Afera szpiegowska w Gruzji?

25 marca 2012

Nietypowe zagrożenie komputerowe zwróciło uwagę ekspertów z laboratorium antywirusowego firmy ESET. Przechwycony koń trojański pobiera rozkazy od cyberprzestępcy z domeny należącej do gruzińskiego rządu. Dokładna analiza wykazała, że zagrożenie zaprojektowano w taki sposób, aby wyszukiwało i wykradało m.in. dokumenty zawierające zwroty: minister, tajne, FBI, CIA, pułkownik, Rosja, USA oraz Europa.

Analitycy zagrożeń komputerowych firmy ESET oznaczyli przechwycone zagrożenie jako Win32/Georbot i sklasyfikowali je jako konia trojańskiego, który może być kontrolowany przez cyberprzestępcę zdalnie. Zagrożenie potrafi przechwytywać informacje przechowywane na dyskach twardych komputerów, a także posiada zdolność tworzenia tzw. sieci zombie, czyli grup zainfekowanych maszyn, które wykonują polecenia cyberprzestępców. Georbot wykrada i przesyła dowolne pliki z komputerów swoich ofiar do zdalnego serwera cyberprzestępcy, a także umożliwia szpiegowanie internautów z wykorzystaniem kamer internetowych i mikrofonów, podłączonych do komputerów swoich ofiar.

– Z naszych ustaleń wynika, że Win32/Georbot był najczęściej wykorzystywany przez cyberprzestępców do przeszukiwania dysków zainfekowanych komputerów i pobierania z nich konkretnych plików – podkreśla Pierre-Marc Bureau, analityk firmy ESET.

Od 2011 roku zagrożenie jest monitorowane przez Agencję Wymiany Informacji Ministerstwa Sprawiedliwości Gruzji oraz międzynarodową organizację CERT. Obie te instytucje ściśle współpracują w sprawie wspomnianego zagrożenia z ekspertami firmy ESET.

Wszystkie rozkazy z instrukcjami działania dla Georbota cyberprzestępca wydaje i aktywuje ręcznie, indywidualnie dla

każdej zainfekowanej maszyny, a nie automatycznie, jak ma to miejsce w wypadku tradycyjnych zagrożeń. Win32/Georbot komunikuje się ze zdalnym serwerem cyberprzestępcy po protokole HTTP, za pośrednictwem którego przesyłane są komendy działania. Z takiego serwera szkodnik pobiera również swoje nowe wersje – według informacji zgromadzonych przez ekspertów firmy ESET dotychczas zagrożenie aktualizowało się nawet co kilka dni, głównie w celu lepszego maskowania swojej obecności przed programami antywirusowymi.

Ciekawą funkcją zagrożenia jest umiejętność działania w przypadku niemożności skontaktowania się ze zdalnym serwerem cyberprzestępcy, z którego przesyłane są do zagrożenia instrukcje działania. W momencie zaistnienia takiej sytuacji Win32/Georbot łączy się z jedną z rządowych, gruzińskich domen, skąd otrzymuje adres IP nowego zdalnego serwera, z którym następnie nawiązuje połączenie. Nie oznacza to jednak, że zagrożenie ma coś wspólnego z gruzińskim rządem – często zdarza się, że cyberprzestępcy przechwytują i korzystają z infrastruktury firm lub instytucji bez ich wiedzy i zgody.

Według ekspertów z firmy ESET, analizujących Win32/Georbot, współczesna działalność cyberprzestępcza profesjonalizuje się, czego dowodem mogą być chociażby wyspecjalizowane zagrożenia, takie jak Stuxnet czy Duqu. Również Georbot, mimo prostej architektury, posiada kilka unikatowych funkcji, dzięki którym potrafi skutecznie wykradać wrażliwe informacje z zainfekowanych maszyn. Fakt pobierania przez zagrożenie swoich aktualizacji z gruzińskich serwisów internetowych może sugerować, że głównym jego celem są Gruzini. Jednak z uwagi na fakt, iż Win32/Georbot atakował początkowo komputery użytkowników w dwóch strefach czasowych, niewykluczone, że jego celem mogli być również mieszkańcy Rosji czy Iraku. Według hipotezy analityków firmy ESET – Win32/Georbot został stworzony przez grupę cyberprzestępców w celu kradzieży wrażliwych informacji i późniejszej ich odsprzedaży innym organizacjom.

Opracowanie: paku
Źródło: Dziennik Internautów