**Cyberzagrożenia w Polsce: Kryptominer Coinhive wciąż dominuje. Uwaga na botnety i trojany!**

**Malware „kopiący” kryptowalutę Monero jest najpopularniejszym złośliwym oprogramowaniem zarówno w Polsce jak i na świecie – wskazują eksperci ds. cyberbezpieczeństwa z firmy Check Point Software Technologies. Choć wciąż wśród zagrożeń dominują kryptominery, to w listopadzie badacze zidentyfikowali szereg kampanii sezonowych, które rozpowszechniały botnet Emotet.**

Stworzony przez badaczy indeks zagrożeń wskazuje, że botnet Emotet znalazł się na 7. miejscu pierwszej dziesiątki najpowszechniejszych zagrożeń, po tym, jak rozprzestrzenił się on w kilku kampaniach, w tym w kampanii związanej ze świętem dziękczynienia.Dawniej botnet Emotet był używany jako trojan bankowy, ale ostatnio jego użycie zmieniło się, ze względu na to, że pozwala on atakującym na wdrażanie innych złośliwych programów i złośliwych kampanii. Jego dystrybucja za pośrednictwem poczty elektronicznej - zawierającej świąteczne motywy, linki i załączniki - zwiększyła się aż o 25% w porównaniu z ubiegłym miesiącem.

Na podstawie analizy polskich sieci firmowych, firma Check Point udostępniła również dane o czołowych zagrożeniach wykrytych w Polsce w listopadzie. Liderem był Coinhive (złośliwa koparka kryptowaluty Monero), infekujący około 13,5% polskich firm. Drugie miejsce, z zasięgiem ponad 11% należy do Roughted, kampanii malwertisingowej, dostarczającej różnego rodzaju scam, adware, exploit kity oraz ransomware. Może być ona przeprowadzona w atakach na każdy typ platform i systemów operacyjnych! Podium zamyka z kolei trojan Emotet (zasięg 8,2%), wysyłający informacje o systemie do wielu serwerów kontrolnych i pobierający liczne pliki konfiguracyjne i inne komponenty. Podobno kampania ta jest kierowana do klientów niektórych banków.

W globalnym rankingu cyberzagrożeń, cztery z dziesięciu pierwszych miejsc zajmują kryptominery, które powoli ustępują miejsca bardziej wielofunkcyjnemu złośliwemu oprogramowaniu, które może dostarczyć różnego rodzaju „ładunki” za jednym zamachem. Kryptominer Coinhive jest niekwestionowanym, światowym liderem Indeksu od grudnia 2017 roku! Ten typ kryptominera wykorzystywał zasoby aż 24% organizacji na całym świecie, podczas gdy całościowy wpływ kryptominerów wyniósł 38%!

**TOP 3 malware na świecie:**

1. **↔ Coinhive -** krypominer 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 wykorzystujący moc procesora lub procesora graficznego ofiary oraz istniejące zasoby do wytworzenia nowej waluty. Dodaje transakcje do tzw. Blockchainu, wprowadzając nową walutę.

1. **↑ 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.

W przypadku urządzeń mobilnych wciąż króluje Triada, czyli modułowy backdoor dla systemu Android. Hiddad wspiął się na drugie miejsce, zastępując Android banking Trojan i info-stealer Lokibot, który spadł na trzecie miejsce.

**TOP 3 mobilnego malware:**

1.  **Triada -** Modułowy backdoor dla systemu Android, który nadaje uprawnienia superusera do pobierania złośliwego oprogramowania.

2. **Hiddad -** złośliwe oprogramowanie na Androida, które przepakowuje legalne aplikacje, a następnie udostępnia je do sklepów stron trzecich. Jego główną funkcją jest wyświetlanie reklam, jednak może również uzyskać dostęp do kluczowych szczegółów zabezpieczeń wbudowanych w system operacyjny, co pozwala atakującemu uzyskać poufne dane użytkownika.

3. **Lokibot -** trojan bankowy na Androida oraz złodziej danych, który w przypadku nadania uprawnień administratorskich jest również w stanie zablokować telefon.

Badacze Check Point przeanalizowali również najczęściej wykorzystywane cyberpodatności. Po raz kolejny CVE-2017-7269 znajduje się na pierwszym miejscu listy najczęściej wykorzystywanych podatności, z oddziaływaniem na 48% organizacji w skali światowej. OpenSSL TLS DTLS DTLS Heartbeat Information Disclosure utrzymuje drugie miejsce z globalnym zasięgiem 44%. CVE-2016-6309, będąca podatnością w funkcji tls\_get\_message\_body OpenSSL jest obecnie na trzecim miejscu i występuje w przypadku 42% organizacji!