Daniel Soliwoda, Wanda Gryglewicz-Kacerka

Państwowa Wyższa Szkoła Zawodowa we Włocławku

Ataki sieciowe w przestrzeni wirtualnej

Network attacks in cyber space

Streszczenie

Praca zawiera charakterystykę nielegalnych ataków sieciowych prowadzonych w przestrzeni wirtualnej. Celem ataków jest przejęcie kontroli nad źródłami informacji znajdującymi się w Internecie, skrzynkach pocztowych oraz bazach danych różnych instytucji. W pracy zostały scharakteryzowane dwie odmiany ataków: atak kierowany oraz atak zmasowany oraz najczęściej stosowane systemy wykrywania zagrożeń to IPS oraz IDS.

Słowa kluczowe: ataki komputerowe, bezpieczeństwo teleinformatyczne

Abstract

The thesis presents the characteristics of the illegal network attacks conducted in cyber space. The aim of the attacks is to take control over the sources of information located on the Internet, mailboxes and databases of various institutions. Described in the thesis are two varieties of attacks: directed attack and a mass attack as well as the most commonly used Intrusion Detection (IDS) and Prevention (IPS) systems.

Keywords: computer attack, information security

1. Wstęp

Cyber atak to nielegalne działanie prowadzone w przestrzeni wirtualnej, którego celem jest przejęcie kontroli nad stronami internetowymi, zawartością skrzynek pocztowych lub baz danych jakiejś instytucji, firmy itp.

Cyberterroryzm to wykorzystywanie środków komunikacji elektronicznej do aktów przemocy, zwykle o podłożu politycznym bądź ideologicznym, wymierzonych przeciwko bezpieczeństwu informacyjnemu.

Cyber przestępstwo to przestępstwo popełnione za pośrednictwem środków komunikacji elektronicznej, zwłaszcza Internetu.

Te trzy definicje nowych pojęć [1] charakteryzują nielegalną działalność pozwalającą ujawnić wiele ważnych informacji. Zwyczajnie te działania to dokonywanie ataków sieciowych. Przykładowo obecne możliwości techniczne pozwalają dokonać ataku sieciowego, którego wynikiem jest pozyskanie poufnych danych dotyczących finansów, dóbr materialnych lub profilu działalności atakowanego podmiotu. W nowoczesnym słownictwie tego typu proces nazywamy Cyber atakiem.

2. Rodzaje Cyber ataków

- Ataki DoS (*dential of service*)

Celem ataków DoS jest uniemożliwienie działania systemu komputerowego lub usługi sieciowej. Tego typu cyberataki mają swoje wersje, w zależności od sposobu ich realizacji. Ataki typu **DoS** starają się spowodować blokowanie dostępu do systemu lub przeciążanie danego serwisu, aby nie mógł on realizować swojej funkcji.

W sieciach komputerowych atak DoS oznacza zwykle zalewanie sieci (*flooding*) nadmiarową ilością danych mających na celu wysycenie dostępnego pasma, którym dysponuje atakowany host. Niemożliwe staje się wtedy osiągnięcie go, mimo że usługi pracujące na nim są gotowe do przyjmowania połączeń.

Wszystkie statystyki zespołów badających cyberprzestrzeń na świecie wykazują ciągły wzrost tego typu ataków.

- Atak DDoS

Cel tego typu ataku jest wysycenie zasobów systemu informatycznego poprzez infekowanie systemu (bez wiedzy właściciela). Ta metoda ataku utrudnia obronę. DDoS (*distributed denial of service*) to atak na system komputerowy lub usługę sieciową mający na celu uniemożliwienia

działania (poprzez zajęcie wszystkich wolnych zasobów, przeprowadzany równocześnie z wielu komputerów).

Do przeprowadzenia ataku służą najczęściej komputery, nad którymi przejęto kontrolę przy użyciu specjalnego oprogramowania. Na dany sygnał komputery zaczynają jednocześnie atakować system ofiary, zasypując go fałszywymi próbami skorzystania z usług, jakie oferuje. Efektem takiego działania dochodzi do zawieszenia systemu [1].

Atak DDoS bywa używany do szantażowania firm, w których przerwa w działaniu systemu transakcyjnego przekłada się na bezpośrednie straty finansowe firmy i jej klientów. W takich przypadkach osoby stojące za atakiem żądają okupu za odstąpienie od ataku lub jego przerwanie. Szantaż taki jest przestępstwem.

- Atak DRDOS (*distributed reflected denial of service*)

Atak DRDOS to odmiana ataku odmowy dostępu DoS. DRDOS pozwala na zwiększenie efektywności działania ataku DoS poprzez wykorzystanie zjawiska odbicia. W tym przypadku wykorzystano zwykły proces komunikacji komputerów w Internecie. Posłużono się metodą, która polega na tym, że każdy komputer i urządzenie podłączone do sieci odpowiada na każde zapytanie w Internecie, jakie dostanie ze świata. Metoda powstała w wyniku połączenia metody zalewania żądaniami synchronizacji i metod wykorzystywanych przy rozproszonych atakach odmowy dostępu DDoS.

Metoda polega na generowaniu specjalnych pakietów SYN, mających fałszywy adres źródłowy, na który wysyłane są do sieci duże ilości informacji. W porównaniu do tradycyjnego ataku typu DDoS utrudnia to skutecznie wykrycie rzeczywistego źródła ataku.

- Amplification DDoS (wzmocniony atak DDoS)

Wzmocniona odmiana ataku DDoS, polegająca na wysłaniu zapytań do serwerów ze sfałszowanym adresem zwrotnym (*spoofing*). Najczęściej wykorzystuje się do tego sieć przejętych przez włamywacza komputerów (*botnet*). Serwery, w odpowiedzi na tysiące zapytań, wysyłają odpowiedzi na jeden komputer włamywacza, zajmując jego całą pamięć. Obrona przed takim atakiem bardzo trudna. W przypadku tego ataku wykorzystano nie tylko zjawisko odbicia, ale dodatkowo dołożono zjawisko wzmocnienia?

Metod ataków typu DoS wciąż przybywa. Ataki dotykają praktycznie dowolnego serwisu internetowego, np. systemów VoIP do rozmów telefonicznych przez Internet. Ponadto metody ataków DoS zaczynają przechodzić do najwyższych warstw komunikacji internetowej. Przykładowo możliwe są ataki:

- ReDoS

  Celem ReDoS jest maksymalne wykorzystanie mocy obliczeniowej aplikacji internetowej lub zapętlenie jej algorytmu działania.

- APDoS

  To bardzo skomplikowany typ ataku DDoS, który wykorzystuje wiele metod jednocześnie. Skupia się przede wszystkim na aplikacji, ale nie na łączu (co nie oznacza, że łącze nie jest atakowane). Ten typ ataku wymaga przygotowania całego scenariusza ataku, wykorzystując różne płaszczyzny takiego działania: skanowanie i sprawdzanie zabezpieczeń (rozpoznanie), rozpoznanie i przygotowanie scenariusza ataku, wybór *motywacji* w ramach działań cyberwojny (jednoczesność realizacja wielu typów ataków w tej samej chwili, okresowość polega na cyklicznym wykonywaniu różnego typu ataków). Taka forma działania atakujących nazywana jest Hit-and-run DoS.

Rodzajów ataków DoS wciąż przybywa. Hakerzy analizują zwykłe sposoby komunikacji urządzeń lub aplikacji w Internecie i szukają scenariuszy, które pozwolą na „wyłączenie" serwisu internetowego lub otworzą drzwi do włamania. Trwa ciągły wyścig zbrojeń atakujących i firm tworzących systemy obronne.

Angażowane są coraz bardziej zaawansowane technologie w tym zastosowano systemy sztucznej inteligencji, której zadaniem jest wykrywanie każdej anomalii. Samo wystąpienie anomalii nie jest jeszcze informacją o ataku, ale daje sygnał do jeszcze większej aktywności oficerów bezpieczeństwa, analizy tego co się wydarzyło i sprawdzenia czy to było działanie przypadkowe czy celowe. Scenariusze grup atakujących hakerów są coraz bardziej rozbudowane i bazują na wszystkich możliwych metodach ataków. Ochrona przed cyberatakami wymaga ciągłego monitoringu systemów informatycznych oraz weryfikowania każdego sygnału, który może być potencjalnym atakiem.

3. Anatomia ataku oraz metody ochrony

W pracy zostaną scharakteryzowane dwie odmiany ataków: atak kierowany oraz atak zmasowany.

W ataku kierowanym skupiamy się na pozyskaniu informacji o szczególnym znaczeniu i wysokiej wartości. Wykonanie takiego ataku wymaga precyzyjnego przygotowania i dużego nakładu finansowego. Niezbędny zatem jest czas na zorganizowanie zintegrowanego planu działania (rozeznanie, wyznaczenie celu, przyjęcie algorytmu działania). Celem tego typu ataków są informacje o dużym znaczeniu strategicznym, gospodarczym lub finansowym.

W procesie poznawczym określa się otoczenie ofiary. Analiza otoczenia polega na zainfekowaniu obcej stacji roboczej z poziomu np. wiadomości mailowej (wysyła mu informację z zainfekowanym kodem). Otwarcie zainfekowanej wiadomości skutkuje przedostaniem się infekcji na nasz komputer. W dalszym etapie następuje zagnieżdżenie złośliwego kodu na dysku komputera. Infekcja zbiera informacje, które gromadzi i przetwarza a następnie wznawia połączenie z komputerem kierującym całą akcją. Aby zminimalizować szanse na wykrycie, wielkość przesyłanych informacji jest nie duża, dlatego proces infiltracji obcej stacji roboczej jest długi.

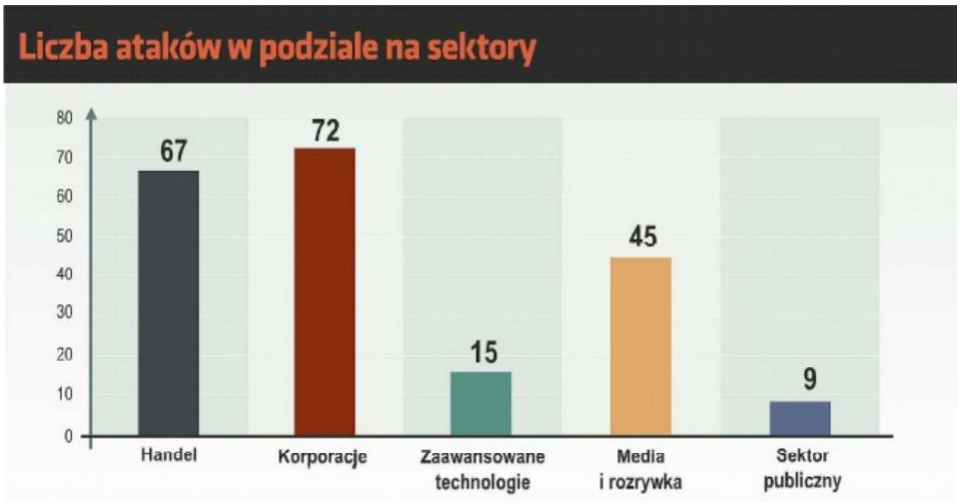
W inny sposób działa atak typu DDoS. Jest to atak zmasowany, którego celem jest wręcz natychmiastowe pozyskanie informacji. Polega on na wysyłaniu do serwera ogromnej ilości zapytań w wyniku których maszyna nawiązująca łączność z serwerem (router lub przełącznik) będą przeciążone lub przestaną działać. Na ruch skierowany do tego serwera zostanie nałożona blokada co będzie oznaczać, że dana witryna internetowa będzie niedostępna. Aby za pomocą jednego komputera z dostępem do sieci wykonać zmasowany atak należy w tym celu wykonać atak rozproszony, w którym generuje się ogromny ruch w sieci z wielu źródeł jednocześnie. Całą operacją steruje się z poziomu własnego komputera. Stosowanie rozgałęzionego systemu połączeń zapewnia hakerowi niewrażliwość na ewentualne odcięcia poszczególnych gałęzi poprzez blokadę jej adresu IP. Do stworzenia odpowiedniej sieci atakującej używa się zazwyczaj botnetu. Botnet to grupa komputerów zainfekowanych złośliwym oprogramowaniem pozostającym w ukryciu przed użytkownikiem i pozwalającym

jego twórcy na sprawowanie zdalnej kontroli nad wszystkimi komputerami w ramach botnetu.

Z przeprowadzonych analiz, publikowanych przez firmę Prolexic wynika, że średnia liczba ataków w ciągu 1 roku wzrasta o 22%. Sam proceder trwa o wiele dłużej – z 28,5h przedłuża się do 34,5h. Średni ruch generowany podczas ataku wynosi 2 Gb/s i jest mniej więcej o 25% większy niż w 2012 roku.

Poniższy wykres prezentuje liczbę ataków w podziale na sektory gospodarki.

Rysunek. 1. Wykres prezentujący analizę celów ataków hackerskich. Badania przeprowadzone przez Akamai [3)].



Z wykresu wynika, że najczęstszym obiektem ataku są korporacje. Operacje finansowe przeprowadzane na dużą skale także i informacje na temat prowadzonych przedsięwzięć to ogniwo zapalne dla działań potencjalnego hakera.

Czy istnieje sposób aby ochronić własne dobra intelektualne i materialne przed dostaniem się w niepowołane ręce? Obecnie podstawowa zapora sieciowa przestaje być wystarczającym zabezpieczeniem. Ataki na infrastrukturę stają się coraz to bardziej rozwinięte i lepiej zorganizowane. Nie wystarczają już standardowe zabezpieczenia jakie zapewniają nam statyczne systemy bezpieczeństwa.

4. Systemy wykrywania zagrożeń

Najczęściej stosowane systemy wykrywania zagrożeń to IPS (*Intrust Prevention System*) oraz IDS (*Intrust Detection System*).

System IPS działa podobnie jak zapora sieciowa, ale wyróżnia się faktem posiadania zaawansowanej bazy sygnatur. Zapora sieciowa bazuje na mechanizmach blokady protokołów sieciowych, czyli przeważnie na podstawie warstwy 2 i 3 modelu OSI/ISO. IPS potrafi blokować bardziej zaawansowane formy przepływu informacji, wykrywa znane ataki sieciowe. Ten system może pełnić dodatkowe funkcje np. ograniczanie ilości ruchu, zapobieganie atakom DDoS. IPS zawiera narzędzia zapobiegające utracie danych i wykrywające anomalie sieciowe. Główne jego zadanie dotyczy analizy i oceny zagrożeń na podstawie wskazanej bazy sygnatur. Następnie podejmowane są działania mające na celu wyeliminowanie zagrożeń. IPS jest zintegrowany z zaporą sieciową. Takie rozwiązanie nazywane jest (*Universal Threat Management*) w skrócie UTM.

System detekcji incydentów IDS realizuje odmienne funkcje od IPS. Są one przeznaczone do rozwiązywania rozmaitych problemów związanych z bezpieczeństwem. IDS może jednak współpracować z IPS w dość szerokim zakresie zadań. Potrafi on wspierać tworzenie sygnatur. IDS w przeciwieństwie do IPS jest umiejscowiony poza centralną lokalizacją w sieci i nie monitoruje całego przepływu danych. System IDS monitoruje ruch w różnych punktach sieci i może zostać porównany do rozproszonego analizatora sieci. IDS analizuje dane pochodzące z różnych punktów sieci w zakresie bezpieczeństwa. Realizuje to na podstawie znanych sygnatur, ale może także pracować inteligentnie, realizując wsparcie w zakresie tworzenia nowych sygnatur. Informuje o naruszeniach polityki bezpieczeństwa, infekcjach lokalnych komputerów, wyciekach informacji, problemach z konfiguracjami i wielu innych problemach sieciowych.

Obecnie sieć informatyczna stwarza przed użytkownikami duże możliwości ale obarczone wielkim ryzykiem. Statystycznie w 2015 roku jeden atak na komputer odbywał się z częstotliwością raz na sekundę. Należy skoncentrować swoją uwagę na obronie własnych danych.

Przechowywane zbiory plików w lokalnych bazach danych mogą stać się celem skoncentrowanego ataku pojedynczego hakera lub

zorganizowanej grupy hakerów. Większość osób lub przedsiębiorstw bagatelizuje problem i poprzestaje na podstawowej ochronie. Takie niedopatrzenie i pozostawienie luki w swoich zabezpieczeniach może skutkować utratą cennych plików. Istotne w takim razie jest zorganizowanie zaplecza i infrastruktury do przechowywania danych, którymi firma zarządza na co dzień. Wartości materialne jak i zarówno intelektualne a przede wszystkim wiedza zasługują na istotne traktowanie i bezpieczeństwo.

5. Literatura

1. https://pl.wikipedia.org
2. http://www.komputerswiat.pl/nowosci/bezpieczenstwo/2013
3. http://www.frazpc.pl
4. https://pl.glosbe.com/pl/pl/cyberatak
5. http://www.computerworld.pl/news/395436/Ataki.DDoS.wykrywanie.i.zwalczanie.html
6. http://www.computerworld.pl/news/390436_2/Informatyka.antywlamaniowa.html
7. http://www.computerworld.pl/news/391903/Czy.polskim.firmom.grozi.atak.kierowany.html