Wojna cybernetyczna

Wykorzystanie komputerów, Internetu i innych środków przechowywania lub rozprzestrzeniania informacji w celu przeprowadzania ataków na systemy informatyczne przeciwnika

W ramach wojny cybernetycznej, napastnik może dążyć do realizacji rozmaitych celów strategicznych, od rozpowszechniania propagandy lub wywoływania paniki pośród ludności cywilnej, po trwałe uszkodzenie kluczowych elementów infrastruktury technologicznej (elektrownie, systemy komunikacyjne, itp). Ataki mogą też być narzędziem wywiadu technologicznego i pozyskiwania informacji.

W zależności od celu, ataki mogą wykorzystywać pełną gamę narzędzi:
a) komputery zombie - komputer przyłączony do Internetu, w którym bez wiedzy jego posiadacza został zainstalowany program sterowany z zewnątrz przez inną osobę. Celem takiego działania jest zazwyczaj wykorzystanie komputera do działań sprzecznych z prawem używane do ataków **DDoS**,
a) exploity pozwalające na przejęcie kontroli nad systemami, exploit - program mający na celu wykorzystanie istniejących błędów w oprogramowaniu.
b) metody socjotechniczne zmierzające do manipulacji ludźmi, itp. Ataki tego typu mogłyby osłabić lub uszkodzić systemy wykorzystywane przez siły zbrojne przeciwnika, co mogłoby doprowadzić do ich całkowitego odsłonięcia na polu walki w czasie wojny elektronicznej.

Wojna cybernetyczna

DDoS *- distributed denial of service*, rozproszona odmowa usługi) – atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów, przeprowadzany równocześnie z wielu komputerów (np. zombie).
Atak DDoS jest odmianą ataku DoS polegającą na zaatakowaniu ofiary z wielu miejsc jednocześnie. Do przeprowadzenia ataku służą najczęściej komputery, nad którymi przejęto kontrolę przy użyciu specjalnego oprogramowania (różnego rodzaju tzw. boty i trojany). Na dany sygnał komputery zaczynają jednocześnie atakować system ofiary, zasypując go fałszywymi próbami skorzystania z usług, jakie oferuje. Dla każdego takiego wywołania atakowany komputer musi przydzielić pewne zasoby (pamięć, czas procesora, pasmo sieciowe), co przy bardzo dużej liczbie żądań prowadzi do wyczerpania dostępnych zasobów, a w efekcie do przerwy w działaniu lub nawet zawieszenia systemu.

Anonymous – globalna, zdecentralizowana grupa aktywistów sprzeciwiająca się ograniczaniu wolności obywatelskich, korupcji, konsumpcjonizmowi, cenzurze, fair use –dozwolony użytek , łamaniu praw zwierząt. Anonymous jest również definiowana jako ideologia dążąca m.in. do sprawiedliwości, obrony wolności obywatelskich oraz rozwiązania innych problemów społecznych.

Rodzaje ataków, złośliwe oprogramowanie

Malware – złośliwe oprogramowanie (zbitka słów malicious czyli „złowrogi, złośliwy” i software czyli „oprogramowanie”). Rodzajów takiego oprogramowania jest wiele. Zawsze wtedy, kiedy mówisz, że komputer nabawił się wirusa, robaka, konia trojańskiego – mówisz o malware. Złośliwe oprogramowanie ma różne zastosowanie, ale jedną wspólną cechę: działa na komputerze użytkownika bez jego zgody i wiedzy.
Minimum ostrożności: dobry antywirus i regularna aktualizacja oprogramowania.

Ransomware – to również rodzaj malware, ale zasługuje na szczególną uwagę. Bardzo popularny typ cybeataku, którego celem jest zaszyfrowanie danych na komputerze ofiary, a następnie żądanie okupu w zamian za ich odblokowanie (stąd nazwa – ransom czyli „okup”). Bardzo groźny atak, naraża na ogromne straty materialne zarówno osoby fizyczne, jak i przedsiębiorstwa.
Minimum ostrożności: zawsze antywirus i regularna aktualizacja oprogramowania, ale w tym przypadku również ważne jest szyfrowanie poufnych dokumentów oraz wykonywanie kopii zapasowych.

Man in the Middle – rodzaj ataku kryptologicznego. Haker („człowiek pośrodku”) podsłuchuje i modyfikuje wiadomości przesłane pomiędzy dwiema stronami bez ich zgody. Są to wszystkie ataki związane z przejęciem danych niezbędnych do logowania do bankowości elektronicznej (podsłuchanie) i podmianą strony płatności w sklepie internetowym na przygotowaną przez przestępców (modyfikacja).
Minimum ostrożności: certyfikaty bezpieczeństwa i szyfrowanie transmisji danych.

Cross site scripting – sposób ataku na serwis WWW. Haker szuka luki, a następnie osadza w treści atakowanej strony swój kod, na przykład własny tekst, baner etc. Taki atak na serwisy internetowe CBS News i BBC umożliwił rozpowszechnienie fałszywej informacji o tym, że dziewięciolatek został nominowany na szefa departamentu bezpieczeństwa informatycznego w USA. Tu akurat mieliśmy do czynienia z dowcipnisiem, ale najczęściej takie ataki służą przestępcom do przygotowania trudnego do wykrycia phishingu albo rozesłaniu groźnego wirusa.
Minimum ostrożności: to zależy. Przed wirusem może ochronić Cię dobry antywirus i zaktualizowane oprogramowanie. W kwestii phishingu rekomendujemy ostrożność i poszerzanie swojej wiedzy o metodach, jakie wykorzystują przestępcy w trakcie takiego ataku.

Rodzaje ataków

Phishing – atak, którego celem jest pozyskanie danych ofiary do logowania do bankowości elektronicznej, serwisów społecznościowych, poczty itd. Przestępca najczęściej podszywa się pod inną osobę lub instytucję, a próba wyłudzenia informacji odbywa się za pośrednictwem maila. Zobrazujmy to. Otrzymujesz informację z banku, że ktoś próbował się włamać na twoje konto, więc czym prędzej powinieneś zmienić hasło do logowania. Mail zawiera instrukcję, abyś zrobił to klikając w poniższego linka. Klikasz, wydaje Ci się, że jesteś na stronie banku, wpisujesz login i hasło, przestępca je przechwytuje, a ty nawet tego nie zauważasz. Atakujący właśnie je „złowił" (phishing pochodzi od słów password czyli „hasło" i fishing czyli „wędkowanie").
Minimum ostrożności: edukacja, edukacja i jeszcze raz edukacja. Łatwo się nabrać na taki atak, dlatego nieustannie poszerzaj swoją wiedzę na temat phishingu.

DDoS – atak DDoS prowadzi do zablokowania strony internetowej i polega na jednoczesnym logowaniu się na nią wielu osób w tym samym czasie. Tak, to również jest cyberatak, choć nie wymaga żadnego złośliwego oprogramowania, szukania luk na stronie ani znajomości technik manipulacji.
Minimum ostrożności: jeśli nie chcesz, by taki incydent przydarzył się na Twojej stronie, pamiętaj o filtrowaniu ruchu w witrynie.

SQL Injection – atak polega na znalezienie luki w zabezpieczeniach aplikacji po to, aby uzyskać nieuprawniony dostęp do bazy danych (kradzież listy klientów wraz z danymi kontaktowymi etc.).
Minimum ostrożności: zabezpieczenie na poziomie bazy danych przygotowuje administrator strony internetowej.

Malvertising – polega na zainstalowaniu różnego typu złośliwego oprogramowania. Nośnikiem jest tu reklama internetowa.
Minimum ostrożności: zainstaluj AdBlocka