdefender z firmy Marken, „Citadel Virus był zmodyfikowaną wersją trojana Zeus, którego celem byli użytkownicy banków. W większości przypadków używany był do kradzieży poświadczeń bankowych lub innych poufnych informacji które mogły zostać znalezione na komputerach ofiar.”- dodaje.

„Twórca złośliwego kodu skorzystał ze specjalnej funkcji Scan4you, która umożliwiła zaimplementowanie wspomnianego systemu spyware poprzez Interfejs Programowania Aplikacji (API). Narzędzie pozwalało użytkownikowi na możliwość skanowania malware bez potrzeby bezpośredniego uploadu na stronie internetowej Scan4you.”, czytamy w oświadczeniu Departamentu Sprawiedliwości.

W przeciwieństwie do legalnych usług skanowania plików, Scan4you został zaprojektowany do diagnozowania złośliwego oprogramowania dostarczanego anonimowo - bez dzielenia się informacjami o przesłanych plikach z bazą znanych wirusów.