newss.pl
27 popularnych witryn zainfekowanych złośliwym kodem z serwera zarejestrowanego w Rosji!

Specjaliści firmy CORE dystrybutora oprogramowania antywirusowego AVG Technologies zdemaskowali infekcję 27 stron skryptem – Cross Site Scripting (persistent XSS). Jedną z ofiar infekcji padł popularny polski serwis finansowy.
„Wspólnie ze specjalistami AVG Technologies analizujemy wykryty przez nas przypadek zainfekowania popularnych witryn złośliwym kodem" – pisze na blogu technicznym AVG (http://techblog.avg.pl/) , Arkadiusz Zakrzewski specjalista pomocy technicznej AVG.pl

– „Na ten moment trudno podać więcej szczegółów z czym dokładnie mamy do czynienia i jakie zagrożenie oraz jakie dokładnie typy exploitów mogły zostać pobrane i zainstalowane. Wiemy na pewno, że infekcja polega na doklejeniu do każdego z pliku strony internetowej złośliwego kodu – skryptu, w tym przypadku szyfrowany JavaScript."

Do każdego z plików zaatakowanej polskiej witryny, w treść źródła strony został doklejony szkodliwy kod w postaci skryptu JavaScript. Działanie skryptu opiera się na wykonaniu przekierowania w tle do strony (adres zmodyfikowany) http://dirty****.ru:8##0/google.com/booking.com/huffingtonpost.com.p** po pomyślnym ustanowieniu połączenia z tą stroną wywoływany jest prosty skrypt php, który uruchamia pobieranie exploita do naszego systemu Windows.

Wykrycie infekcji.
Infekcja została w pierwszej kolejności wykryta przez jeden z modułów AVG – LinkScanner. Składnik dostępny zarówno w darmowej wersji AVG Free jak i we wszystkich wersjach komercyjnych.

Zadaniem składnika **LinkScanner** jest między innymi śledzenie ukrytych przekierowań z witryny i tą właśnie metodą składnik podniósł alarm wyłapując próbę przekierownia użytkownika na wspomniany wcześniej adres. Składnik LinkScanner czuwa w przeglądarkach Internet Explorer, FireFox oraz Opera.

W chwili obecnej witryna docelowa została zablokowana i nie jest dostępna w przeglądarce Mozilli. Czekamy na potwierdzenie z Opera Software o dodaniu wyjątku dla ich przeglądarki. Niestety użytkownicy Internet Explorera nie mogą zostać objęci wyjątkiem – IE takiej możliwości nie oferuje i pozostaje moduł **LinkScanner w AVG**.

Jak dodaje Arkadiusz Zakrzewski – „Wśród 27 zainfekowanych stron znalazły się takie witryny jak: silkroadmax.org, wepportal.com, watch-family-guy-episodes.org, mamy też jeden przypadek polskiego serwisu finansowego. Pragnę podkreślić, iż jesteśmy w stałym kontakcie i firma CORE służy pomocą przy usuwaniu infekcji."

Serwer, do którego kieruje przekierowanie,według raportu Bota Google zawiera 50 script exploitów, 40 trojanów, 24 exploity. Dogłębna analiza serwera jeśli nie zostanie całkowicie odcięty od sieci potrwa kilka dni . Sprawa z pewnością jest rozwojowa, dlatego więcej szczegółów z czym dokładnie mamy do czynienia i jakie zagrożenie oraz jakie dokładnie typy exploitów mogły zostać pobrane i zainstalowane będziemy informować na blogu technicznym AVG. Wstępnie możemy potwierdzić, że pierwsze z namierzonych exploitów są wykrywane przez AVG pod nazwą Known.Exploit.Type750
Rozwój sprawy można śledzić na blogu technicznym AVG http://techblog.avg.pl/ oraz zapoznać się z informacjami jak przed atakiem typu Cross Site Scripting zabezpieczyć serwer www.

Przedsiębiorstwo Informatyczne CORE