**Kaspersky Lab wykrywa operację cyberszpiegowską Grabit**

**Kaspersky Lab informuje o wykryciu nowej kampanii cyberszpiegowskiej o nazwie Grabit, której celem są małe i średnie firmy. W ramach swoich działań cyberprzestępcy zdołali ukraść około 10 000 plików z organizacji znajdujących się głównie w Tajlandii, Indiach oraz Stanach Zjednoczonych.**

Lista sektorów stanowiących cele omawianej kampanii obejmuje m.in. branżę chemiczną, nanotechnologię, edukację, rolnictwo, media oraz budownictwo.

Inne atakowane państwa to Zjednoczone Emiraty Arabskie, Niemcy, Izrael, Kanada, Francja, Austria, Sri Lanka, Chile oraz Belgia.

„Obserwujemy wiele kampanii szpiegowskich, których celem są przedsiębiorstwa, organizacje rządowe oraz inne szeroko znane podmioty, ale małe i średnie firmy rzadko figurują na liście celów. Jednak kampania Grabit pokazuje, że nie chodzi tu tylko o 'grube ryby' – w cyberświecie każda organizacja, niezależnie od tego czy posiada pieniądze, informacje czy wpływy polityczne, może stać się przedmiotem zainteresowania tej czy innej grupy przestępczej. Kampania Grabit nadal jest aktywna, dlatego niezwykle ważne jest sprawdzenie swojej sieci, aby mieć pewność, że jest się bezpiecznym. Analiza wykazała, że prosty keylogger Grabit przechowywał tysiące danych uwierzytelniających do kont ofiar pochodzących z setek zainfekowanych systemów. Nie wolno lekceważyć tego zagrożenia” – powiedział **Ido Noar**, starszy badacz bezpieczeństwa, Globalny Zespół ds. Badań i Analiz (GReAT), Kaspersky Lab.

Infekcja zaczyna się od otrzymania przez pracownika atakowanej firmy e-maila z załącznikiem, który przypomina plik aplikacji Microsoft Office Word (.doc). Gdy ofiara kliknie załącznik w celu pobrania dokumentu, na maszynę zostanie dostarczony program szpiegujący pochodzący ze zdalnego serwera, który został zhakowany przez ugrupowanie przestępcze, aby pełnił funkcję centrum rozprzestrzeniania szkodliwego oprogramowania. Atakujący kontrolują swoje ofiary przy użyciu keyloggera HawkEye – komercyjnego narzędzia szpiegującego firmy [HawkEyeProducts](http://hawkeyeproducts.com/), oraz modułu zawierającego wiele narzędzi zdalnej administracji (ang. RAT). Zadaniem keyloggera jest przechwytywanie wszystkich znaków wprowadzanych z klawiatury zainfekowanego komputera.

Aby zobrazować skalę operacji, eksperci z Kaspersky Lab obliczyli, że na zaledwie jednym z cyberprzestępczych serwerów kontroli znalazło się aż 2 887 haseł, 1 053 wiadomości

e-mail oraz 3 023 nazw użytkowników pochodzących z 4 928 maszyn. Skradziono m.in. dane logowania do serwisów i aplikacji takich jak Facebook, Skype, Gmail, Outlook, Pinterest, Yahoo, LinkedIn oraz Twitter, a także informacje bankowe i inne poufne dane.

**Chaotyczna grupa cyberprzestępcza**

Z jednej strony, ugrupowanie Grabit nie wysila się specjalnie, aby ukryć swoją aktywność: niektóre szkodliwe próbki wykorzystywały ten sam serwer, a nawet te same dane uwierzytelniające, osłabiając własne bezpieczeństwo. Z drugiej strony, atakujący stosują mocne techniki zaciemniania, aby ukryć swój kod przed analitykami. To daje ekspertom z Kaspersky Lab powody, by sądzić, że za całą operacją szpiegowską stoi dość chaotyczna grupa, w której niektórzy członkowie mają większe umiejętności techniczne niż inni i bardziej dbają o to, by pozostać w ukryciu.

Analiza ekspercka sugeruje, że ktokolwiek zaprogramował omawiany szkodliwy program nie napisał całego kodu od zera.

**Jak się chronić**

W celu zapewnienia sobie ochrony przed atakami przeprowadzanymi w ramach kampanii Grabit Kaspersky Lab zaleca przestrzeganie poniższych reguł:

- Sprawdź lokalizację C:Users<Nazwa\_Użytkownika>AppDataRoamingMicrosoft. Jeśli znajdują się tam pliki wykonywalne, Twoje urządzenie może być zainfekowane szkodliwym oprogramowaniem. To sygnał ostrzegawczy, którego nie powinieneś ignorować.

- Uruchom „msconfig” i upewnij się, że na liście obiektów aktywowanych wraz ze startem systemu operacyjnego nie ma pliku grabit1.exe lub obiektu o podobnej nazwie.

- Nie otwieraj załączników ani odsyłaczy od nieznanych osób. Jeśli na Twoim komputerze firmowym ograniczono możliwość otwierania określonych typów plików, nie proś o ich uruchomienie innych pracowników – zwróć się o pomoc do administratora IT.

- Korzystaj z zaawansowanego, uaktualnionego rozwiązania antywirusowego i zawsze stosuj się do zaleceń oprogramowania bezpieczeństwa w przypadku podejrzanych procesów.

Produkty firmy Kaspersky Lab wykrywają wszystkie znane próbki Grabita i chronią użytkowników przed tym zagrożeniem.

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>.