Jedna na pięć wiadomości spam pochodzi z USA, jedna na 20 z Wielkiej Brytanii. Polska poza „parszywą dwunastką". Sophos, firma specjalizująca się w technologiach ochrony informacji, opublikował swój najnowszy raport zawierający listę dwunastu najbardziej spamujących krajów w trzecim kwartale 2010 roku.

Od drugiego kwartału tego roku, produkcja spamu pochodzącego ze Stanów Zjednoczonych znacząco wzrosła z 15,2% do 18,6% światowego spamu, oznacza to, że prawie jedna na pięć niechcianych wiadomości ma swoje źródło w USA. Stany Zjednoczone produkują niemal 2,5 razy więcej spamu niż kolejny na liście kraj – Indie.

Wielka Brytania zanotowała spadek o jedną pozycję w stosunku do poprzedniego kwartału – z czwartej na piątą – i jest odpowiedzialna za 5% globalnego spamu.

Lista dwunastu krajów, które od lipca do września 2010 r. wysłały najwięcej spamu kształtuje się następująco:

1. Stany Zjednoczone 18,6%
2. Indie 7,6%
3. Brazylia 5,7%
4. Francja 5,4%
5. Wielka Brytania 5,0%
6. Niemcy 3,4%
= 7. Rosja 3,0%
= 7. Korea Południowa 3,0%
9. Wietnam 2,9%
10. Włochy 2,8%
11. Rumunia 2,3%
12. Hiszpania 1,8%

Pozostałe 38,5%

Rozkład spamu ze względu na kontynenty w okresie lipiec - wrzesień 2010:

Europa 33,1%
Azja 30,0%
Ameryka Północna 22,3%
Ameryka Południowa 11,5%
Afryka 2,3%

Pozostałe 0,8%

Prawie wszystkie wiadomości spam pochodzą z komputerów zainfekowanych złośliwym oprogramowaniem (znanych jako boty lub zombie), które są kontrolowane przez cyberprzestępców. Jedna z głównych taktyk wykorzystywanych przez cyberprzestępców do rozwoju botnetów polega na nakłanianiu użytkowników do kliknięcia na złośliwe linki - zawarte w spamie lub wiadomościach w sieciach społecznościowych - które kierują do zainfekowanych złośliwym oprogramowaniem stron internetowych.

"Spam nie jest tylko utrapieniem dla użytkowników, jest wykorzystywany przez cyberprzestępców do rozwoju ich działalności," powiedział Graham Cluley, starszy konsultant ds. technologii w Sophos. „Nie powinieneś nawet otwierać spamu z ciekawości, ponieważ spamerzy w ciągu kilku sekund mogą skutecznie przejąć kontrolę nad twoim komputerem. Jeśli twój pecet stanie się częścią botnetu, jesteś skazany na dalsze infekcje, a to może ujawnić twoje dane osobiste lub szczegóły dotyczące logowania do banku."
Sophos zauważa również wzrost spamu w sieciach społecznościowych w trzecim kwartale 2010, z mocno nagłaśnianym exploitem 'OnMouseOver', wykorzystywanym do generowania spamu na Twitterze i ciągiem ataków scam na

Facebooku, tworzonych przez spamerów do zarabiania na naiwności użytkowników.

„Charakterystyczną cechą oszustw na Facebooku jest to, że wykorzystują ludzkie słabości – wyłudzają od użytkowników informacje osobiste w zamian za możliwość obejrzenia szkoującego zdjęcia czy nagrania wideo, które nawet nie istnieje," dodaje Cluley. "Niestety, takie oszustwa są nadal rozprzestrzeniane, a nowe pojawiają się każdego dnia i Facebook nie jest w stanie sobie z nimi poradzić."

Jeden ze spamerów na Facebooku został jednak niedawno ukarany grzywną za korzystanie z sieci społecznościowej do promocji sprzedaży narkotyków. Na Adama Guerbueza nałożono grzywnę $200 za każdy z 4.366.386 postów, które Kanadyjczyk dodał, co dało sumę $873.300.000.

"Zawsze czuwaj nad tym gdzie wpisujesz swoje dane do logowania – miej świadomość, że możesz się znajdować na fałszywej stronie, utworzonej tylko w celu przejęcia twojej nazwy użytkownika oraz hasła, które później są wykorzystywane do rozsyłania spamu," wyjaśniał Cluley.

Sophos zaleca, aby firmy automatycznie aktualizowały oprogramowanie antywirusowe i uruchomiły skonsolidowane rozwiązania dla poczty e-mail oraz przeglądarek internetowych, aby bronić się przed spamem i wirusami.

Więcej informacji na temat najnowszego raportu można znaleźć na blogu Grahama Cluleya, pod adresem: http://www.sophos.com/blogs/gc/g/2010/10/14/usa-poorly-protected-pcs

Sophos