Kwartalny raport bezpieczeństwa: dane do logowania na celowniku cyberprzestępców

Kraków, dnia 24.10.2017 r. – Firma Bakotech, wyłączny dystrybutor rozwiązań firmy WatchGuard w Polsce, informuje, że WatchGuard ogłosił wyniki swojego najnowszego Raportu Bezpieczeństwa dotyczącego zagrożeń w sieci.

Najnowszy raport o bezpieczeństwie internetowym firmy WatchGuard ujawnia, że 47% wszystkich szkodliwych programów jest oprogramowaniem nowym lub zero-day oraz zawiera kompleksową analizę WannaCry.

WatchGuard® Technologies, lider w dziedzinie zaawansowanych rozwiązań bezpieczeństwa sieciowego, ogłosił wyniki kwartalnego raportu o bezpieczeństwie internetowym, który analizuje najnowsze zagrożenia komputerowe i sieciowe dotyczące małych i średnich firm (SMB) oraz rozproszonych przedsiębiorstw. Ustalenia z Q2 2017 wykazały, że przestępczość wykorzystywana do uzyskiwania dostępu do danych do logowania użytkownika wzrasta, a rekordowa ilość – 47% całego złośliwego oprogramowania to zupełnie nowy kod i oprogramowanie typu zero-day. Systemy sygnaturowe są zupełnie nieskuteczne w walce z tego typu zagrożeniem.

"Dane zebrane z Fireboxów w Q2 pokazują, że autorzy zagrożeń koncentrują się bardziej na kradzieży danych do logowania niż kiedykolwiek wcześniej", powiedział Corey Nachreiner, szef technologii firmy WatchGuard Technologies. "Od ataków phishingowych z włączoną obsługą języka JavaScript oraz próbami kradzieży haseł systemu Linux, poprzez intensywne ataki na serwery WWW, wspólnym tematem jest to, że dostęp do logowania jest dla przestępców najważniejszy. Wiedząc o tym firmy muszą zabezpieczać narażone serwery, poważnie rozważyć wieloskładnikowe uwierzytelnianie, szkolić użytkowników w celu identyfikowania ataków phishingowych i wdrażać zaawansowane rozwiązania do zapobiegania zagrożeniom w celu ochrony cennych danych ".

Raport o bezpieczeństwie internetowym firmy WatchGuard dostarcza najlepszych praktyk w zakresie informacji o zagrożeniach, badaniach i bezpieczeństwie w celu informowania i edukowania czytelników o przeciwnikach online, aby mogli lepiej chronić siebie i swoje organizacje.

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

Najważniejsze wnioski z raportu z Q2 2017:

- **Mimikatz odpowiada za 36% topowego szkodliwego oprogramowania**
  Najpopularniejsze narzędzie typu open source wykorzystywane do kradzieży autentyczności Mimikatz po raz pierwszy w tym kwartale znalazł się na liście 10 najbardziej szkodliwych programów. Często używany do kradzieży danych do logowania systemu Windows, Mimikatz pojawił się z tak dużą częstotliwością, że uzyskał status najczęściej spotykanego złośliwego oprogramowania w drugim kwartale. Ten nowy dodatek do znanej grupy najczęstszych wariantów złośliwego oprogramowania wskazuje, że napastnicy stale zmieniają taktykę.
- **Ataki phishingowe zawierają złośliwy kod JavaScript w celu zmylenia użytkowników**
  Od kilku kwartałów napastnicy wykorzystują kod JavaScript, co odczuwają pobierający szkodliwe oprogramowanie w atakach webowych i poczty elektronicznej. W drugim kwartale atakujący wykorzystywali JavaScript w załącznikach HTML do wyłudzających wiadomości e-mail, które naśladują strony logowania podobne do popularnych, legalnych witryn, takich jak Google, Microsoft i innych po to, aby skłonić użytkowników do przekazania swoich poświadczeń.
- **Hasła Linuksa na celowniku w Europie Północnej**
  Cyberprzestępcy wykorzystywali starą lukę w aplikacjach systemu Linux, aby skierować do kilku krajów nordyckich i Holandii ataki przeznaczone do kradzieży haseł. Ponad 75% ataków, które wykorzystują lukę w dostępie do pliku / etc / passwd, dotyczy Norwegii (62,7%) i Finlandii (14,4%). Przy tak dużej liczbie przychodzących ataków, użytkownicy powinni aktualizować serwery i urządzenia Linuxa, jako podstawowe środki ostrożności.
- **Wzrost ataków typu Brute Force na serwery internetowe**
  Latem tego roku napastnicy wykorzystywali zautomatyzowane narzędzia przeciwko serwerom sieci web do złamania poświadczeń użytkowników. Wraz ze zwiększoną częstotliwością występowania ataków opartych na sieci WWW na poziomie uwierzytelniania w Q2, zagrożenia związane z logowaniem do serwerów internetowych znalazły się wśród 10 największych ataków sieciowych.
- **Prawie połowa całego szkodliwego oprogramowania jest w stanie ominąć dotychczasowe rozwiązania AV**
  W 47 procentach, coraz więcej nowego złośliwego oprogramowania lub zero-day sprawia, że dotychczasowe oprogramowanie antywirusowe traci na skuteczności. Dane pokazują, że oprogramowanie starego typu, oparte na sygnaturach AV, staje się coraz bardziej niewiarygodne, jeśli chodzi o wykrywanie zagrożeń nowego typu, co tylko potwierdza potrzebę stosowania rozwiązań działających na zasadzie behawioralnej.

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 o bezpieczeństwie internetowym firmy WatchGuard oparty jest na anonimowych danych pochodzących z Fireboxów z ponad 33,500 aktywnych urządzeń WatchGuard UTM na całym świecie. Ogółem, urządzenia te zablokowały w Q2 ponad 16 milionów wariantów złośliwego oprogramowania, przy czym odnotowano średnio 488 próbek zablokowanych przez każde urządzenie.

W ciągu kwartału rozwiązanie Gateway AV firmy WatchGuard zatrzymało prawie 11 milionów wariantów złośliwego oprogramowania (35% wzrost w porównaniu z Q1), podczas gdy APT Blocker wykrył dodatkowe 5,484,320 wariantów złośliwego oprogramowania (53% wzrost w porównaniu do pierwszego kwartału). Dodatkowo urządzenia WatchGuard Firebox zatrzymały prawie trzy miliony ataków sieciowych w drugim kwartale, z prędkością 86 ataków zablokowanych na urządzenie.

Pełny raport zawiera szczegółowy opis największych ataków złośliwego oprogramowania i ataków od drugiego kwartału 2017, obszerny opis znanych ataków WannaCry ransomware oraz kluczowych praktyk dotyczących bezpieczeństwa dla użytkowników poruszających się w sieci. W tym raporcie, najnowszy projekt badawczy pochodzący z Threat Lab WatchGuarda, koncentruje się na trendach zagrożeń z SSH i Telnet honeypots, które stale są ukierunkowane przez automatyczne ataki. Kluczowe w raporcie jest zwrócenie uwagi na niebezpieczeństwa pochodzące z kradzieży danych do logowania i waga ochrony typu IoT.

Cały raport jest możliwy do pobrania tutaj.

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.