**Cyberprzestępcy atakują trojanami bankowymi w wakacje. Wzrost aktywności nawet o 50%!**

**Lawinowo rośnie zagrożenie trojanami bankowymi – rodziną niebezpiecznych wirusów, które m.in. wykradają poufne informacje o naszych kontach bankowych podczas używania zainfekowanego komputera – wskazują eksperci w raporcie Globalny Indeks Zagrożeń Check Point.**

 **Eksperci zwracają uwagę, że cyberprzestępcy za pomocą trojanów chcą m.in. wykorzystać mniejszą świadomość cyberbezpieczeństwa turystów i podróżnych, którzy korzystają z mobilnych urządzeń dokonując wielu płatności. Najwięcej ataków było na Mołdawię i Macedonię. Choć Polska ulokowała się dopiero na 22 miejscu w Europie, to należała do najmniej narażonych na ataki krajów świata.**

W ciągu ostatnich czterech miesięcy, tzw. trojany bankowe zwiększyły swoją aktywność o 50%, a ich dwa rodzaje dołączyły do dziesiątki najpowszechniejszych złośliwych programów wg Global Threat Index firmy Check Point. Choć w okresie letnim rośnie zagrożenie tego typu atakami, ogólna sytuacja w poszczególnych państwach poprawiła się: Lichtenstein, Islandia i Estonia były najbezpieczniejszymi krajami w Europie; natomiast na przeciwległym biegunie znalazły się Mołdawia i Macedonia. Polska, która uplasowała się na 22 pozycji w Europie, znalazła się wśród najbezpieczniejszych krajów na świecie (współczynnik zagrożenia poniżej 40).

W czerwcu 2018 r. trojan bankowy o nazwie Dorkbot (kradnie poufne informacje i uruchamia ataki typu denial-of-service) zainfekował 7% wszystkich organizacji na całym świecie, awansując z 8 na 3 miejsce na liście najbardziej popularnych typów malware (Check Point's Most Wanted Malware). W zeszłym miesiącu aktywny był również Emotet, bankowy trojan, który kradnie konta bankowe ofiar podczas wykorzystywania komputera ofiary do rozprzestrzeniania się. W ciągu ostatnich dwóch miesięcy gwałtownie wzrosła również popularność wariantu Emotet: z 50. miejsca w kwietniowym Indeksie „awansował” na 11. pozycję w najnowszym zestawieniu. Wraz z Dorkbotem w pierwszej dziesiątce znalazł się również trojan Ramnit, który kradnie dane bankowe oraz hasła FTP.

**Badacze Check Pointa zaobserwowali podobny agresywny schemat ataków cyberprzestępców wykorzystujących bankowe konie trojańskie latem 2017 roku. Sugeruje to, że cyberprzestępcy mogą próbować wykorzystywać turystów do zwiększenia swoich zysków, ponieważ podczas lata i wakacji poświęcają mniej uwagi praktykom w zakresie bezpieczeństwa cybernetycznego. Potencjalnie mogą oni uzyskiwać dostęp do bankowości internetowej za pośrednictwem współdzielonych urządzeń dostępowych i mniej bezpiecznych połączeń, takich jak publiczne punkty dostępu WiFi.**

Aby zapobiec wykorzystywaniu sieci przez bankowe konie trojańskie i inne rodzaje ataków, przedsiębiorstwa muszą stosować wielowarstwową strategię bezpieczeństwa cybernetycznego, która chroni zarówno przed atakami cybernetycznymi z rodzin o ustalonej pozycji, jak i przed zupełnie nowymi zagrożeniami.

Poniżej przedstawiamy listę najpopularniejszych typów malware wg Check Pointa:

**Top 5 malware w czerwcu 2018:**

1. **↔ Coinhive** - Crypominer przeznaczony do wydobywania kryptowaluty Monero bez zgody użytkownika odwiedzającego stronę internetową. Coinhive pojawił się dopiero we wrześniu 2017 r., ale już w tym czasie infekował 12% organizacji na całym świecie.

2. **↔ Cryptoloot** - Cryptominer JavaScript, przeznaczony do wydobywania kryptokrypty Monero podczas odwiedzin użytkownika na stronie internetowej bez jego zgody.

3. **↑Dorkbot-** Oparty na IRC robak umożliwiający zdalne wykonywanie kodu przez operatora oraz pobieranie dodatkowego złośliwego oprogramowania do zainfekowanego systemu. Jest to bankowy trojan, którego głównym zadaniem jest kradzież poufnych informacji i przeprowadzanie ataków typu denial-of-service.

4. **↑ Andromeda** - Modułowy bot używany głównie jako backdoor do dostarczania dodatkowego złośliwego oprogramowania na zainfekowanych hostach, ale może być modyfikowany w celu utworzenia różnego rodzaju botnetów.

5. **↓ Roughted** - kampania malvertisingowa na olbrzymią skalę, dostarczająca różnego rodzaju scam, adware, exploit kity oraz ransomware. Może być przeprowadzona w atakach na każdy typ platform i systemów operacyjnych.

Eksperci Check Pointa przeanalizowali również najbardziej wykorzystane podatności. Na czele jest CVE-2017-7269, z udziałem na poziomie 40%. Kolejne miejsce zajęła podatność CVE-2017-10271 dotycząca 35% organizacji na całym świecie. Na trzecim miejscu znalazło się SQL injection wpływające na 15% organizacji na całym świecie.