# Eksperci z laboratorium Threat Lab: przewidzieli ataki typu WannaCry, teraz prognozują co wydarzy się w 2018

**Kraków, dnia 12.12.2017 r. – Firma Bakotech, wyłączny dystrybutor rozwiązań firmy WatchGuard w Polsce, przedstawia przewidywania laboratorium badawczego Threat Lab od WatchGuard'a, dotyczące cyberbezpieczeństwa w 2018 roku.**

**Trafione prognozy cyberbezpieczeństwa 2017 – Ransomworm jednak zaatakował**

Eksperci z laboratorium badawczego WatchGuard, tzw. Threat Lab, przewidzieli to, że pojawi się pierwszy w historii Ransomworm, który spowoduje, że oprogramowanie Ransomware rozprzestrzeni się jeszcze szybciej. Faktycznie, cyberprzestępcy przenieśli oprogramowanie typu Ransomware na nowy poziom w 2017 roku, wprowadzając cechę automatycznego rozprzestrzeniania się w tradycyjnie spotykanych robakach sieciowych typu CodeRed i Conficker. Oprogramowanie miało tworzyć nieskończoną liczbę duplikatów, rozprzestrzeniając infekcję w całej sieci. Biorąc pod uwagę atak WannaCry, można uznać, że przewidywania okazały się bardzo trafione.

Prognozy z 2017 roku można znaleźć tutaj:

https://www.secplicity.org/2016/12/19/2017-security-predictions-threats-real/

**Jak będzie wyglądało cyberbezpieczeństwo w 2018 roku?**

**Kryptowalutowa awaria:** czy hakerzy znajdą podatność na tyle poważną, aby całkowicie wyprzeć popularną kryptowalutę?

Wartość kryptowalut stale rośnie i monety Bitcoin, Ethereum i Litecoin są warte miliardy, natomiast przestępcy potrzebują szybkiej gotówki. W 2016 kwoty uzyskane na atakach na Ethereum sięgały kwot między 100 a 500 milionów dolarów, możliwość hakowania została jednak zablokowana. Możliwe, że przestępcy wykorzystają luki w łańcuchach relacji kryptowalutowych w nadchodzącym roku i obalą główną kryptowalutę.



BAKOTECH Sp. z o.o.
ul. Św. Tomasza 34/B09, 31-027 Kraków
e-mail: kontakt@bakotech.com, tel. +48 12 376 95 08

**Hakowanie Wi-Fi:** Wi-Fi jest popularnym celem hakerów, ale w jaki sposób radio zdefiniowane przez oprogramowanie wpłynie na wybór docelowego protokołu bezprzewodowego w 2018 roku?

Od kilku lat Wi-Fi Pineapple ułatwia pracę hakerom amatorom na całym świecie. Oczekują oni, że utowarowienie narzędzi ataków Wi-Fi zmieni się w programowo zdefiniowane radia (SDR), które umożliwią im łatwy dostęp do bezprzewodowych protokołów, takich jak Zigbe, Sigfox, Bluetooth i inne. Łatwo dostępne SDR-y mogą pozwolić na kradzież danych uwierzytelniających sieć w lokalnym centrum handlowym.

**Korporacyjne zabezpieczenia przeciw cybernetycznym atakom zyskają na popularności:** Przestępcy posługujący się atakami typu ransomware chcą zwiększyć skuteczność swoich działań – czy klienci korzystający z usług wymuszenia cybernetycznego będą bardziej skłonni do płacenia?

Hakerzy będą koncentrować się na zwiększeniu zysku, za pomocą oprogramowania ransomware będą atakować firmy zabezpieczone cybernetycznie. W porównaniu z wiadomościami spamowymi, które zazwyczaj mają mniej niż 1% skuteczności, większość badań wykazuje, że przynajmniej 1/3 ofiar ransomware płaci. Hakerzy opracowują nowe plany dotyczące ataków na dostawców ubezpieczeń (w celu uzyskania dostępu do list klientów), ale także dzielenia ich na drugorzędne ataki na firmy, które obejmują.

**Botnety IoT wymuszają nowe regulacje:** ile czasu minie zanim poważny atak botnetowy IoT spowoduje, że rządy będą zajmować się bezpieczeństwem IoT poprzez wprowadzenie regulacji?

Bruce Scheiner, ekspert ds. bezpieczeństwa opublikował w zeszłym roku esej, gdzie nazwał bezpieczeństwo urządzeń typu IoT formą „niewidzialnego zanieczyszczenia", gdzie nie ma zachęt rynkowych dla producentów do budowania bezpieczniejszych produktów. Właśnie dlatego w 2017 obserwowaliśmy dużo ataków typu DDoS, które opierały się na ogromnej liczbie niezabezpieczonych urządzeń, takich jak kamery internetowe, cyfrowe rejestratory wideo i inteligentne żarówki. Z kolei analityk zagrożeń WatchGuard, Marc Laliberte, przewiduje, że niezwykle skuteczny atak botnet, podobny do Mirai, uderzy w 2018, a to z kolei powinno spowodować wprowadzenie nowych regulacji dotyczących minimalnych wymagań bezpieczeństwa dla producentów urządzeń IoT. Zdalny dostęp przez Telnet lub SSH powinien być domyślnie wyłączony (lub usunięty), trzeba byłoby zastosować zakodowane hasła (lub co najmniej wymagające zmiany hasła podczas instalacji).


BAKOTECH Sp. z o.o.
ul. Św. Tomasza 34/B09, 31-027 Kraków
e-mail: kontakt@bakotech.com, tel. +48 12 376 95 08

**Podwoi się ilość ataków linuxowych:** na podstawie badań przeprowadzonych przez WatchGuard Threat Lab, ataki specyficzne dla Linuksa rosną, ale czy będą kontynuowane w 2018 roku?

Wiele urządzeń IoT wykorzystuje wbudowane systemy Linux, które są znane z posiadania niezabezpieczonych ustawień domyślnych. Poprzez stworzenie niewielkiego kodu złośliwego oprogramowania, hakerzy uważają, że mogą podwoić moc swoich botnetów. Szkodliwe oprogramowanie dla Linuxa stanowiło 36% topowego złośliwego oprogramowania od Q1 2017, a WatchGuard Threat Lab oczekuje, że liczba ta podwoi się w 2018. W tym wypadku ujednolicone rozwiązania do zarządzania zagrożeniami (UTM) sprawdzą się najlepiej jako ochrona przed takim zagrożeniem.

**Uwierzytelnianie wieloskładnikowe:** w jaki sposób małe i średnie firmy będą radzić sobie z naruszaniem danych i wyciekami haseł – czy dzięki wieloczynnikowemu uwierzytelnianiu, będziemy mogli zastosować nowe rozwiązania MFA (multi-factor authentication)?

Pełne prognozy cyberbezpieczeństwa na 2018 rok są dostępne tutaj:

https://www.watchguard.com/wgrd-resource-center/2018-security-predictions



BAKOTECH Sp. z o.o.
ul. Św. Tomasza 34/B09, 31-027 Kraków
e-mail: kontakt@bakotech.com, tel. +48 12 376 95 08

**O WatchGuard**

Firma WatchGuard Technologies powstała w 1996 roku w Seattle. Od samego początku producent skupił się na rozwiązaniach dotyczących bezpieczeństwa sieciowego. To właśnie WatchGuard zaprojektował i uruchomił pierwszą zaporę sieciową. Firma zatrudnia ponad 500 pracowników i ma swoje przedstawicielstwa na wszystkich kontynentach. Producent regularnie klasyfikowany jako lider i wizjoner w raportach Gartnera dla UTM/NGFW, ma na swoim koncie ponad milion wdrożonych rozwiązań do zapewniania bezpieczeństwa, zarówno w sektorze małych i średnich przedsiębiorstw, jak i w dużych firmach na całym świecie. System raportowania, wizualizacji systemu i zarządzania, **WatchGuard Dimension,** uznawany jest jako wzór dla konkurencji, co potwierdzają liczne nagrody branżowe.

**Więcej informacji:**

BAKOTECH Sp. z o.o.
Agnieszka Trenda
PR&Marketing Manager, tel. 660 910 074
e-mail: agnieszka.trenda@bakotech.com
www.bakotech.pl

**O BAKOTECH**

Bakotech Sp. z o.o. z siedzibą w Krakowie, jest częścią międzynarodowej grupy dystrybucyjnej Bakotech®. Jako specjalizowany dystrybutor rozwiązań IT w zakresie bezpieczeństwa, sieci i infrastruktury IT, spółka koncentruje się na dostarczaniu najwyższej jakości produktów i usług w centralnej i wschodniej Europie, w szczególności w: Polsce, Bułgarii, Rumunii, Słowacji, Chorwacji i na Węgrzech, a także w krajach nadbałtyckich. Firma zajmuje się sprzedażą w kanale partnerskim, poprzez rozbudowaną sieć partnerów. Bakotech posiada w swoim portfolio innowacyjne produkty, które odniosły sukces międzynarodowy, a dzięki dystrybutorowi wchodzą nie tylko na rynek polski, ale również krajów Europy Środkowo-Wschodniej.