aut. Szymon Palczewski 10.09.2020

NAJPIERW FRANCJA, TERAZ JAPONIA I NOWA ZELANDIA. SERIA CYBERATAKÓW TRWA

Francja, Japonia i Nowa Zelandia ostrzegają przed światową kampanią hakerską, wymierzoną w podmioty prywatne oraz państwowe. W ramach operacji cyberprzestępcy wykorzystują złośliwe oprogramowanie Emotet do kradzieży wrażliwych danych i prowadzenia szeroko zakrojonych kampanii spamowych. Ofiarami hakerów padli między innymi prawnicy pracujący w jednym z sądów w Paryżu.

Agencje cyberbezpieczeństwa z Francji, Japonii i Nowej Zelandii wydały specjalne alerty, ostrzegające przed wzrostem liczby cyberataków, wykorzystujących złośliwe oprogramowanie Emotet.

Francuska National Cybersecurity Agency (fra. *Agence nationale de la sécurité des systèmes d'information*, ANSSI) zaobserwowała cyberataki wymierzone w krajowe firmy oraz sektor państwowy, których kluczowym elementem jest wirus Emotet. „Emotet jest obecnie używany do deponowania innego złośliwego kodu, który może mieć silny wpływ na ofiary" – czytamy w alercie opublikowanym przez CERT-FR.

Początkowo Emotet był uznawany za trojana bankowego, jednak z biegiem czasu wirus ewoluował. Obecnie złośliwe oprogramowanie pozwala między innymi na przejęcie haseł przechowywanych w systemach ofiar, w tym przeglądarkach internetowych oraz poczty, a także kradzież danych pochodzących z e-maili (np. plików z załącznikach czy listy kontaktów). Emotet łatwo rozprzestrzenia się w docelowej sieci, wykorzystując luki w zabezpieczeniach oraz pozyskane hasła dostępu.

Francuski CERT wskazuje, że złośliwe oprogramowanie jest rozsyłane za pomocą masowych kampanii e-maili phishingowych. „Te wiadomości phishingowe zazwyczaj zawierają złośliwe załączniki Word lub PDF" – stwierdzono w alercie. Analiza przeprowadzona przez specjalistów ANSSI wykazała, że po pięciomiesięcznym okresie „wygaszenia" kampanie z użyciem Emotet ponownie pojawiły się w lipcu bieżącego roku.

„Po włamaniu do skrzynki odbiorczej pracownika podmiotu będącego ofiarą (lub ogólnej skrzynki odbiorczej podmiotu) złośliwy kod Emotet wydobywa zawartość niektórych wiadomości e-mail" – tłumaczą francuscy specjaliści. Na tej podstawie hakerzy generują wiadomości phishingowe w postaci odpowiedzi w ramach wewnętrznej komunikacji w danej placówce. „Tytuł wiadomości poprzedza słowo >Re:<, a sam e-mail zawiera historię całej korespondencji oraz przesyłanych plików" – czytamy w alercie.

Złośliwe wiadomości są rozsyłane do kontaktów ofiary, w szczególności osób, które brały udział w określonej korespondencji. Ma to na celu zwiększenie wiarygodności przesyłanych treści i skłonienie odbiorców do dalszej interakcji.

Z kolei japoński CERT (JPCERT) wykrył wzrost liczby operacji hakerskich z udziałem Emotet dopiero od

września bieżącego roku. Analiza przeprowadzona przez specjalistów pokrywa się z wynikami otrzymanymi przez francuską ANSSI. „Główna droga infekcji Emotet jest nadal taka sama, czyli poprzez załączniki lub wiadomości e-mail z linkami w treści" – czytamy w alercie wydanym przez JPCERT.

Japońscy specjaliści scharakteryzowali złośliwe oprogramowanie jako wirusa, który nie tylko kradnie informacje, ale także rozsyła wiadomości spamowe, wykorzystując pozyskane z systemu ofiary dane w celu rozprzestrzeniania infekcji.

„Po infekcji wirus umożliwia pobranie innego złośliwego oprogramowania, takiego jak TrickBot i Qbot (Qakbot), co może spowodować poważny incydent, w tym zaszyfrowanie danych przy pomocy ransomware" – wskazują specjaliści japońskiego CERT-u.

O kampanii z udziałem Emotet zaalarmował również nowozelandzki CERT. W ostrzeżeniu wskazano, że hakerzy przywiązują dużą staranność do ukrycia swojej operacji. „CERT NZ jest świadomy zagrożenia związanego ze zwiększoną aktywnością Emotet, wpływającą na nowozelandzkie organizacje" – czytamy na oficjalnej stronie CERT-u. Specjaliści nie mają wątpliwości, że celem cyberataków mogą być zarówno osoby fizyczne, jak i firmy.

Serią cyberataków z udziałem wirusa Emotet zainteresował się również Joseph Roosen, specjalista ds. cyberbezpieczeństwa firmy Cryptolaemus.

> Kinda surprised that Ivan hasn't come roaring back this week. I wonder how much of an issue it was that E3 bots were moved to E1. E3 is still alive with modules of it's own coming down. Something likely broke in the backend or cleaning up Fri's mess. Be back when they spam again https://t.co/HgykhibEb4
>
> — Joseph Roosen (@JRoosen) September 9, 2020

W wywiadzie dla serwisu ZDNet specjalista wskazał, że w czasie trwania kampanii wymierzonej w Nową Zelandię, równocześnie można było zaobserwować cyberataki ukierunkowane w japońskie podmioty. Przeniesienie działań hakerskich do tych państw sprawiło, że we Francji spadła liczba incydentów z udziałem Emotet.

Cyberprzestępcom udało się jednak skutecznie naruszyć sieci i systemy jednego z paryskich sądów. Wśród ofiar cyberataku znajdowali się nie tylko sędziowie, ale także francuscy prawnicy – poinformował francuski tygodnik Le Journal du Dimanche.

Rémy Heitz, jeden z poszkodowanych prokuratorów, wszczął śledztwo w celu ustalenia sprawców incydentu. Jego przeprowadzenie zostało powierzone Dyrekcji Bezpieczeństwa Wewnętrznego (DGSI) ze względu na „delikatny charakter sprawy".

Czytaj też: Cyberatak na Gruzję. Jest reakcja Stanów Zjednoczonych