**Spam w maju 2013 r.: „Złoty bilet” Microsoftu**

**W maju odsetek spamu w ruchu pocztowym zmniejszył się o 2,5 punktu procentowego i wynosił średnio 69,7%. Eksperci z Kaspersky Lab odnotowali bardzo niewielki wzrost udziału wiadomości phishingowych w porównaniu z kwietniem, natomiast szkodliwe załączniki zostały wykryte w 2,8% e-maili – co stanowi wzrost o 0,4 proc. w stosunku do poprzedniego miesiąca. Próbując przekonać użytkowników, aby otworzyli takie załączniki, spamerzy podrabiali legalne powiadomienia z popularnych serwisów internetowych i firm kurierskich, takich jak Amazon, UPS czy Western Union. Zgodnie z przewidywaniami, najatrakcyjniejszym celem phisherów pozostały portale społecznościowe.**

Większość światowego spamu pochodziła z dwóch państw – z Chin (21,4%) oraz Stanów Zjednoczonych (16,3%). Pierwszą trójkę zamknęła Korea Południowa – wkład tego państwa wciąż rósł i w maju osiągnął 12%.

Spamerzy nadal wykorzystywali święta narodowe – Dzień Matki i Dzień Pamięci (obchodzony w Stanach Zjednoczonych) – w celu reklamowania towarów i usług. Dzień Matki stanowi drugie po walentynkach święto najaktywniej wykorzystywane w wysyłkach spamowych, a ilość spamu dystrybuowanego za pośrednictwem „kwiatowych” programów partnerskich znacznie wzrasta w dniach i tygodniach poprzedzających tę datę.

Eksperci z Kaspersky Lab ostrzegają, że nie wszystkie z tych „świątecznych” wiadomości spamowych są nieszkodliwe – głównym celem spamerów mogą być osobiste dane użytkowników - w tym bankowe dane uwierzytelniające. Przykładem są wysłane w maju wiadomości phishingowe, które podszywały się pod e-maile z działu obsługi klientów firmy Microsoft, a ich głównym celem była kradzież danych osobistych.

Wiadomości te, które na pierwszy rzut oka wydawały się pochodzić z domeny microsoft.com, informowały o planowanym zawieszeniu usługi „Microsoft Window Records”, wynikającym z tego, że użytkownik nie zainstalował aktualizacji rzekomo zalecanych we wcześniejszych wiadomościach. Odbiorcy zostali poinstruowani, że aby temu zapobiec, należy jak najszybciej kliknąć zawarty w e-mailu odsyłacz. Użytkownicy, którzy dali się nabrać na to oszustwo, zostali przekierowani na stronę phishingową stworzoną w celu kradzieży informacji osobistych.

Inne masowe wysyłki zawierały fałszywe powiadomienia o wygranych w nieistniejącej loterii, która została rzekomo zorganizowana przez firmę Microsoft. W niektórych wysyłkach oszuści wysyłali powiadomienia o rzekomej wygranej i prosili odbiorców o skontaktowanie się z nimi w celu uzyskania dalszych informacji, podczas gdy inne wiadomości obiecywały ogromne kwoty, w zamian prosząc o przelanie niewielkiej sumy na pokrycie kosztów operacyjnych.

Wraz ze zbliżającym się okresem letnich wakacji eksperci przewidują dalszy wzrost liczby fałszywych powiadomień, w których cyberprzestępcy będą podszywali się pod znane firmy.

*„Zalecamy ostrożność w przypadku otrzymania powiadomienia z jakiegokolwiek serwisu. Warto pamiętać, że oficjalne wysyłki nigdy nie są wysyłane w celu poproszenia klientów o podanie lub potwierdzenie informacji osobistych lub bankowych za pośrednictwem odsyłaczy zawartych w e-mailach. Nie straszą również zablokowaniem kont klientów. Nigdy nie należy klikać odsyłaczy zablokowanych przez program antywirusowy lub przeglądarkę. Zawsze trzeba zwracać uwagę na odsyłacze zawarte w wiadomości - jeżeli taki odsyłacz prowadzi do nieoficjalnej strony lub jeśli treść wiadomości zawiera adres oficjalnej strony, podczas gdy odsyłacz prowadzi do innej, może to oznaczać, że mamy do czynienia z wiadomością phishingową. W razie jakichkolwiek wątpliwości co do autentyczności e-maila, warto skontaktować się z działem obsługi klientów organizacji, która wysyłała tę wiadomość, i dowiedzieć się, czy taka masowa wysyłka rzeczywiście miała miejsce”* – powiedziała Daria Gudkowa, szefowa działu badań i analizy zawartości, Kaspersky Lab.

Pełna wersja raportu spamowego dla maja 2013 jest dostępna w serwisie SecureList.pl prowadzonym przez Kaspersky Lab: <http://securelist.pl/analysis/7231,spam_w_maju_2013.html>.

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