**Gameover Zeus - cyberatak finansowy na dwa fronty**

**W ubiegłym tygodniu świat obiegła informacja o tym, że agentom FBI udało się opanować „najbardziej wyszukany i niszczycielski botnet, jaki kiedykolwiek widzieli”.**

Mowa o ataku Gameover Zeus, w ramach którego niesławny trojan ZeuS kradnący informacje finansowe współdziałał z oprogramowaniem Cryptolocker wyłudzającym okup za przywrócenie dostępu do zaszyfrowanych danych użytkownika. Eksperci z Kaspersky Lab tłumaczą, jakie konsekwencje dla użytkowników mogą mieć tego rodzaju ataki i jak się przed nimi chronić.

Informacja o zamknięciu niszczycielskiego botnetu Gamever Zeus mogła wywołać niepokój u wielu użytkowników komputerów i internetu. W ramach jednej akcji cyberprzestępczej wykorzystano dwa bardzo niebezpieczne zagrożenia:

- ZeuS - trojan szukający na komputerze informacji osobistych, takich jak hasła czy dane finansowe. Gdy ofiara pracująca z systemem Windows kliknie zainfekowany załącznik, z komputera pobierane są żądane dane, a zarażona maszyna zaczyna wysyłać wiadomości spamowe mające na celu przyciągniecie kolejnych ofiar i szybie rozprzestrzenienie ataku w internecie;

- Cryptolocker - trojan szyfrujący dane na dysku zainfekowanego komputera i żądający zapłacenia okupu za przywrócenie dostępu do plików (tzw. oprogramowanie ransomware); szkodnik był aktywowany, gdy ZeuS nie był w stanie zgromadzić wystarczającej ilości wartościowych informacji finansowych.

**David Emm**, starszy ekspert ds. bezpieczeństwa, Globalny Zespół ds. Badań i Analiz (GReAT), Kaspersky Lab, powiedział: „Zagrożenia tego typu nie należą do rzadkości – w naszym laboratorium antywirusowym każdego dnia analizujemy ponad 315 000 próbek szkodliwych programów, łącznie z trojanami bankowymi, oprogramowaniem ransomware i wieloma innymi niebezpiecznymi aplikacjami. W przypadku ZeuSa ważne jest to, że jego oryginalny kod jest dostępny w Sieci od wielu lat i obecnie istnieją setki jego modyfikacji, co ułatwia cyberprzestępcom skorzystanie z wersji, która może zostać wpuszczona do atakowanego systemu przez oprogramowanie antywirusowe słabej jakości".

Produkty Kaspersky Lab wykrywają wszystkie komponenty wykorzystane w ataku Gameover Zeus jako Trojan-Spy.Win32.Zbot (sygnatura dotyczy trojana ZeuS, w ten sam sposób wykrywane są także wszystkie pozostałe modyfikacje ZeuSa), Trojan-Ransom.Win32.Cryptolocker (w ten sposób wykrywany jest moduł wyłudzający okup za przywrócenie dostępu do danych użytkownika) oraz Trojan-Ransom.Win32.Blocker (w ten sposób wykrywane są niektóre modyfikacje Cryptolockera). Dodatkowo, rozwiązania bezpieczeństwa Kaspersky Internet Security oraz Kaspersky PURE są wyposażone w technologię Bezpieczne pieniądze, która zapewnia dodatkową warstwę ochrony przed atakami wycelowanymi w dane finansowe użytkowników.

**Jak się chronić przed atakami finansowymi**

Eksperci z Kaspersky Lab przygotowali kilka porad, które pozwolą ustrzec się przed atakami takimi jak Gameover Zeus i innymi zagrożeniami mającymi na celu pieniądze użytkowników.

Ważne jest, by użytkownicy nie tylko chronili swoje komputery, ale także zadbali o regularne zapisywanie kopii zapasowych swoich danych w bezpiecznym miejscu. Jest to szczególnie istotne w przypadku oprogramowania żądającego okupu - posiadając aktualną kopię zapasową, będziemy mogli błyskawicznie przywrócić wszystkie dane, nawet gdy dojdzie do infekcji trojanem takim jak Cryptolocker.

Aby chronić swoje dane finansowe (przed ZeuSem i innym szkodliwym oprogramowaniem przeznaczonym do kradzieży pieniędzy), warto zastosować się do kilku prostych reguł:

- nie klikaj odnośników przychodzących od nieznanych nadawców (w wiadomościach e-mail lub przez portale społecznościowe);

- nie pobieraj, nie otwieraj i nie przechowuj nieznanych plików na swoim urządzeniu;

- nie używaj niezabezpieczonych (publicznych) sieci Wi-Fi do wykonywania transakcji finansowych oraz do wszelkich działań wymagających logowania się do serwisów online;

- zanim wprowadzisz jakieś dane uwierzytelniające lub informacje poufne, zawsze dwa razy sprawdź serwis – strony phishingowe celowo są tak zrobione, aby niczym nie różniły się od autentycznych;

- pracuj jedynie ze stronami, których adres rozpoczyna się od „https” - są one bardziej bezpieczne niż te z „http”;

- upewnij się, że posiadasz aktualne i skuteczne oprogramowanie bezpieczeństwa, także dla urządzeń mobilnych.

Jeżeli komputer został już zainfekowany w ramach ataku Gameover Zeus, użytkownik może usunąć zagrożenie przy użyciu bezpłatnego narzędzia TSDDKiller przygotowanego przez ekspertów z Kaspersky Lab. Jest ono dostępne do pobrania na stronie <http://support.kaspersky.com/pl/viruses/disinfection/5350>.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.

Wszystkie informacje prasowe Kaspersky Lab Polska są dostępne na stronie <http://www.kaspersky.pl/news>.