Bezpieczeństwo w sieci za Q4 2017: ataki typu „Makro” i „Zero-Day” wzrosły o 167 procent

Kraków, dnia 26.04.2018 r. – Firma Bakotech, wyłączny dystrybutor rozwiązań firmy WatchGuard w Polsce, informuje, że WatchGuard opublikował kolejny raport dotyczący bezpieczeństwa w internecie, obejmujący okres Q4 2017.

Wśród najważniejszych wniosków raportu, informacje o zagrożeniach ze sprzętu Firebox chroniące małe i średnie firmy (SMB) i rozproszone przedsiębiorstwa na całym świecie wykazały, że liczba ataków szkodliwego oprogramowania wzrosła o 33 procent, a cyberprzestępcy coraz częściej wykorzystują dokumenty Microsoft Office do dostarczania malwaru. WatchGuard uruchomił także nowe narzędzie do wizualizacji danych o zagrożeniach, dostępne publicznie, aby uzyskać dostęp do codziennych aktualizacji dotyczących najczęściej występujących zagrożeń bezpieczeństwa komputerowego i sieciowego mających wpływ na małe i średnie firmy oraz przedsiębiorstwa rozproszone.

"Po całym roku zbierania i analizowania danych Firebox Feed możemy wyraźnie zobaczyć, że cyberprzestępcy nadal wykorzystują zaawansowane ataki i pomysłowe schematy dostarczania złośliwego oprogramowania w celu kradzieży cennych danych" - powiedział Corey Nachreiner, dyrektor ds. Technologii w WatchGuard Technologies. "Chociaż te taktyki mogą się zmieniać w czasie, możemy być pewni, że ten trend utrzyma się, więc ryzyko nigdy nie było większe dla małych i średnich organizacji dysponujących mniejszymi zasobami IT i bezpieczeństwa. Zachęcamy firmy różnej wielkości do proaktywnego łagodzenia tych zagrożeń za pomocą warstwowych usług bezpieczeństwa, zaawansowanej ochrony przed złośliwym oprogramowaniem oraz edukacji pracowników i szkoleń w zakresie najlepszych praktyk bezpieczeństwa. "

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

Raport Internet Security WatchGuard zawiera kwartalną aktualizację najbardziej powszechnych zagrożeń bezpieczeństwa skierowanych obecnie do firm, a także kluczowe strategie, które mogą wykorzystać do ochrony pracowników i klientów przed kradzieżą danych.

Najważniejsze wnioski z raportu za IV kwartał 2017:

- **Cyberprzestępcy wykorzystali złośliwe dokumenty Office, aby oszukać ofiary**

Dynamiczne wymiany danych (DDE) znalazły się w pierwszej dziesiątce szkodliwych programów WatchGuard w czwartym kwartale, a hakerzy coraz częściej wykorzystywali problemy w tym standardzie Microsoft Office do wykonywania kodu. Nazywane również "złośliwym oprogramowaniem bezzakłóceniowym", te złośliwe dokumenty często używają PowerShell i specjalnego skryptu, aby ominąć zabezpieczenia sieciowe. Ponadto dwa z dziesięciu najczęstszych ataków sieciowych w czwartym kwartale dotyczyły exploitów Microsoft Office, dodatkowo podkreślając rosnącą tendencję do złośliwych ataków na dokumenty.

- **Ogólne ataki szkodliwego oprogramowania znacznie wzrosły, podczas gdy malware typu zero-day wzrósł o 167 procent**

WatchGuard Fireboxes zablokował w czwartym kwartale ponad 30 milionów wszystkich wariantów złośliwego oprogramowania, co stanowiło 33-procentowy wzrost w stosunku do poprzedniego kwartału. Spośród ogółu zagrożeń wyeliminowanych w czwartym kwartale, liczba nowych lub złośliwych instancji złośliwego oprogramowania gwałtownie wzrosła o 167 procent w porównaniu do trzeciego kwartału. Wzrost ten prawdopodobnie można przypisać zwiększonej działalności przestępczej w okresie wakacyjnym.

- **Prawie połowa wszystkich szkodliwych programów nie była rozpoznawana przez podstawowe rozwiązania antywirusowe (AV).**

WatchGuard Fireboxes blokuje złośliwe oprogramowanie za pomocą obu technik wykrywania opartych na sygnaturach i nowoczesnym, proaktywnym rozwiązaniu do wykrywania zachowań - APT Blocker. Kiedy APT Blocker wykrywa wariant złośliwego oprogramowania, oznacza to, że starsze programy AV oparte na sygnaturach, go przegapiły. To złośliwe oprogramowanie typu zero-day stanowiło 46 procent wszystkich złośliwych programów w czwartym kwartale. Ten poziom wzrostu sugeruje, że przestępcy używają bardziej wyrafinowanych technik

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

maskowania się, zdolnych do zrzucania ataków poza tradycyjne usługi AV, co dodatkowo podkreśla znaczenie mechanizmów obronnych opartych na zachowaniu.

- **Ataki przy użyciu skryptów stanowią 48 procent złośliwego oprogramowania**

Ataki oparte na skryptach przechwycone przez sygnatury dla skryptów JavaScript i Visual Basic Script, takie jak downloadery i droppery, stanowiły większość wykrytych złośliwych programów w czwartym kwartale. Użytkownicy powinni wziąć pod uwagę ciągłą popularność tych ataków i uważać na złośliwe skrypty na stronach internetowych i wszelkiego rodzaju załączniki do wiadomości e-mail.

Pełny raport o zabezpieczeniach internetowych zawiera opis najbardziej rozpowszechnionego złośliwego oprogramowania i ataków sieciowych w kwartale, zalecenia dotyczące użytecznych strategii obronnych w dzisiejszym środowisku zagrożeń oraz szczegółową analizę "the Krack Attack" - jednego z najważniejszych problemów związanych z bezpieczeństwem informacji w 2017 roku.

Ponadto raport zawiera nowy projekt badawczy z WatchGuard Threat Lab, który analizuje bazę danych zawierającą ponad 1 miliard skradzionych rekordów haseł, aby podkreślić, jak często użytkownicy wybierają słabe hasła i ponownie wykorzystują dane uwierzytelniające na wielu kontach. Wnioski z tego kwartału oparte są na anonimowych danych Firebox Feed z prawie 40 000 aktywnych firewalli WatchGuard na całym świecie, które blokowały ponad 30 milionów wariantów szkodliwego oprogramowania (783 na urządzenie) i 6,9 milionów ataków sieciowych (178 na urządzenie) w czwartym kwartale 2017 r.

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.