

Sam na sam z cyberprzestępcą

Nie jest tajemnicą, że większość ataków, na które jesteśmy narażeni, organizowana jest przez organizacje przestępcze. Celem jest zarabianie pieniędzy na podsłuchanych hasłach, wykorzystanie kontrolowanych komputerów do dystrybucji oprogramowania wyświetlającego reklamy czy niechcianych przesyłek pocztowych, a także np. szantaż. Wszystkie te działania obliczone są na określony zysk, i tak też działają przestępcy. Złośliwy kod przez nich zamawiany musi być maksymalnie skuteczny w krótkim okresie infekcji i możliwie niewykrywalny po niej. Jeden z ojców Internetu, Vint Cerf, postawił tezę, że jedna czwarta komputerów w Internecie funkcjonuje jako zombie, wykonując zdalne polecenia napastników lub ich zleceniodawców.

Skuteczny atak wymusza kreatywność w zakresie kanałów dystrybucji – jest to dziś najczęściej niewinnie wyglądająca strona WWW, komunikator internetowy czy P2P. Najnowszy sondaż CSI pokazuje powrót tzw. ataków targetowanych. Atak pomyślany jest więc jak kampania marketingowa. Atakujący wie, ile osób zatrudnia przedsiębiorstwo, jaki system antywirusowy używany jest na jego komputerach, stać go, żeby zapłacić kilka tysięcy złotych za stworzenie kodu niewykrywalnego dla tego oprogramowania. Co więcej, zadaje sobie trud, aby dowiedzieć się, z kim i na jaki temat komunikują się pracownicy, co pozwala zastawioną pułapkę uczynić bardziej wiarygodną. Kryterium skuteczności jest jasne – liczba zainfekowanych komputerów i wartość danych, które można z nich wyprowadzić.

W tej sytuacji niezmiernie istotna jest ochrona wielowarstwowa. Ta stara zasada budowania bezpiecznych systemów jest

jedną z najskuteczniejszych, jakie dotąd wymyślono. Im mniej punktów wspólnych mają poszczególne warstwy, tym lepiej. Wskazane jest między innymi, aby drugi system ochronny, najczęściej umieszczony w sieci, wytwarzany był przez innego producenta niż zabezpieczenia zainstalowane na komputerach.

Żaden system nie daje stuprocentowej ochrony, ale obowiązkiem administratora jest optymalizować ją w ramach dostępnego budżetu. Na co należy więc zwrócić uwagę? Z całą pewnością chronione powinny być te kanały, przez które wrogowie kod rozprzestrzenia się najczęściej – sieć Web i komunikatory internetowe. P2P jest mniej groźne, ponieważ polityka bezpieczeństwa większości firm nie dopuszcza jego stosowania – dobrze jest jednak mieć wypróbowany sposób blokowania tej komunikacji na poziomie sieci. Niezmiernie istotne jest, aby ochrona była jednakowo skuteczna w każdym oddziale firmy, nawet najmniejszym. W miarę rosnącej popularności telepracy Fortinet obserwuje rosnące zainteresowanie małymi urządzeniami, w które można zaopatrzyć domowe biuro pracownika. Urządzenie takie jest zamkniętym systemem, znacznie łatwiejszym w zdalnym kontrolowaniu czy zarządzaniu niż mobilny komputer, poza tym nie jest narażone na infekcję uszkadzającą oprogramowanie antywirusowe (jak na przykład populama ostatnio instalacja rootkitów, ukrywających obecność wrogiego kodu w systemie).

Fortinet jest producentem całej rodziny urządzeń zintegrowanego bezpieczeństwa (UTM), nazywanych FortiGate. Wszystkie one oferują identyczną funkcjonalność i interfejs zarządzania, wszystkie są

również wyposażone w dedykowany układ scalony przyspieszający pracę modułu antywirusowego. Jest to szczególnie istotne podczas ochrony ruchu Web, ze względu na wrażliwość na opóźnienia. Badania ergonomiczne pokazują, że statystyczny użytkownik czekający kilkanaście sekund na załadowanie strony WWW dojdzie do wniosku, że *Internet nie działa*. Oznacza to niepotrzebne telefony i czas stracony przez pracowników IT, a należy pamiętać, że ruch webowy to średnio 60% użycia łącza w przedsiębiorstwie.

Inną ciekawą cechą FortiGate jest możliwość ochrony przed niechcianą pocztą i potężna baza kategoryzująca ponad 40 mln stron webowych. Uaktualnienia odbywają się w czasie rzeczywistym i można je skonfigurować w ten sposób, aby to centrum dystrybucyjne samo informowało zainteresowane urzędnika o dostępności krytycznej informacji. W ten sposób wszystkie zainteresowane urzędnika dostają szczepionkę w ciągu 5 minut od jej publikacji przez dział R&D Fortineta.

System jest wyposażony w sprzętowe moduły centralnego zarządzania i raportowania, co predestynuje go do pracy tak w małych, jak i w dużych sieciach. W Polsce systemów Fortineta używa już ponad 3500 zadowolonych klientów, w tym PKP Energetyka i Małopolska Komenda Wojewódzka Policji.

Michał Kułakowski



Michał Kułakowski, inżynier w polskim oddziale Fortinet Inc. Z autorem można się skontaktować, pisząc na adres: michal.kulakowski@fortinet.com