**Spam w kwietniu 2014 – giełdowe oszustwa i e-maile z trojanami**

**Eksperci z Kaspersky Lab przeanalizowali ewolucję spamu w kwietniu 2014 r. – szczególnie popularny był szkodliwy spam z życzeniami oraz z fałszywymi powiadomieniami z serwisów faksowych.**

Wykryto także nową falę spamu typu „pump and dump”, polegającego na sztucznym pompowaniu cen udziałów w firmach celem szybkiego zarobienia pieniędzy.

Rzekome kwietniowe życzenia wielkanocne okazały się trojanem Fareit.aonw o dość ograniczonej funkcjonalności: program ten nie próbował kraść żadnych haseł, ale pobierał i uruchamiał o wiele bardziej niebezpiecznego trojana szpiegującego Zbot, którego celem jest atakowanie serwerów i kradzież danych osobistych. Drugi przypadek dotyczył fałszywych wiadomości pochodzących rzekomo z popularnego serwisu faksowego online. Wiadomość ta zawierała niewielkiego trojana, który instalował ten sam program szpiegujący z niesławnej rodziny Zeus/Zbot.

W kwietniu Kaspersky Lab wykrył także kilka dużych ataków wykorzystujących szkodliwe oprogramowanie pod przykrywką faksów wysyłanych za pośrednictwem popularnego serwisu internetowego eFax, który umożliwia użytkownikom wysyłanie i otrzymywanie faksów jako załączników do wiadomości e-mail. Fałszywe wiadomości zawierały zwykle powiadomienie o przychodzącym faksie oraz liczbę jego stron, tak aby były bardziej przekonujące. W rzeczywistości jednak plik zip krył szkodliwe oprogramowanie, które stanowił Trojan-Downloader.Win32.Cabby.a – raczej niewielki szkodliwy program, który zawiera w swoim kodzie dokument lub obrazek, który wyświetla się użytkownikowi po uruchomieniu pliku. Podczas gdy ofiara jest zajęta przeglądaniem dokumentu, Cabby potajemnie pobiera i instaluje inną niebezpieczną aplikację. W zaobserwowanych przez ekspertów z Kaspersky Lab przypadkach drugi szkodliwy program należał – podobnie jak w przypadku niebezpiecznego spamu z życzeniami świątecznymi – do szeroko rozpowszechnionej rodziny ZeuS/Zbot (Trojan-Spy.Win32.Zbot.shqe).

**Phishing**

W kwietniu phisherzy najczęściej atakowali organizacje z kategorii „serwisy pocztowe i wyszukiwarki”, która stanowiła cel 31,9% ataków. Na drugim miejscu znalazły się „portale społecznościowe” (których udział wynosił 23,8%, o 0,2 punktu procentowego mniej w stosunku do poprzedniego miesiąca). Na trzeciej pozycji uplasowały się „organizacje finansowe i płatności” (13%, o 0,2 punktu procentowego mniej niż w marcu).

Najczęściej atakowaną organizacją w badanym miesiącu była chińska firma z branży telekomunikacyjnej Tencent, która oferuje między innymi wsparcie techniczne dla komunikatora internetowego QQ. Oszuści próbowali uzyskać loginy i hasła klientów przy użyciu dobrze znanych sztuczek, takich jak poinstruowanie użytkownika, aby kliknął odsyłacz w celu odzyskania dostępu do swojego konta. W rzeczywistości jednak odsyłacz ten prowadził do strony phishingowej. Powiadomienie zostało wysłane w formie grafiki, co pomogło obejść filtry spamowe i sprawiło, że wiadomość bardziej przypominała legalną.

„W zeszłym miesiącu odnotowaliśmy nową falę spamu typu ‘pump and dump’. Stojący za takimi wysyłkami oszuści reklamowali oferty nabycia udziałów w określonej firmie po bardzo niskich cenach, które miały znacznie wzrosnąć w najbliższej przyszłości. W efekcie wzrastało zapotrzebowanie na udziały w firmie i ich ceny zostały sztucznie zawyżone – po czym oszuści sprzedali swoje udziały. Następnie ceny udziałów zaczęły spadać, a oszukani inwestorzy zostali z udziałami o niższej wartości i stracili na swojej inwestycji. Oszuści wybierają zwykle do takich przekrętów mało znane firmy, w przypadku których handel udziałami odbywa się rynku wtórnym. W kwietniu wykorzystano do tego celu amerykańską firmę Rich Pharmaceuticals” – powiedziała **Tatiana Szczerbakowa**, starszy analityk spamu, Kaspersky Lab.

Odsetek spamu w globalnym ruchu e-mail wynosił w kwietniu średnio 71,1% - o 7,6 punktu procentowego więcej w stosunku do zeszłego miesiąca.

Pełny raport poświęcony ewolucji spamu w kwietniu 2014 r. pojawi się już wkrótce w serwisie [SecureList.pl](http://www.securelist.pl) prowadzonym przez Kaspersky Lab.

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>