**Mistrzostwa świata 2014: cyberprzestępcy i oszuści biorą na celownik święto fanów piłki nożnej**

**Podczas gdy w Brazylii trwają ostatnie przygotowania do mistrzostw świata FIFA w piłce nożnej, które rozpoczną się 12 czerwca, cyberprzestępcy intensyfikują kampanie wymierzone przeciwko kibicom futbolu.**

Eksperci z Kaspersky Lab przygotowali kilka wskazówek, które pozwolą zabezpieczyć się przed atakami phishingowymi oraz szkodliwym oprogramowaniem wykorzystującymi temat mistrzostw świata i bezpiecznie cieszyć się największym wydarzeniem sportowym na świecie.

Oszuści internetowi aktywnie tworzą wyrafinowane strony internetowe imitujące autentyczne domeny mistrzostw świata, sponsorów i partnerów tej imprezy – w tym znane marki – próbując nakłonić użytkowników, aby podali swoje prywatne dane, takie jak nazwy użytkowników, hasła czy numery kart kredytowych.

**Fabio Assolini**, starszy badacz bezpieczeństwa z Globalnego Zespołu ds. Badań i Analiz (GReAT), Kaspersky Lab, powiedział: „W samej tylko Brazylii każdego dnia wykrywamy 50-60 nowych domen phishingowych, a utrzymywane na nich strony są bardzo wyrafinowane i umiejętnie zaprojektowane. W rzeczywistości, zwykłemu użytkownikowi może być trudno odróżnić fałszywą stronę od autentycznej”.

Niektóre strony phishingowe wydają się być bezpieczne. Na przykład, ich adresy mogą zaczynać się od prefiksu „https” (gdzie *s* oznacza ‘bezpieczny’), jeśli cyberprzestępcy zdołają kupić ważne certyfikaty SSL od odpowiednich organów certyfikacyjnych. Domeny phishingowe posiadają niekiedy również swoje wersje mobilne, które wyglądają na autentyczne i są wycelowane w użytkowników smartfonów i tabletów.

Przestępcy wykorzystują legalne certyfikaty SSL również w celu infekowania komputerów użytkowników szkodliwym oprogramowaniem. W jednym z oszustw użytkownicy z Brazylii otrzymywali wiadomość, w której zostali poinformowani o wygraniu biletu na mistrzostwa. Jednak odsyłacz, który mieli kliknąć w celu wydrukowania biletu, prowadził do podpisanego cyfrowo trojana bankowego.

W kolejnym ataku wykorzystano rzekome włamanie się do bazy danych klientów. Oszuści wysyłali spersonalizowane e-maile informujące odbiorców, że wygrali bilet na mistrzostwa. Wiadomości te – zawierające imię i nazwisko odbiorcy, jego datę urodzenia oraz pełny adres pobrany z nieznanej bazy danych – miały załączony dokument PDF, który stanowił rzekomo wygrany bilet, w rzeczywistości jednak także krył trojana kradnącego dane dotyczące bankowości online.

Cyberprzestępczość żerująca na ogromnym zainteresowaniu mistrzostwami świata nie ogranicza się tylko do Brazylii, ale stanowi zjawisko na skalę globalną. Nie jest również niczym nowym: już w lutym eksperci z Kaspersky Lab informowali o innych kampaniach spamowych oraz oszustwach nigeryjskich wykorzystujących temat nadchodzącego święta fanów piłki nożnej.

Eksperci z Kaspersky Lab przygotowali zestaw wskazówek, które pozwolą zabezpieczyć się przed atakami phishingowymi i szkodliwym oprogramowaniem wykorzystującym otoczkę mistrzostw świata:

1. Należy dokładnie sprawdzić stronę, zanim podamy na niej jakiekolwiek dane uwierzytelniające lub informacje poufne. Strony phishingowe są celowo tworzone w taki sposób, aby wyglądały na autentyczne.

2. Chociaż strony z prefiksem „https” są bezpieczniejsze niż te z „http”, nie oznacza to, że można mieć do nich całkowite zaufanie - cyberprzestępcy mogą zdobyć legalne certyfikaty SSL.

3. Należy zachować ostrożność w przypadku wszelkich wiadomości pochodzących od nieznanego nadawcy. W szczególności należy powstrzymać się od klikania odsyłaczy zawartych w wiadomościach e-mail, jeśli nie ma całkowitej pewności, że pochodzą z bezpiecznych źródeł. Nie wolno również pobierać ani otwierać załączników niewiadomego pochodzenia.

4. Należy dopilnować, aby na urządzeniu zainstalowana była uaktualniona ochrona przed szkodliwym oprogramowaniem, która umieszcza na czarnej liście strony phishingowe.

Informację oraz infografikę 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>.