FIRMA ODPORNA NA CYBERZAGROŻENIA – technologia GateScanner Content Disarm and Reconstruction (CDR)

Żyjemy w świecie coraz bardziej wyrafinowanych cyberzagrożeń. Ataki APT (ataki ukierunkowane), ransomware (oprogramowanie szantażujące) czy złośliwe oprogramowanie malware nieustannie „umykają" technologiom wykrywania. Zagrożeniem są też sami użytkownicy, a raczej brak świadomości zagrożeń albo zdrowego rozsądku. Uruchamianie nieznanego oprogramowania, pobieranie plików z nieznanych źródeł lub otwieranie niezweryfikowanych stron www może prowadzić do poważnych w skutkach incydentów naruszenia bezpieczeństwa IT.

Szkodliwe oprogramowanie malware – wróg organizacji nr 1

Stosowanie przez organizacje coraz bardziej zaawansowanych zabezpieczeń sprawia, że hakerzy coraz częściej atakują zaufane kanały organizacji – ponad 90% złośliwego oprogramowania malware pochodzi z wiadomości e-mail, przeglądania stron www, mobilnych nośników i przesyłania plików B2B. Zapobieganie cyberzagrożeniom może być skuteczne, ale wtedy każdy plik i wiadomość e-mail należy traktować jako podejrzane i potencjalnie niebezpieczne. I tak właśnie działa technologia GateScanner CDR firmy Sasa Software.

Innowacyjna technologia GateScanner Content Disarm and Reconstruction (CDR)

Technologia GateScanner CDR zapewnia bezpieczeństwo poprzez przekształcenie plików w bezpieczne, zneutralizowane i nieszkodliwe kopie, którym można zaufać. Zapobiega zaawansowanym, niewykrywalnym zagrożeniom i atakom z użyciem złośliwego oprogramowania, w tym APT i ransomware, przy zachowaniu pełnej użyteczności, widoczności i funkcjonalności plików.

Sposób działania GateScanner CDR

Krok 1. Dekonstrukcja

W pierwszym kroku GateScanner rozkłada wiadomości e-mail i pliki, przekształcając je na podstawowe elementy, aby wyszukać głęboko ukryte zagrożenia (np. oddzielenie poszczególnych plików w dokumentach zip czy plików osadzonych w innym pliku, rozłożenie wiadomości pocztowej zgodnie ze standardem RFC2822).

Krok 2. Wykrywanie zagrożeń

Po dekonstrukcji następuje proces automatycznego skanowania i wykrywania zagrożeń za pomocą wielu silników antywirusowych oraz technologii wykrywania nowej generacji (Artificial Intelligence, Machine Learning). Proces ten zapewnia, że znane złośliwe oprogramowanie pozostanie nieaktywne nawet przed rozpoczęciem procesu rozbrajania i rekonstrukcji. GateScanner integruje się również z zewnętrznymi rozwiązaniami bezpieczeństwa, takimi jak Sandbox czy Next-Gen AV.

Krok 3. Rozbrojenie i rekonstrukcja

Technika rozbrajania lub neutralizacji usuwa wszystkie potencjalnie złośliwe elementy, skrypty, makra, łącza, zachowując zaufane treści. Ostatnim elementem procesu jest rekonstrukcja, w której plik jest tworzony na nowo, a bezpieczna zawartość z pliku źródłowego jest przenoszona.

Lepiej skutecznie zapobiegać...

Gate Scanner nie tylko zapobiega niewykrywalnym zagrożeniom, np. Zero-Day, APT i ransomware, ale także zatrzymuje wszystkie zagrożenia w bezpiecznej strefie, ograniczając ryzyko związane również z zaniedbaniami pracowników. Z punktu widzenia bezpieczeństwa całej organizacji takie proaktywne podejście jest skuteczne, ponieważ wszystkie „zanieczyszczenia", które zazwyczaj zawierają potencjalnie szkodliwe treści, są wcześnie eliminowane. Rozwiązanie może być zastosowane w postaci kiosku, serwera aplikacyjnego, bramki pocztowej. Uzupełnieniem może być dioda danych (ang. Gate Scanner Injector) separująca sieci o różnych poziomach bezpieczeństwa, zapewniając jednokierunkowe przesyłanie danych.

Przyszłość to proaktywne cyberbezpieczeństwo

Najlepsze silniki CDR, takie jak GateScanner, dostarczają zestaw zaawansowanych technologii, które zapewniają równowagę pomiędzy bezpieczeństwem a użytecznością. Zapewniają, że pliki są bezpieczne, zachowując przy tym ich pełną funkcjonalność. Technologia GateScanner CDR gwarantuje ochronę i proaktywne podejście do wykrywania niebezpieczeństw – obecnie jest to najskuteczniejsze zabezpieczenie organizacji przed różnymi formami ataków i zagrożeń, nawet tych, których jeszcze nie znamy, a na pewno o nich i o szkodach, jakie wyrządziły, jeszcze usłyszymy. ■

Gate Scanner® Content Disarm and Reconstruction (CDR)