Raport bezpieczeństwa internetowego Q3 2017: wzrost liczby ataków skryptowych

Kraków, dnia 22.02.2018 r. – Firma Bakotech, wyłączny dystrybutor rozwiązań firmy WatchGuard w Polsce, informuje, że WatchGuard opracował najnowszy Internet Security Report za trzeci kwartał 2017.

WatchGuard® Technologies, lider w dziedzinie zaawansowanych rozwiązań bezpieczeństwa sieciowego, opublikował wyniki swojego kwartalnego raportu bezpieczeństwa internetowego, w którym przedstawiono najnowsze zagrożenia bezpieczeństwa komputerowego i sieciowego mające wpływ na małe i średnie firmy (MSP) oraz przedsiębiorstwa rozproszone. Raport kładzie nacisk na gwałtowne ataki na skryptach połączone ze wzrostem ogólnej ilości złośliwego oprogramowania i pokazuje niesłabnący wzrost nowych technik ataków i złośliwego oprogramowania, podkreślając potrzebę warstwowej ochrony, zaawansowanego zapobiegania zagrożeniom i rygorystycznych zasad bezpieczeństwa.

Badanie ujawniło masowy wzrost liczby ataków skryptowych i ogólnych ataków szkodliwego oprogramowania dla średnich firm w trzecim kwartale 2017 r. Wyniki potwierdzają oczekiwania dotyczące dalszego wzrostu liczby nowych złośliwych programów i różnych technik ataków w nadchodzących miesiącach, dodatkowo podkreślając znaczenie warstwowych zabezpieczeń i zaawansowanych rozwiązań w zakresie zapobiegania zagrożeniom.

"Twórcy zagrożeń nieustannie dostosowują swoje techniki, zawsze szukając nowych sposobów wykorzystania luk w zabezpieczaniu cennych danych" - powiedział Corey Nachreiner, dyrektor ds. Technologii w WatchGuard Technologies. "W tym kwartale odkryliśmy, że ataki oparte na skryptach - takie jak odkryte we wrześniu fałszywe pakiety bibliotek Pythona - pojawiły się 20 razy częściej niż w drugim kwartale, podczas gdy liczba ogólnych ataków złośliwego oprogramowania wzrosła. Zachowanie czujności w związku z tymi wydarzeniami to połowa sukcesu. Każda firma może lepiej chronić siebie i osoby powiązane z firmą, stosując wiele poziomów ochrony, udostępniając zaawansowane usługi bezpieczeństwa i monitorowanie dzienników sieciowych w odniesieniu do ruchu związanego z najważniejszymi zagrożeniami wymienionymi w tym raporcie. "

Nieustannie zmieniający się krajobraz zagrożeń bezpieczeństwa może wydawać się przytłaczający dla przeciętnego małego biznesu przy ograniczonych zasobach i personelu. Raport Internet Security WatchGuard bada współczesny

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

krajobraz zagrożeń i dostarcza kluczowe dane, wskazówki edukacyjne i dogłębne badania, aby pomóc czytelnikom zrozumieć najnowsze trendy ataków i zaktualizować ich mechanizmy obronne.

Najważniejsze ustalenia z raportu za trzeci kwartał 2017 przedstawione zostały poniżej:

- **Zagrożenia związane ze skryptami stanowią 68% wszystkich złośliwych programów.** Rozwiązanie WatchGuard's Gateway AntiVirus (GAV) wykorzystuje sygnatury blokujące różne typy skryptów JavaScript i skryptów Visual Basic, takich jak downloadery. Suma wszystkich ataków opartych na skryptach stanowiła ogromną większość złośliwego oprogramowania wykrytego w trzecim kwartale.
- **Liczba złośliwych programów gwałtownie wzrosła; ten trend prawdopodobnie będzie kontynuowany.** Całkowita liczba szkodliwych programów wzrosła w tym kwartale o 81%. Z ponad 19 milionami wariantów zablokowanych w trzecim kwartale, próby ataków złośliwego oprogramowania prawdopodobnie wzrosną dramatycznie również w czwartym kwartale.
- **Ataki typu Cross-site Scripting (XSS) atakują przeglądarki internetowe i rozprzestrzeniają się na całym świecie.** Ataki XSS, które umożliwiają cyberprzestępcom wprowadzanie złośliwego skryptu na stronach ofiar, nadal rosną w wyznaczonym tempie. Poprzednie raporty szczegółowo opisują ataki XSS przeciwko samej Hiszpanii, ale w trzecim kwartale miały one duży wpływ na każdy kraj.
- **Oprogramowanie antywirusowe (AV) starego typu przeoczyło tylko 24% nowego złośliwego oprogramowania.** W ciągu ostatnich trzech kwartałów, antywirusy bazujące na sygnaturach, nie zauważyły wzrostu złośliwego oprogramowania aż do 47% w drugim kwartale. Ale w tym kwartale była wyraźna poprawa, a tylko 23,77% nowego malwaru lub typu zero-day mogło ominąć AV. Chociaż dane te są obiecujące, behawioralne rozwiązania do wykrywania są nadal najskuteczniejszym sposobem blokowania zaawansowanych, trwałych zagrożeń.
- **Podejrzane elementy iframe HTML pojawiają się wszędzie.** Atakujący nadal wymyślają sposoby, gdzie wykorzystują znacznik iframe HTML, by wymuszać na ofiarach wejścia na podejrzane i często złośliwe witryny. Potencjalnie złośliwe elementy iframe pojawiły się wszędzie, w tym w USA i Kanadzie, natomiast ich liczba znacznie wzrosła zarówno w Wielkiej Brytanii, jak i w Niemczech.
- **Uwierzytelnienie wciąż jest atrakcyjnym celem dla hakerów.** Chociaż nie tak powszechne jak w Q2, ataki ukierunkowane na uwierzytelnianie i poświadczenia (takie jak Mimikatz) powróciły w dużym stopniu w tym

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

kwartale. Oprócz Mimikatz, próby logowania w sieci typu brute force były również bardzo widoczne, co świadczy o tym, że hakerzy nadal atakują najsłabszy link - poświadczenia.

Raport Internet Security WatchGuard oparty jest na anonimowych danych Firebox Feed pochodzących z prawie 30 000 aktywnych urządzeń UTM WatchGuard na całym świecie, które blokowały ponad 19 milionów wariantów złośliwego oprogramowania i 1,6 miliona ataków sieciowych w trzecim kwartale. Kompletny raport zawiera strategie obronne reagowania na najnowsze trendy ataków, w oparciu o analizy najczęstszych zagrożeń złośliwego oprogramowania i sieci. Raport analizuje również rosnący trend ataków łańcucha dostaw, oceniając najbardziej znaczące przypadki z Q3 - NetSarang, Ccleaner i fałszywe pakiety Pythona.

Cały raport można znaleźć tutaj:

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

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.