**Walentynki i czekoladki nie zawsze oznaczają miłość**

**Dziś Walentynki – święto zakochanych, którzy idąc z duchem święta szukają najlepszego sposobu świętowania z najbliższymi. Jednak nie tylko zakochani próbują jak najlepiej wykorzystać ten czas… Przez ostatnie dwa lata Check Point Research identyfikowało użycie słowa „Walentynka” (Valentines) w złośliwych witrynach internetowych. Zarówno w 2018, jak i 2019 roku wzrosty wyniosły ponad 200% w porównaniu z innymi miesiącami, co świadczy o tym, że cyberprzestępcy wybierają m.in. ten okres na swoje „łowy” – piszą na swoim blogu eksperci Check Point.**

Podobny, choć mniej stabilny trend zaobserwowano na stronach internetowych używających słowa „czekolada” - w 2018 r. Wzrost wyniósł prawie 500% w lutym, podczas gdy w 2019 r. był bardziej umiarkowany i wynosił zaledwie 39%.

Używanie m.in. tych słów przez osoby atakujące służy dwóm głównym celom: zwabieniu użytkowników, którzy prawdopodobnie są zainteresowani stronami związanymi z walentynkami, i ukryciu się wśród wielu innych legalnych stron walentynkowych, które są odwiedzane o tej porze roku. Tylko w pierwszym tygodniu lutego 2020 r. internauci mieli dostęp do ponad 10 000 domen zawierających słowo „Walentynki” (Valentine).

Cyberprzestępcy nie tylko zatrzymują się na zwodniczych nazwach witryn, ale również wykorzystują fałszywe wiadomości e-mail w celu zwabienia użytkowników do stron phishingowych, a nawet w celu bezpośredniego rozprzestrzeniania złośliwego oprogramowania. Jak twierdzi Check Point, w zeszłym roku kampania spamowa odbywająca się w okresie walentynkowymi, z tematem wiadomości „To jest mój list miłosny do ciebie”, rozprzestrzeniała GandCrab Ransomware. W tym roku eksperci zauważyli już kilka przykładów walentynkowych spamów. Pierwszy e-mail, na który powinniśmy zwrócić uwagę jest częścią kampanii Ursnif z tematem wiadomości „Przeglądam twój profil i uwielbiam go… Więc to są moje najlepsze zdjęcia…” – podszywający się pod portale randkowe.

Pozostałe wykryte złośliwe pliki były częścią kampanii Emotet Botnet, która jest obecnie najbardziej znanym złośliwym oprogramowaniem, rozpowszechnianym za pośrednictwem szeroko zakrojonych kampanii spamowych. Najczęściej dotyczą one dużych wydarzeń (takich jak Halloween i Boże Narodzenie) aby zwabić ofiary do pobrania złośliwego oprogramowania. Tym razem złośliwe pliki zostały wysłane m.in. w wiadomości e-mail o temacie: „Nie wyobrażam sobie życia sam. Potrzebuję ukochanego”.

Jak uniknąć zagrożeń związanych z zainfekowanym spamem? Zalecenia Check Pointa są następujące:

1. Sprawdź, czy zamawiasz online z autentycznego źródła. Jednym ze sposobów na to jest NIE klikanie linków promocyjnych z e-maili; zamiast tego wykorzystaj wyszukiwarkę Google do odnalezienia oferty.

2. Uważaj na „wyjątkowe” oferty. 80% zniżki na nowy iPad zazwyczaj nie jest niezawodną ani godną zaufania okazją do zakupu.

3. Uważaj na podobne domeny, błędy ortograficzne w wiadomościach e-mail lub witrynach internetowych oraz nieznanych nadawców wiadomości e-mail.