**Check Point ujawnia nową kampanię phishingową, wykorzystującą gorączkę Mistrzostw Świata**

**Nowy schemat phishingu wykorzystuje ofiary pobierające na komputery PC zainfekowany harmonogram Mistrzostw Świata FIFA w Piłce Nożnej oraz tracker wyników.**

**Firma Check Point® Software Technologies, jeden z wiodących dostawców rozwiązań w zakresie bezpieczeństwa cybernetycznego, wykrył kampanię phishingową wykorzystującą moment rozpoczęcia Mistrzostw Świata FIFA w Piłce Nożnej. Cyberprzestępcy próbowali zachęcić potencjalne ofiary do pobierania harmonogramu oraz trackera wyników meczów.**

Po otwarciu, załącznik wykorzystuje złośliwy wariant oprogramowania zwany "DownloaderGuide", będący znanym downloaderem potencjalnie niechcianych programów (PUP), który jest najczęściej używany jako instalator w aplikacjach takich jak paski narzędzi, adware lub optymalizatory systemu. Badacze Check Pointa ustalili, że w sumie kampania obejmuje dziewięć różnych plików wykonywalnych, z których wszystkie zostały wysłane w wiadomościach e-mail z tematem: "World\_Cup\_2018\_Schedule\_and\_Scoresheet\_V1.86\_CB-DL-Manager".

Kampania została po raz pierwszy zidentyfikowana została w dniu 30 maja 2018 r., a jej szczyt przypadł na 5 czerwca; jednak w ciągu ostatniego tygodnia nabrała ona nowego tempa wraz z dniem rozpoczęcia mistrzostw.

*- Wydarzenia cieszące się ogromnym zainteresowaniem są postrzegane przez cyberprzestępców jako doskonała okazja do rozpoczęcia nowych działań* - twierdzi Maya Horowitz, kierownik grupy analitycznej ds. zagrożeń w firmie Check Point. - *Przy tak wielkim oczekiwaniu i szumie mediowym wokół Mistrzostw Świata, cyberprzestępcy polują na pracowników, którzy mogą być w tym okresie mniej czujni podczas otwierania niechcianych e-maili i załączników. Dlatego ważne jest, aby organizacje podjęły kroki w celu przypomnienia swoim pracownikom o zalecanych praktykach w zakresie bezpieczeństwa.*

- *Ponadto, organizacje powinny również podjąć kroki w celu uniemożliwiania kampaniom phishingowym dotarcia do skrzynek odbiorczych. Powinno to obejmować zastosowanie wielowarstwowej strategii bezpieczeństwa cybernetycznego, która chroni zarówno przed atakami cybernetycznymi dokonywanymi przez zarejestrowane rodziny złośliwych oprogramowań, jak i przed zupełnie nowymi zagrożeniami oraz zapobieganiu ich rozprzestrzenianiu się w sieci* – dodaje Horowitz.

W związku z tym, że Check Point przewiduje dalszy zakres oszustw internetowych i ataków phishingowych podczas miesięcznego turnieju, firma wydała następujące wskazówki dla osób prywatnych, chcących chronić się przed zagrożeniami cybernetycznymi podczas Mistrzostw Świata FIFA w Piłce Nożnej:

**- Aktualizuj oprogramowanie** - upewnij się, że system operacyjny, oprogramowanie zabezpieczające, aplikacje i przeglądarki internetowe na Twoim komputerze PC lub urządzeniu mobilnym są zaktualizowane. Powinno to stanowić skuteczną ochronę przed większością złośliwego oprogramowania i innymi zagrożeniami internetowymi.

**- Ostrzeżenie przed fałszywymi stronami internetowymi** - Podczas poprzednich dużych imprez publicznych cyberprzestępcy tworzyli fałszywe strony internetowe i domeny, obejmujące wszystko, od merchandisingu po wiadomości i transmisję strumieniową na żywo, które wydają się być oficjalne, ale mogą być wykorzystywane do dostarczania złośliwego oprogramowania lub przechwytywania poufnych informacji.

**- Uważaj na wiadomości od nieznanych nadawców** - cyberprzestępcy będą prawdopodobnie wysyłać różne emaile phishingowe podczas turnieju, oferując szereg darmowych ofert lub możliwość losowania biletów na mecze. Może to przybrać formę hiperłączy lub załączników, które będą albo pobierać złośliwe oprogramowanie na maszyny, albo próbować ukraść Twoje dane osobowe. Najlepiej jest unikać otwierania wiadomości e-mail lub załączników od nierozpoznanego nadawcy.

**- Publiczne hotspoty Wi-Fi** - ponieważ mecze rozgrywane są przez cały dzień, wiele osób będzie chciało korzystać z publicznych punktów dostępu do sieci Wi-Fi do oglądania gier na urządzeniach przenośnych. Jednak niepewne punkty dostępu są łatwym celem dla hakerów, którzy mogą zagrażać naszym komputerom i smartfonom oraz przechwytywać dane osobowe, takie jak e-maile i hasła.