Internet: coraz więcej agresji

Informatycy biją na alarm: usługi finansowe są coraz częstszym celem działań napastników nastawionych na osiągnięcie nielegalnego zysku. Próbują oni uzyskać dostęp do danych osobowych lub finansowych, takich jak np. bankowe lub numery kart kredytowych. Niekiedy usiłują po prostu zakłócić funkcjonowanie jakiejś instytucji finansowej.

MAŁGORZATA AZEMBSKA

Tylko w pierwszym półroczu 2007 r. w instytucje finansowe wymierzonych było 5 proc. wszystkich ukierunkowanych ataków, co lokuje tę branżę na drugiej pozycji pod względem zagrożeń (tuż za użytkownikami domowymi). I wbrew rozpowszechnionemu przekonaniu, że głównym motywem jest złośliwość napastników z analizowanych danych wynika, że jest nim po prostu chęć zysku.

AGRESORÓW STYL

Rozpowszechnione było przede wszystkim rozpoczęcie sesji innego typu niż SMTP (40 proc. wszystkich atakujących adresów IP). Protokół SMTP (Simple Mail Transfer Protocol) jest wykorzystywany do przesyłania wiadomości pomiędzy serwerami poczty elektronicznej. Wykrycie tego ataku jest najczęściej wynikiem działań napastników, którzy manipulują protokołami przesyłania informacji mejlowych – może to być próba wyszukania przez spamera komputerów, których można użyć do wysyłania niepożądanej poczty e-mail. Atakujący mogą również obierać za cel usługi SMTP, aby ułatwić sobie przeprowadzanie ataków typu „phishing". Ten jest coraz częstszym i realnym problemem instytucji finansowych. Pisaliśmy już o nim wielokrotnie, ale warto przypomnieć: polega on na próbie uzyskania przez nieuprawnioną osobę poufnych informacji od danej osoby, grupy osób lub organizacji, zwykle w celu osiągnięcia korzyści finansowych. Usiłuje nakłonić użytkowników do ujawnienia osobistych danych, takich jak numery kart kredytowych, informacje umożliwiające dostęp do kont w trybie online itd. Są one wykorzystywane do oszustw. Bardzo często ataki typu „phishing" przeprowadzane są przy użyciu poczty e-mail. Atakujący wysyła ofierze lub grupie ofiar wiadomość e-mail, w której padają pytania o poufne dane, np. informacje umożliwiające dostęp do kont bankowych w trybie online. Takie wiadomości mogą zawierać również łącza do destrukcyjnych witryn internetowych, które udają autentyczne witryny instytucji finansowych. Jeżeli użytkownik skorzysta z takiego łącza, może zostać podstępnie nakłoniony, by wprowadzić do formularza umieszczonego w destrukcyjnej witrynie dane służące do uwierzytelnienia. Gdy włamywaczowi uda się uzyskać wpływ na serwer pocztowy firmy finansowej, może go wykorzystać w celu wysyłania fałszywych wiadomości e-mail z firmowych kont pocztowych. Symantec ocenia, że tylko w I półroczu ub.r. miało miejsce blisko 200 tysięcy wysyłek informacji typu „phishing". Oznacza to wzrost o 18 proc. w porównaniu z analogicznym okresem poprzedniego roku! Złodzieje są coraz przebieglejsi, bo wysyłane przez nich wiadomości bywają kierowane przeciw tym samym markom i firmom, ale różnią się drobnymi szczegółami – dla uniemożliwienia ich wykrycia przy użyciu popularnych metod ochrony przed atakami typu „phishing". Również atakiem wykrywanym przez czujniki rozmieszczone w sektorze usług finansowych było ogólne zdarzenie dodatkowego pakietu SYN w połączeniu TCP, występujące w przypadku 21 proc. atakujących adresów IP. TCP/IP jest protokołem służącym do kierowania transmisją danych między dwoma urządzeniami końcowymi. Częstość występowania tego ataku wskazuje, że włamywacze mogą próbować manipulować połączeniem

HAKERZY GODZĄ W SEKTOR USŁUG FINANSOWYCH

Miejsce	Atak	Procentowa część ataków w sektorze finansowym
1	Rozpoczęcie sesji innego typu niż SMTP	40
2	Ogólne zdarzenie dodatkowego pakietu SYN w połączeniu TCP	21
3	Komunikat ICMP o błędzie niewidzianego pakietu	10
4	Ogólny atak na usługę SMTP przy użyciu nieprawidłowych nazw domen	7
5	Ogólne zdarzenie segmentu TCP z nieprawidłową sumą kontrolną	5
6	Ogólny atak odmowy usługi typu UDP Flood	3
7	Atak przepełnienia buforu serwera Microsoft SQL	2
8	Ogólny atak odmowy usługi typu TCP RST-ACK Flood	2
9	Przepełnienie usługi Windows SMTP	1
10	Wykrycie zniekształconego pakietu protokołu HTTPS TLS	1

Źródło: Symantec Corporation

TCP/IP, stanowiącym podstawę większości protokołów internetowych. Atakujący, który skutecznie zmanipuluje połączenie TCP/IP, próbuje wywołać stan odmowy usługi (DoS, Denial of Service) oraz odczytać lub zmodyfikować dane przesyłane w tym połączeniu. W ten sposób napastnik może poznać lub zmienić poufne informacje przesyłane przez internet (np. numery kart kredytowych, dane osobowe lub dane służące do uwierzytelniania użytkownika). Aby bronić się przed takim atakiem, instytucje finansowe muszą dbać o to, aby wszystkie systemy, w tym zapory i routery, miały zainstalowane aktualne poprawki. Powinny także wdrożyć systemy wykrywania włamań obsługujące sygnatury, które wykrywają anomalie protokołu TCP/IP i innych, a wszystkie alerty powinny być badane. Trzecim pod względem częstości występowania atakiem w tym sektorze był komunikat ICMP o błędzie niewidzianego pakietu. Ten atak polega na odesłaniu odpowiedzi na internetowy komunikat sterujący (np. polecenie ping), który nigdy nie został wysłany. Może on być ubocznym skutkiem ataku typu „odmowa usługi" (DoS) przeciwko innemu serwerowi w internecie, przeprowadzanego przy użyciu sfałszowanych adresów IP. Atakujący za pomocą ataków typu DoS często fałszują adresy IP, a kiedy występuje błąd, komunikat o błędzie jest przesyłany nie na adres IP nadawcy, tylko na sfałszowany adres IP. Jeśli sfałszowany został adres IP czujnika, czujnik wykryje błąd dotyczący pakietu, którego nigdy nie wysłał. Atak typu „odmowa usługi" może spowodować, że witryny internetowe i inne usługi będą niedostępne dla klientów i pracowników. W efekcie może nastąpić przerwa w komunikacji internetowej firmy i znaczący spadek dochodów, a ponadto może zostać nadszarpnięta reputacja firmy. Banki powinny zadbać o opracowanie udokumentowanej procedury postępowania w przypadku ataków typu „odmowa usługi" (DoS). Jednym z najlepszych sposobów ograniczenia skutków takich ataków jest filtrowanie danych przed urządzeniem docelowym. Dla większości firm oznacza to konieczność skontaktowania się ze swoim usługodawcą internetowym. Pożyteczne jest również filtrowanie całego ruchu wychodzącego. Wiele rodzajów zapór i systemów operacyjnych ma parametry konfiguracyjne, których można użyć do ograniczenia skutków ataku typu „flood". Firmy powinny prawidłowo skonfigurować wszystkie urządzenia, które mogą stać się celem ataków typu „odmowa usługi", aby ograniczyć ewentualne następstwa tych ataków.

FINANSE – NAJCZĘŚCIEJ ATAKOWANA BRANŻA

Miejsce	Podział marek, których dotyczyły ataki typu „phishing" według sektorów	Proc.
1	Finanse	79
2	Usługodawcy Internetowi	11
3	Handel detaliczny	3
4	Społeczności internetowe	2
5	Ubezpieczenia	2
6	Inne	2
7	Sprzęt komputerowy	1
8	Instytucje publiczne	1
9	Oprogramowanie	1
10	Organizacje non profit	<1

Źródło: Symantec Corporation

PORTY POD OSTRZAŁEM

Miejsce	Port	Udział procentowy	Usługa
1	TCP 25	6	Poczta e-mail (SMTP)
2	TCP 80	3	Sieć WWW (HTTP)
3	TCP 21	3	FTP
4	UDP 1434	2	Microsoft SQL Server
5	UDP 53	2	DNS
6	TCP 443	2	Bezpieczne połączenia WWW (HTTPS)
7	UDP 8116	2	Checkpoint Clustering
8	UDP 161	2	SNMP
9	UDP 137	2	Usługa nazw protokołu NetBIOS
10	TCP 1433	2	Microsoft SQL Server

Źródło: Symantec Corporation

Tylko w I półroczu ub.r. miało miejsce blisko 200 tysięcy wysyłek informacji typu „phishing". Oznacza to wzrost o 18 proc. w porównaniu z analogicznym okresem poprzedniego roku!

PRZESZŁO POŁOWA ATAKÓW NA BANKI

Spośród 198 tys. wykrytych wiadomości typu „phishing", 54 proc. dotyczyło branży usług finansowych. Atakujący starali się dotrzeć do jak największej liczby instytucji finansowych, aby wykorzystać markę danej firmy. Może mieć to poważne, negatywne konsekwencje, wpływając niekorzystnie na zaufanie klientów i szkodząc reputacji firmy oraz w niektórych przypadkach obligując instytucję finansową do wypłacenia odszkodowania ofiarom oszustw wykorzystujących jej markę. A firmy z branży usług finansowych stanowią 79 proc. marek wykorzystywanych w atakach typu „phishing"! Branży usług finansowych dotyczyło również 72 proc. witryn internetowych służących do ataków typu „phishing".

Instytucje finansowe nie mogą spać spokojnie. Wraz z rozbudowywaniem usług złodzieje siłą rzeczy mają większe pole do popisu. Jednym z głównych obowiązków instytucji jest zapewnienie bezpieczeństwa zdeponowanych przez klientów w jakiejkolwiek formie pieniędzy – w ich oraz we własnym interesie. ■