**WatchGuard Internet Security Report: 30% malwaru to nowości lub zero-day**

**WatchGuard Technologies, lider w zaawansowanej ochronie sieciowej, 30 marca 2017 opublikował wyniki inauguracyjnego raportu, który przedstawia najnowsze zagrożenia sieciowe na jakie narażone są firmy typu SMB oraz przedsiębiorstwa rozproszone. Raport pokazuje najnowsze trendy dotyczące sieci i szkodliwego oprogramowania od czwartego kwartału 2016, analizuje najważniejsze historie dotyczące bezpieczeństwa sieciowego, zawiera szczegółowe badania przeprowadzone przez Threat Lab (laboratorium WatchGuard) oraz praktyczne wskazówki dotyczące bezpieczeństwa skierowane do specjalistów z tej dziedziny.**

Dane w raporcie są oparte na anonimowych danych Firebox Feed z urządzeń UTM WatchGuard zainstalowanych na całym świecie.

„Nasze **Laboratorium - Threat Lab** monitoruje najczęstsze zagrożenia i trendy w branży zabezpieczeń od lat, a teraz dzięki dodatkowi Firebox Feed – anonimowemu narzędziu analitycznemu z Fireboxów zainstalowanych na całym świecie, mamy bezpośredni wgląd w ewolucję cyberataków oraz w to, jak zachowują się użytkownicy objęci atakiem” – powiedział Corey Nachreiner, Chief Technology Oficer z WatchGuard Technologies. „Co kwartał, nasz raport będzie zawierał nowe dane pochodzące z Firebox Feed wraz z oryginalnymi badaniami i analizą najważniejszych wydarzeń związanych z bezpieczeństwem informacji, po to aby ujawnić kluczowe trendy dotyczące zagrożeń oraz zapewnić najlepsze działania ochronne”.

W 2016 cyberprzestępcy mieli mnóstwo „pracy”, biorąc pod uwagę cyberataki takie jak Mirai Botnet, ataki bankowe SWIFT oraz domniemaną ingerencję rosyjską w wyborach prezydenckich, w Q4 nie było inaczej. Ransomware poprzez fałszywe e-maile i złośliwe witryny internetowe próbował wyłudzić dane pozwalające na uporczywe ataki skierowane na banki, instytucje rządowe oraz służbę zdrowia.

**Oto pięć najważniejszych ustaleń wynikających z raportu:**

l **Maksymalnie 30% zagrożeń typu malware, zostało zakwalifikowanych jako nowe lub „zero day”,** ponieważ nie zostały wykryte przez oprogramowanie antywirusowe. To potwierdza, że zdolność cyberprzestępców do automatycznego przepakowywania lub modyfikowania szkodliwego oprogramowania przewyższała zdolność przemysłu AV do nadążania za nowymi sygnaturami. Bez zaawansowanego rozwiązania zapobiegającego zagrożeniom i identyfikującego w sposób aktywny złośliwe oprogramowanie, przy użyciu nowoczesnych technik, firmy mogą przegapić nawet 1/3 malwaru.

l **Stare zagrożenia stają się nowe.** Po pierwsze, złośliwe oprogramowanie bazujące na makrach, wciąż jest bardzo popularne. Pomimo starego triku, wiele prób wyłudzania informacji wciąż zawiera dokumenty ze złośliwymi makrami i atakujący dostosowują swoje sztuczki do najnowszego formatu dokumentów Microsoft. Po drugie, atakujący wciąż wykorzystują złośliwe serwery internetowe do przejęcia serwerów WWW. Mechanizmy PHP są wciąż aktualne i napastnicy wykorzystują tą starą metodę przy użyciu nowych metod ukrywania zamierzonego kierunku komunikacji.

l **JavaScript jest popularnym mechanizmem dostarczania złośliwego oprogramowania i ukrywania zamierzonego kierunku komunikacji.** Firebox Feed zanotował wzrost złośliwego kodu JavaScript, zarówno w mailach, jak i przez Internet.

l **Większość ataków sieciowych dotyczy usług internetowych i przeglądarek.** 73% największych ataków dotyczy przeglądarek internetowych w atakach typu drive-by download.

l **Topowe ataki sieciowe tj. Wscript.shell Remote Code Execution, niemal całkowicie dotyczyły Niemiec.** Przyglądając się poszczególnym krajom, ten atak dotyczył Niemiec w 99% czasu.

WatchGuard Internet Security Report bazował na anonimowych danych pochodzących z ponad 24,000 aktywnych urządzeń UTM zainstalowanych na całym świecie. Urządzenia te blokowały ponad 18,7 miliona wariantów złośliwego oprogramowania w Q4, co średnio dawało 758 wariantów na urządzenie uczestniczące. Urządzenia blokowały również ponad 3mln ataków sieciowych w Q4, co średnio daje 123 ataki na każde urządzenie uczestniczące. Raport zawiera szczegółowy opis największych ataków złośliwego oprogramowania i trendów bezpieczeństwa, największych incydentów bezpieczeństwa oraz trendów w zakresie ataków sieciowych i poczty elektronicznej. W odpowiedzi na gwałtowne rozprzestrzenianie się botnetu Mirai, Threat Lab uruchomiło trwający projekt badawczy, który analizuje urządzenia IoT pod względem luk w zabezpieczeniach. Badania kładły nacisk na ocenę kamer IP podłączonych przez Wi-Fi, akcesorii do fitnesu oraz innych nowych urządzeń których cechą charakterystyczną jest wbudowany system operacyjny pozwalający na ruch sieciowy. To wszystko pokazuje głębsze spojrzenie na luki w zabezpieczeniach, które Threat Lab znalazło w stosunkowo popularnych bezprzewodowych kamerach IP oraz działania jakie konsumenci powinni podjąć aby zabezpieczyć kupione urządzenia IoT.

**Cały raport jest dostępny tutaj:**

<http://www.watchguard.com/wgrd-resource-center/security-report>

**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](http://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.