



Usługa firmy RSA – FraudActionSM Anti-Trojan

Podstawowe informacje

- Proaktywna identyfikacja oprogramowania wyłudniającego dane (crimeware), którego działalność jest wymierzona w firmy i użytkowników pracujących w trybie online.
- Zrozumienie sposobu działania oprogramowania wyłudniającego, poprzez przeprowadzenie szczegółowej analizy punktów infekcji, serwerów sterujących oraz stref zrzutu (miejsc zbierania danych).
- Blokowanie dostępu do znanych punktów infekcji.
- Wyłączanie punktów infekcji i stref zrzutu gromadzących skradzione dane uwierzytelniające.

Badania potwierdziły, że w 2006 roku konie trojańskie stanowiły prawie połowę wszystkich nowych wariantów szkodliwego oprogramowania. Wraz z pojawianiem się zaawansowanych zagrożeń takich jak konie trojańskie, a w szczególności oprogramowanie wyłudające – organizacje muszą dokładać starań w celu ochrony kluczowych danych osobowych oraz użytkowników pracujących w trybie online. O ile ataki typu phishing mogą niszczyć i narażać na uszkodzenie kluczowe dane, są zwykle kierowane przeciwko konkretnemu celowi lub grupie celów, a ponadto wymagają od użytkownika wejścia na fałszywą stronę przygotowaną przez oszustów. Natomiast finansowe konie trojańskie zwane również programami wyłudzającymi infekują po cichu komputery podłączone do sieci w celu wykradania cennych danych z przeznaczeniem do ich dalszego wykorzystania, lub do przechwytywania zabezpieczonych sesji użytkowników, po czym dokonują działań przestępczych, gdy użytkownik jest już wylogowany z systemu.

Ponadto, finansowe konie trojańskie często pozostają nie wykryte przez kilka miesięcy, czego przykładem jest program o nazwie „Gozi”. Wobec tego, w jaki sposób firmy mogą chronić swych użytkowników przed atakami koni trojańskich?

Usługa FraudActionSM Anti-Trojan oferuje proaktywne, wszechstronne rozwiązanie, umożliwiające eliminowanie zagrożeń (konie trojańskie oraz programy wyłudzące) bezpośrednio u samych źródeł.

Usługa ta zajmuje się dwoma typami finansowych koni trojańskich:

Kradzież tożsamości: Program przeznaczony do wykradania danych uwierzytelniających, takich jak nazwy użytkowników lub hasła, które mogą być później używane do popełniania przestępstw.

Przelewanie funduszy: Program służący do automatycznego przelewania funduszy przy pomocy sesji przeglądarki klienta, po pomyślnym zalogowaniu.

Usługa FraudActionSM Anti-Trojan pomaga organizacjom w:

- identyfikowaniu oprogramowania wyłudniającego, którego działalność jest wymierzona w użytkowników;
- analizowaniu sposobu działania oprogramowania wyłudniającego;
- blokowaniu dostępu do znanych punktów infekcji, aby zminimalizować wpływ na użytkowników pracujących w trybie online;
- wyłączaniu punktów infekcji i stref zrzutu gromadzących skradzione dane uwierzytelniające.

Jak to działa?

Dzięki centrum zwalczania oszustw finansowych (Anti-Fraud Command Center – AFCC) działającemu w trybie 24x7 oraz globalnej sieci partnerów, firma RSA oferuje rozwiązanie warstwowe umożliwiające: identyfikowanie, analizowanie, blokowanie oraz wyłączanie oprogramowania wyłudniającego.

Identyfikacja i analiza

W wyniku połączenia danych zidentyfikowanych przez centrum AFCC oraz sieć dostawców programów antywirusowych, firma RSA jest w stanie zidentyfikować oprogramowanie wyłudzące, działające przeciwko danej firmie lub jej klientom, a także przeprowadzić wszechstronną analizę sposobu działania tego typu oprogramowania.

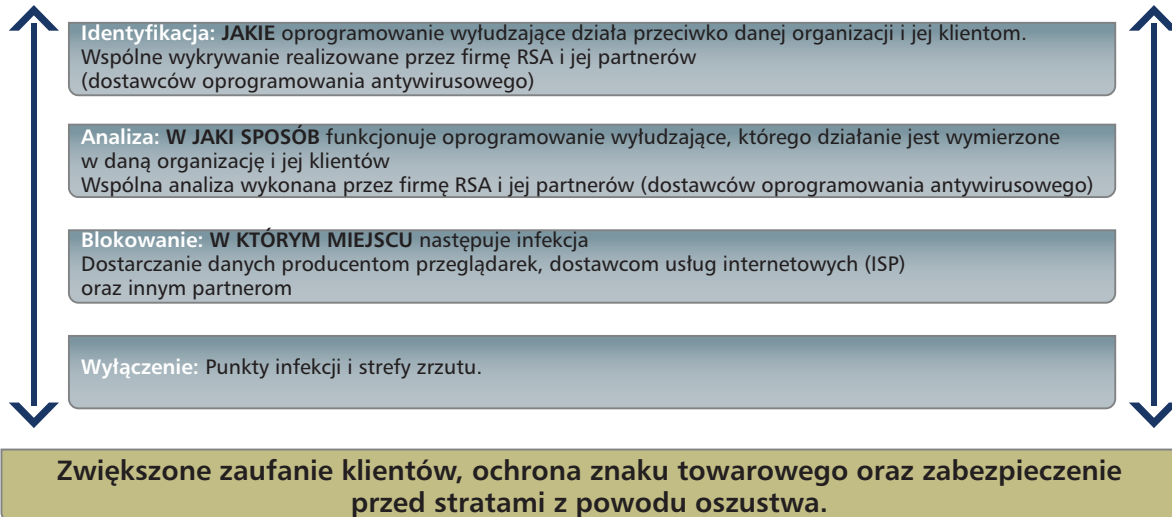
Dzięki zrozumieniu sposobu infekowania komputerów przez oprogramowanie wyłudzące, metod sterowania tym oprogramowaniem oraz zidentyfikowaniu stref zrzutu gromadzących skradzione dane uwierzytelniające, można podjąć działania mające na celu zmniejszenie tego zagrożenia.



The Security Division of EMC



RSA FraudActionSM Anti-Trojan



Usługa FraudAction SM Anti-Trojan oferuje kompleksową metodę zwalczania zagrożeń powodowanych przez oprogramowanie wyłudzające.

Blokowanie i wyłączenie

Po zidentyfikowaniu fałszywej strony oraz potwierdzeniu, że rozsyła ona oprogramowanie wyłudzające, centrum AFCC pracujące w trybie 24x7 – poprzez globalną sieć partnerów liczącą już prawie 4.000 dostawców usług internetowych (ISP), urzędników, producentów przeglądarek oraz firm specjalizujących się w przesyłaniu danych – blokuje i wyłącza punkty infekcji rozsyłające konie trojańskie, a także wyłącza znane strefy zrzutu do których przesyłane są skradzione dane uwierzytelniające. Oprócz tego, centrum AFCC oferuje pomoc techniczną w ponad 150 językach, aby zapewnić szybsze wyłączenie punktów infekcji i stref zrzutu.



The Security Division of EMC

© 2007 r. RSA Security Inc. Wszystkie prawa zastrzeżone.
Nazwy: RSA, RSA Security, FraudAction oraz logo RSA, są znakami towarowymi lub zarejestrowanymi znakami towarowymi firmy RSA Security Inc. w USA i/lub innych krajach. EMC jest zarejestrowanym znakiem towarowym firmy EMC Corporation. Wszystkie pozostałe produkty i usługi wymienione w niniejszym dokumencie, są znakami towarowymi poszczególnych firm.