



The Security Division of EMC

Przegląd rozwiązania firmy RSA

RSA FraudActionSM

usługa Anti-Trojan

Usługi realizowane w trybie online nigdy nie doświadczały tak częstych ataków ze strony wyrafinowanych, innowacyjnych i zintegrowanych w skali globalnej sieci przestępczych, jak obecnie. Pomimo świadomości użytkowników odnośnie coraz większej liczby ataków typu phishing, w każdym miesiącu organizacje (niezależnie od typu i wielkości) narażone są na dziesiątki tysięcy groźnych ataków. Ponadto, rozprzestrzenianie się oprogramowania wyłudniającego dane (crimeware) zwiększyło problemy firm dotyczące ochrony klientów, znaków towarowych i aktywów oraz zapewnienia integralności usług online.

W 2006 roku programy wyłudające stanowiły prawie połowę wszystkich nowych wariantów szkodliwego oprogramowania, przy czym ich liczba stale rośnie. Analiza przygotowana przez laboratorium firmy RSA (Trojan & Phishing Lab) wykazała, że pojedynczy wariant konia trojańskiego „Gozi / Bank-Sniff” zainfekował w okresie jednego miesiąca ponad 30.000 komputerów. Biorąc po uwagę coraz większą ilość treści udostępnianych w sieci – np. serwisach społecznościowych – zagrożenie szkodliwym oprogramowaniem staje się poważnym problemem.

FraudActionSM jest sprawdzoną, kompleksową usługą przeznaczoną do eliminowania zagrożeń związanych z oprogramowaniem szpiegowskim oraz atakami typu phishing / pharming – umożliwiającą skuteczne zwalczanie zagrożeń teraz i w przyszłości. Dzięki innowacyjności i bezkompromisowości firmy RSA, klienci są zawsze o krok do przodu w stosunku do nowych ataków.

Obecnie, z usługi FraudAction korzysta ponad 200 wiodących organizacji, w tym Barclays, Washington Mutual, ING Direct i E*Trade, a także wiele banków regionalnych i unii kredytowych (np. PESCU, CFEFCU i innych). Usługa FraudAction jest oferowana jako modułowa usługa zarządzana, którą można szybko wdrożyć, przy minimalnym wpływie na zasoby wewnętrzne. Usługa ta jest dostępna w wielu opcjach cenowych, dostosowanych do różnych potrzeb i wymagań poszczególnych organizacji.

Sprawdzone rozwiązanie – korzystanie z centrum zwalczania oszustw finansowych

Usługa FraudAction potwierdziła swą skuteczność pod względem minimalizowania ryzyka i błyskawicznego dostarczania wyników. Działające w firmie RSA centrum zwalczania oszustw finansowych (AFCC), pomogło w skróceniu okresu istnienia typowych stron służących do wykonywania ataków phishing – z 110 godzin do średnio około 5 godzin. Centrum

współpracuje z prawie 4.500 firmami hostingowymi i eliminuje nawet najbardziej skomplikowane ataki na całym świecie. Według opinii klientów, w następstwie zastosowania rozwiązań firmy RSA, udało się wykryć 95 - 99% ataków typu phishing.

Centrum AFCC zlikwidowało już ponad 40.000 unikatowych ataków phishing w ponad 135 krajach. Firma RSA zidentyfikowała nowe i powstające tendencje dotyczące oszustw, poinformowała o nich klientów, a także opracowała rozwiązania umożliwiające wyeliminowanie zagrożeń – a to wszystko w krótkim czasie. W wyniku rozszerzenia usług na skalę globalną, utworzenia potężnej sieci partnerów i wprowadzenia najnowocześniejszych technologii, rozwiązania firmy RSA zajęły pierwsze miejsce w testach, pod względem: wykrywalności, czasu wyłączenia i całkowitej ochrony przed oszustwami.

Obecnie, firma RSA włączyła oprogramowanie wyłudające do zakresu działania centrum AFCC. Jest to możliwe dzięki rozbudowaniu sieci wykrywającej, która pozwala na szybkie identyfikowanie, analizowanie i eliminowanie oprogramowania wyłudającego, którego działania są wymierzone w firmy i ich klientów.

Ponadczasowa usługa zarządzana

FraudAction jest usługą zarządzaną, wykonywaną na zewnątrz organizacji, pozwalającą na zminimalizowanie kosztów inwestycji oraz szybkie wdrożenie. Działająca w ramach firmy RSA organizacja Online Threats Managed Services, zapewnia stałą ochronę w obliczu ewoluujących oszustw sieciowych oraz nowych rodzajów ataków – oferując klientom usługi FraudAction najbardziej aktualne informacje. Firma RSA nadal pozostaje wiodącym dostawcą zaawansowanych rozwiązań, umożliwiających ochronę klientów przed najnowszymi zagrożeniami. Działalność firmy RSA obejmuje między innymi partnerską sieć blokującą oraz usługi pozwalające na identyfikację, analizę i eliminowanie programów typu koń trojański.

Główne korzyści – usługa FraudAction Anti-Trojan

Usługa FraudAction oferuje kilka zasadniczych korzyści, obejmujących:

Elastyczne opcje cenowe

Firma RSA zapewnia elastyczną strukturę cen, dzięki czemu organizacje mogą wybrać plan cenowy, który najlepiej pasuje do konkretnych potrzeb biznesowych.

Ochronę przed oprogramowaniem wyłudającym dane (crimeware), realizowaną na zewnątrz organizacji

Ochrona przed atakami programów wyłudających jest procesem czasochłonnym, zużywającym dużo zasobów. Co więcej, do tej pory nikt nie zajmował się tym zagadnieniem w sposób kompleksowy. Działające w firmie RSA centrum AFCC (w trybie 24x7), posiada wszechstronne doświadczenie i korzysta z ekonomii skali. Dzięki temu, klienci nie muszą już martwić się programami wyłudającymi dane, ani innymi atakami sieciowymi.

Implementację ponadczasowej ochrony klientów

Firma RSA oferuje jeden z najwszechstronniejszych na rynku pakietów rozwiązań służących do uwierzytelniania użytkowników i zwalczania oszustw, obejmujący: oparte na ryzyku uwierzytelnianie kanałów sieciowych i telefonicznych, usługi zwalczające oszustwa oraz monitorowanie transakcji w czasie rzeczywistym (bankowość elektroniczna i handel elektroniczny). Firma RSA skutecznie pomaga organizacjom w ochronie kanałów sieciowych, zwiększaniu zaufania klientów oraz minimalizowaniu całkowitego ryzyka. Zespół analityków ds. oszustw stale poszukuje sposobów aktualizacji produktów klientów, w celu ochrony kanałów sieciowych przed najnowszymi zagrożeniami.

Główne właściwości usługi FraudAction:

- identyfikacja i generowanie alarmów realizowane prawie w czasie rzeczywistym;

- szczegółowa analiza: punktów infekcji, stref zrzutu, sterowania, itd.;
- ocena poziomu istotności;
- narzędzie Dashboard;
- sieć blokująca FraudAction;
- celowane wyłączenie punktów infekcji i stref zrzutu;
- środki zaradcze – przynęty;
- działania z zakresu informatyki śledczej;
- wydzielanie danych i zdobywanie materiałów dowodowych.

Poniżej przedstawiono skrócony opis właściwości usługi FraudAction Anti-Trojan:

Identyfikacja

W przypadku wykrywania programów wyłudających, występują dwa główne problemy: brak rozpowszechnienia i brak zauważalnych skutków. Finansowe konie trojańskie nie są zwykle rozpowszechnione w tak dużym stopniu, jak inne rodzaje oprogramowania szkodliwego (np. robaki lub zwykłe programy szpiegowskie). Ponadto, finansowe konie trojańskie działają w wyjątkowo „cichy” sposób, dlatego prawdopodobieństwo zgłoszenia przez klientów obecności takich programów jest znacznie mniejsze.

Często zdarza się, że programy antywirusowe nie są w stanie wykryć finansowych koni trojańskich przez wiele miesięcy (np. przypadek konia trojańskiego „Gozi”). Aby uzyskać jak najwyższy poziom wykrywalności, usługa FraudAction Anti-Trojan korzysta z sieci partnerów, która zapewnia znacznie lepsze wyniki w porównaniu z pojedynczym rozwiązaniem. Aby objąć jak największą ilość zagrożeń związanych z oprogramowaniem szpiegowskim, usługa FraudAction korzysta z pomocy partnerów zlokalizowanych w różnych sektorach technologicznych, obejmujących:

1. Dostawców programów antywirusowych. Partnerzy ci wdrażają oprogramowanie antywirusowe w komputerach domowych. Korzystają zarówno z możliwości wykrywających tych programów, jak i fragmentów programów szkodliwych uważanych za „podejrzane”, umożliwiając wykrywanie oprogramowania szkodliwego w stanie naturalnym (in the wild), podczas ataku.

2. Operacje wywiadowcze. Partnerzy ci wykrywają zagrożenia związane z oprogramowaniem szpiegowskim przy pomocy sieci przynęt (honey-pot) takich jak adresy poczty elektronicznej (e-mail), poprzez przeglądanie szkodliwych stron internetowych i forów społecznościowych.
3. Bramki internetowe. Partnerzy ci działają w głównych koncentratorach (hub) obsługujących pocztę elektroniczną. Dzięki temu można od razu wykrywać programy wyludzające, poprzez skanowanie każdego dnia wielu miliardów wiadomości e-mail.

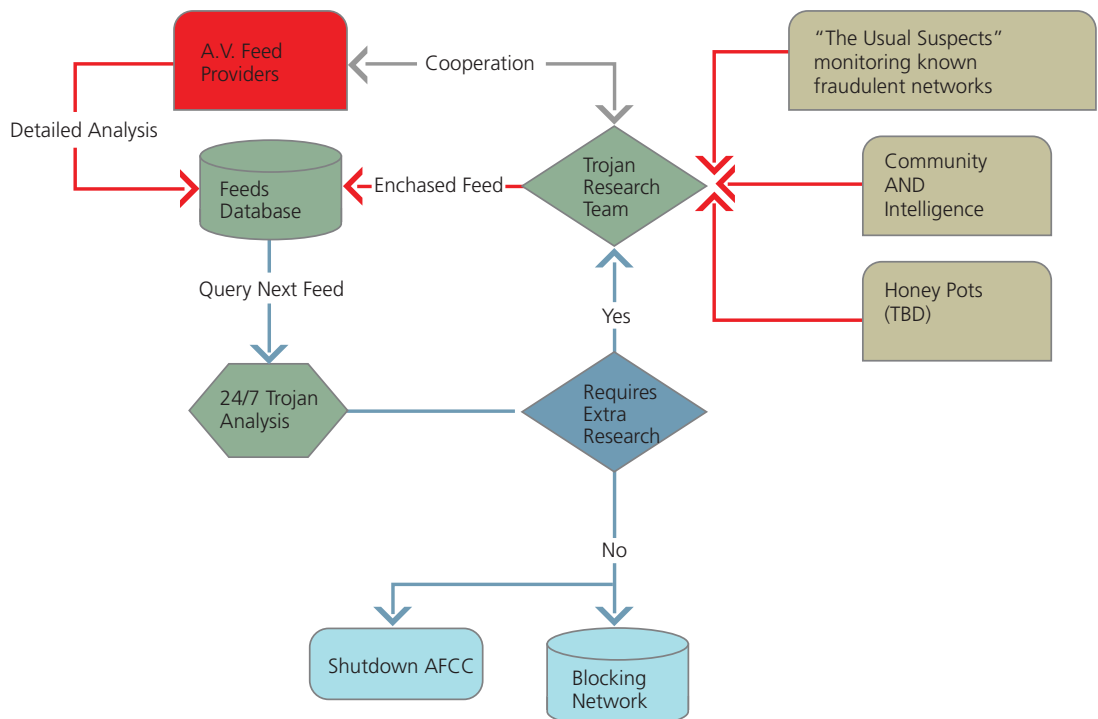
W przypadku wykrycia przez firmę finansowego konia trojańskiego, kod binarny programu oraz jego analiza są przesyłane do działającego w trybie 24-x7 centrum AFCC w firmie RSA. Następnie, koń trojański jest przetwarzany przez automatyczny mechanizm klasyfikująco-analityczny (Unified Feed), który potwierdza czy koń trojański zamierza zaatakować jednego z klientów firmy RSA, po czym próbuje dopasować konia trojańskiego do jednej ze znanych rodzin tego typu programów. Powyższe dane są

przesyłane do analityka specjalizującego się w informatyce śledczej, który określa kanały łączności konia trojańskiego oraz wpływ programu na działalność firmy. Analityk przygotowuje raport na temat konia trojańskiego i przesyła właściwej instytucji finansowej, która miała być celem ataku. Następnie, analityk operacyjny upoważniony do wyłączania stron, przesyła raport wraz z nakazem zaprzestania działalności do stosownego dostawcy usług internetowych (ISP).

Eliminowanie zagrożeń

Usługa FraudAction eliminuje dwa rodzaje działań wykonywanych przez finansowe konie trojańskie:

1. Kradzież tożsamości. Program szpiegowski kradnie dane uwierzytelniające, takie jak nazwy użytkowników lub hasła, które później będą stosowane do popełniania przestępstw.
2. Przelewanie funduszy. Program szpiegowski automatycznie przelewa fundusze przy pomocy sesji przeglądarki klienta, po pomyślnym zalogowaniu.



Zapobieganie rozpowszechnianiu się oprogramowania wyłudającego wykradające dane uwierzytelniające użytkownika (jego tożsamość) jest realizowane poprzez blokowanie i wyłączenie punktów infekcji (stron sieciowych odwiedzanych przez klientów i powodujących infekcję) oraz wszystkich związanych z nimi kanałów sterowania (tj. miejsc w Internecie aktualizujących konie trojańskie i gromadzących skradzione dane uwierzytelniające).

Zapobieganie rozpowszechnianiu się programów szpiegowskich stosowanych do przelewania funduszy może być bardziej skomplikowane. Centrum AFCC monitoruje konta docelowe, na które programy szpiegowskie przelewają fundusze (tzw. kanały), a także dostarcza instytucjom finansowym aktualne informacje. Poprzez śledzenie kont, z których fundusze są przelewane na konta oszustów, instytucje finansowe mogą precyzyjnie określać, które rachunki padły ofiarą oszustów i oceniać całkowite skutki ataku. Centrum AFCC infekuje własne komputery koniami trojańskimi, aby uzyskiwać najnowsze informacje dotyczące zmian w działaniu tych programów.

Ocena poziomu istotności

Ocena poziomu istotności oferowana przez usługę FraudAction dostarcza cenne i aktualne informacje zespołowi zarządzającemu instytucji finansowej. Powyższe informacje wspomagają proces podejmowania decyzji, ułatwiając wybór właściwych środków, które należy zastosować. Zespół firmy RSA współpracuje ściśle z instytucjami finansowymi odnośnie wszystkich aspektów ataków oprogramowania wyłudającego oraz potencjalnego wpływu ataków na systemy instytucji finansowych, właścicieli kont i wizerunek korporacji.

Przy pomocy określonych wcześniej danych statystycznych, modeli i narzędzi centrum AFCC dokonuje wstępnej oceny ataku, tj. ustala wielkość ataku i uzyskuje dodatkowe informacje, np. dane właściciela konta, które mogło ucierpieć w wyniku ataku. Raport wstępny (stanowiący część informacji alarmowych), jest przesyłany do instytucji finansowej wkrótce po wystąpieniu ataku. Raport ten jest okresowo aktualizowany podczas ataku.

Ocena jest stale aktualizowana, w miarę otrzymania nowych informacji, wyników dodatkowych analiz oraz po zmianie stanu bieżącego. W uzasad-

nionych przypadkach ocena jest przesyłana do instytucji finansowej przy pomocy bezpiecznej aplikacji o ograniczonym dostępie, aktualizowanej regularnie przez zespół AFCC. Aktualizacje informacji dotyczących: wielkości ataku, stanu i oceny ryzyka, są przesyłane dopóki atak jest aktywny.

Narzędzie Dashboard

Rozwiązanie FraudAction oferuje klientom raport na temat ataku, a także zapewnia dostęp do raportów szczegółowych za pomocą aplikacji Dashboard, działającej w trybie online. Raport ogólny zawiera wszystkie znane ataki oraz informacje krytyczne, przedstawione w czytelny sposób. Dzięki narzędziu Dashboard, upoważnieni pracownicy instytucji finansowej mogą uzyskać bezpieczny dostęp do raportu i zapoznawać się – w czasie rzeczywistym – z bieżącą sytuacją dotyczącą wszystkich ataków.

Aplikacja Dashboard przedstawia również m.in. dane statystyczne i trendy dotyczące oprogramowania wyłudającego oraz najczęściej zadawane pytania (FAQ) odnośnie sposobu uzyskiwania dalszych informacji na temat programów wyłudających i terminologii związanej z tym zagadnieniem. W przypadku każdego ataku, raport oferuje następujące dane:

- identyfikator ataku;
- czas wykrycia ataku;
- punkty infekcji i strefy zrzutu;
- dostawcę usług internetowych (ISP);
- podjęte środki zaradcze.

Sieć blokująca FraudAction – blokowanie dostępu do znanych punktów infekcji

Sieć blokująca FraudAction składa się z wiodących przedstawicieli:

- dostawców usług internetowych (ISP);
- dostawców oprogramowania antywirusowego;
- dostawców programów służących do zwalczania spamu;
- dostawców pasków narzędziowych.

Firma RSA współpracuje z największymi dostawcami usług internetowych (ISP) i przeglądarek, w tym:

Microsoft®, AOL®, Google / Mozilla, Earthlink® oraz wieloma innymi. Na podstawie informacji dostarczanych przez RSA, partnerzy blokują dziesiątkom milionów swoich użytkowników, z których wielu ma konta u klientów usługi FraudAction, dostęp do stron wykorzystywanych przez oszustów. Innymi słowy, wielu właścicieli kont znajdujących się w instytucjach finansowych korzystających z usługi FraudAction, będzie chronionych przed potencjalną infekcją oprogramowania wyłudniającego. Jest to usługa z wartością dodaną, oferowana klientom FraudAction bez dodatkowych opłat.

Wyłączanie stron

Im szybciej likwidowane są skutki działania programów szpiegowskich, tym mniej szkód mogą one spowodować - jednakże wyłączanie punktów infekcji i stref zrzutu jest zagadnieniem bardziej skomplikowanym, niż mogłoby się wydawać. Należy uwzględnić różne zagadnienia, np. godziny pracy i święta państwowe w poszczególnych krajach oraz bariery językowe. Dzięki współpracy z dostawcami usług internetowych (ISP), firmami hostingowymi i właścicielami zarażonych komputerów, zespół AFCC może powstrzymać ataki w imieniu instytucji finansowych, poprzez wyłączanie stron oszustów. Do tej pory zespół AFCC wyłączył ponad 32.000 stron na całym świecie.

W uzasadnionych przypadkach zespół AFCC przesyła wnioski o zaprzestanie działalności, opracowywane w ponad 15 językach, między innymi: arabskim, holenderskim, niemieckim, japońskim, rosyjskim, chińskim, angielskim, węgierskim, koreańskim, hiszpańskim, czeskim, francuskim, włoskim, rumuńskim i szwedzkim. Zespół oferuje również usługi tłumaczeniowe w ponad 150 językach, realizowane w czasie rzeczywistym.

Wspomniane powyżej rozległe możliwości językowe umożliwiają szybkie wyłączanie stron, niezależnie od lokalizacji źródła ataku.

Dzięki współpracy z czołowymi instytucjami finansowymi na całym świecie oraz monitorowaniu wielu ataków, firma RSA jest w stanie nawiązać relacje z największymi dostawcami usług internetowych (ISP). Stały kontakt zespołu AFCC z dostawcami usług internetowych oraz stosowanie procedury na-

kazu zaprzestania działalności, przyspiesza proces wyłączania stron, i co za tym idzie, redukuje całkowite skutki ataku.

Działania z zakresu informatyki śledczej – wydzielanie danych i zdobywanie materiałów dowodowych

Po wystąpieniu ataku oraz po jego zakończeniu, w celu zdobycia dodatkowych, cennych informacji, zespół AFCC przeprowadza wszechstronne badania z zakresu informatyki śledczej. W niektórych przypadkach zespół AFCC jest w stanie uzyskać aktualną listę skradzionych informacji osobowych oraz konta, na które informacje te zostały przesłane; a także szczegóły dotyczące adresu IP, dane binarne programu szpiegowskiego, itd.

Badania z zakresu informatyki śledczej odbywają się równolegle z innymi czynnościami. Jeżeli zespół AFCC jest w stanie uzyskać skradzione dane, instytucja finansowa może natychmiast podjąć stosowne działania, tj. zawiesić zaatakowane konta i skontaktować się z klientami, którzy ucierpieli w wyniku ataku. Są to bezcenne informacje, które umożliwiają instytucji finansowej zmniejszenie szkód spowodowanych przez programy wyłudzące, a w konsekwencji – uzyskanie wiarygodności jako organizacji, która proaktywnie chroni klientów przed atakami.

Wszystkie skradzione informacje mogą być również bardzo ważne w przypadku współpracy z wymiarem sprawiedliwości. Z powodu braku zasobów, niektóre agencje wymiaru sprawiedliwości mogą nie przyjmować spraw bez dostarczenia dowodu, że dany przypadek jest na tyle znaczący, że stanowi potencjalne zagrożenie dla dużej ilości ofiar.

W wielu przypadkach, te same techniki szpiegowskie są stosowane do wykonywania ataków na wiele instytucji finansowych, przy czym większa ilość ataków może być przeprowadzana przez tę samą grupę oszustów. W takiej sytuacji, po zidentyfikowaniu luki dotyczącej danego klienta oraz przeanalizowaniu jej przez zespół AFCC, uzyskane informacje mają zastosowanie do wielu innych ataków wykonywanych przeciwko innym klientom – co tworzy efekt sieci wykorzystywany przez usługę FraudAction do zdobywania wiedzy dotyczącej ataków wykonywa-

nych na kilka różnych instytucji finansowych jednocześnie.

Oprócz działań z zakresu informatyki śledczej mających na celu zdobycie danych, firma RSA oferuje również informacje dodatkowe, które można wykorzystać w procesie dowodowym i postępowaniach sądowych. Informacje te powstają na podstawie analizy wszystkich ataków. Zespół AFCC zawsze stara się przesyłać jak najwięcej szczegółowych i obszernych informacji dotyczących oceny poziomu istotności oraz uzyskanych danych.

Informacje są gromadzone zawsze w sposób zgodny z prawem i przechowywane przy pomocy zestawu narzędzi odpowiadających za spójność i rzetelność danych, które mogą być później wykorzystywane przez instytucje finansowe.

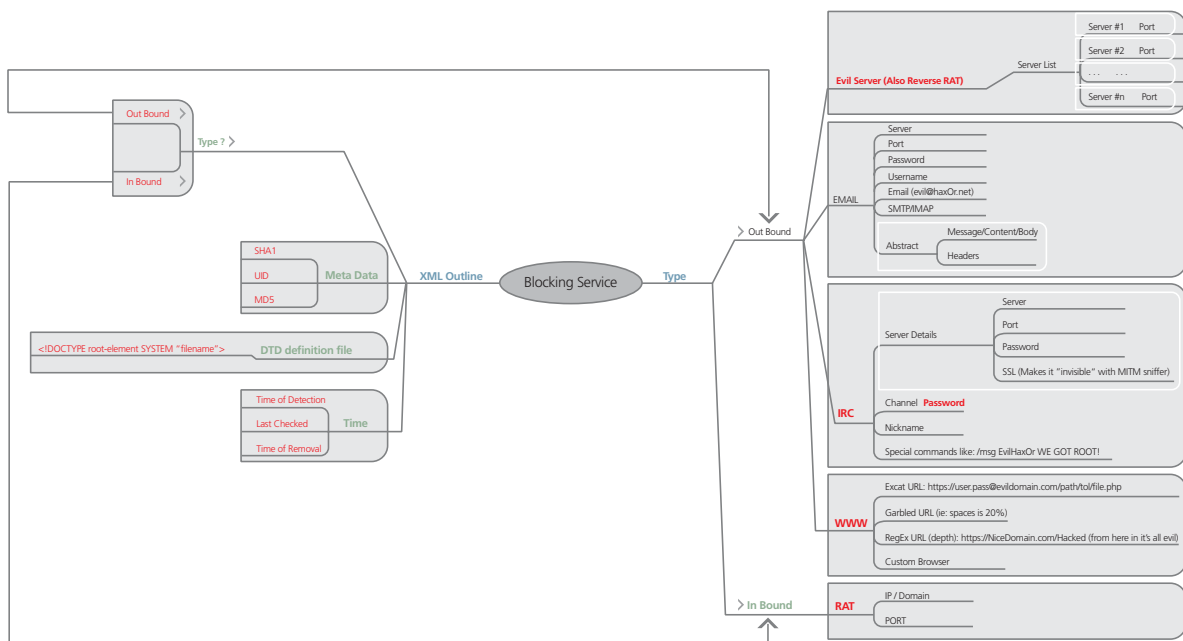
Środki zaradcze

Firma RSA opracowała własne środki zaradcze, które po raz pierwszy umożliwiają instytucjom finansowym działanie w sposób proaktywny przeciwko oszustwom dokonywanym za pomocą poczty elektronicznej (e-mail). Firma opracowała technologie, które oczekują obecnie na nadanie patentu, a które umożliwiają:

- minimalizowanie zagrożeń zawartych w wiadomościach e-mail, wymierzonych przeciwko instytucjom finansowym;
- zredukowanie strat spowodowanych atakami; zwiększenie szans na schwytanie oszustów;
- powstrzymanie oszustów przed przeprowadzaniem dalszych ataków.

Ponadto, aktualnie firma RSA bada kilka metod bezpośredniego atakowania oszustów. Z uwagi na fakt, że oszuści stają się coraz bardziej wyrafinowani, działający w zespole AFCC eksperci ds. bezpieczeństwa i oszustw, ciągle starają się przewidywać następne generacje ataków oraz oszustw przeprowadzanych za pomocą poczty elektronicznej, a także przygotowywać skuteczne środki zaradcze.

Firma RSA opracowała rozwiązanie Randomized Credentials Technology™ (RCT), umożliwiające tworzenie fikcyjnych kont zachowujących się w taki sposób, jakby należały do prawdziwych użytkowników. Konta te są „wystawiane” stronom oszustów nie pozostając wykrytymi. Mechanizm RCT można stosować na wiele sposobów, aby zredukować skutki ataków, ograniczyć straty oraz zmniejszyć ilość użytkowników narażonych na ataki. Firma RSA stosuje tę metodę głównie jako część środków zaradczych rozwiązania FraudAction.



Przynęty

Zadaniem przynęt jest w celu śledzenia działań przestępczych i zwiększenia szans na schwytanie oszustów opracowano odpowiednie formy przynęt. Przy pomocy oczekującej na opatentowanie technologii RCT, dostarczane są aplikacje szpiegowskiej fikcyjne odpowiedzi, które można śledzić i w ten sposób wykryć działalność przestępcza w sieci.

Aby sprowokować konia trojańskiego do działania i wymusić użycie fikcyjnych danych uwierzytelniających, zespół AFCC tworzy dla każdego klienta „skażoną” konfigurację DNS. W przeciwieństwie do ataków typu pharming, taka konfiguracja dostarcza koniowi trojańskiemu odniesienie do fałszywej strony bankowej istniejącej w komputerach zespołu AFCC, która udaje prawdziwą stronę instytucji finansowej. Strona zezwala na zalogowanie się przy pomocy fałszywych danych uwierzytelniających, które są uznane przez konia trojańskiego za prawidłowe. W wyniku tego, koń trojański przesyła te dane do punktu zbierającego informacje.

Liczba rozsyłanych kont-przynęt zależy od szacowanej wielkości ataku. Przynęty służą do „oznaczania” oszustów, którzy próbują wykorzystać zgromadzone dane przeciwko instytucji finansowej. Firma RSA dostarcza plik zawierający wszystkie informacje zastosowane w przynętach, co umożliwia instytucjom finansowym poprawienie swoich systemów wewnętrznych, wykrycie faktu użycia informacji oraz śledzenie działań oszustów. Na przykład, jeżeli informacje użyte podczas ataku są danymi uwierzytelniającymi stosowanymi w bankowości elektronicznej, dzięki śledzeniu przynęt instytucja finansowa może zidentyfikować próby uzyskania dostępu do usług bankowości elektronicznej.

Po zidentyfikowaniu takich prób, instytucja finansowa może zablokować źródło, np. adres IP, z którego próbowano uzyskać dostęp do fałszywych informacji (przynęty). Jeżeli oszust próbuje uzyskać dostęp do prawdziwych kont z tego samego adresu IP, wszystkie próby zostaną zablokowane. Dzięki oznaczeniu źródła ataku, instytucje finansowe mogą pomóc wymiarowi sprawiedliwości w zlokalizowaniu oszustów, którzy próbowali przeprowadzić atak.

RSA eFraudNetwork – nie walczy z oszustwami samotnie

Poprzez subskrypcję usługi FraudAction, nasi klienci mogą korzystać ze wspólnej wiedzy znajdującej się w największej społeczności zapobiegającej oszustwom – eFraudNetwork™. Jest to sieć utworzona przez firmę RSA w celu udostępniania i rozpowszechniania informacji na temat działań przestępczych. Społeczność eFraudNetwork umożliwia międzyorganizacyjne udostępnianie informacji w czasie rzeczywistym (w trybie 24x7), a także śledzenie oszustw w ponad 135 krajach. Jeżeli jeden z członków społeczności został zaatakowany, wszyscy pozostali członkowie społeczności są o tym natychmiast informowani, po czym uruchamiane są stosowne zabezpieczenia. Klienci usługi FraudAction od razu stają się częścią społeczności eFraudNetwork i mogą korzystać z rozwiązania oferowanego całej branży.

Firma RSA jest partnerem godnym zaufania

RSA, oddział firmy EMC zajmujący się bezpieczeństwem, specjalizuje się w ochronie informacji w całym cyklu ich istnienia. Firma oferuje klientom rozwiązania pozwalające na opłacalne zabezpieczanie informacji krytycznych oraz tożsamości wykorzystywanych w transakcjach internetowych, na każdym etapie i niezależnie od lokalizacji, a także zarządzanie informacjami i zdarzeniami dotyczącymi bezpieczeństwa, aby redukować problemy dotyczące zgodności z przepisami.

Firma RSA oferuje najlepsze na rynku rozwiązania w dziedzinie ochrony tożsamości i kontroli dostępu, szyfrowania i zarządzania kluczami, zarządzania informacjami dotyczącymi zgodności i bezpieczeństwa, a także ochrony przed oszustwami. Rozwiązania te zapewniają ochronę tożsamości milionów użytkowników, wykonywanych przez nich transakcji oraz generowanych danych. Więcej informacji na ten temat można znaleźć na stronach: www.RSA.com oraz www.EMC.com.



The Security Division of EMC

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

© 2007 r. RSA Security Inc. Wszystkie prawa zastrzeżone. Nazwy: RSA, RSA Security, FraudAction, eFraudNetwork 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.