Krzysztof Szyling

Systemy Agentowe – Sieci BotNet

Czarna strona wykorzystania systemów agentowych w praktyce.

4/30/2010

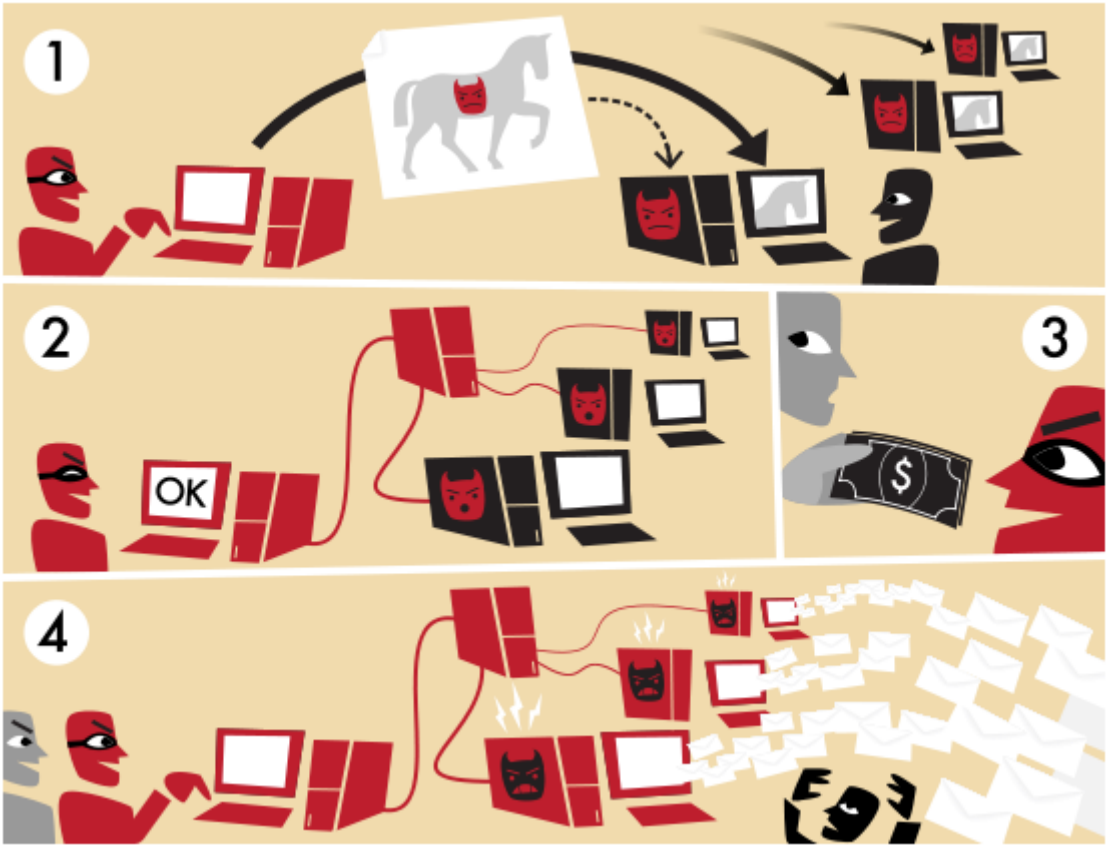
Systemy agentowe mogą zdecydowanie ułatwić korzystanie z usług internetowych oraz zrewolucjonizować wiele aspektów związanych z wykorzystywanie sieci Internet. Nawet w sieciach lokalnych lub korporacyjnych występuje wiele komercyjnych mechanizmów wykorzystujących techniki agentowe, służących do celów nadzorczych, raportowych lub reklamowych. Niemal każdy system oparty na SLA (Service Level Agrement) działa za pomocą rozproszonych sieci agentów zbierających dane o dostępności danego serwisu. Agentowość tego rozwiązania jest niemal konieczna, gdyż serwis który nie jest widziany z "centralnego komputera" niekoniecznie musi być niedostępny w ogóle (awaria obserwatora a nie obserwowanego). Możliwość wielopunktowej obserwacji jest kluczowa dla wiarygodnego określenia SLA wielu serwisów jednocześnie. Przykładów zastosowań zgodnych z prawem można by mnożyć, jednak krok przed rozwiązaniami komercyjnymi zawsze stoi świat przestępczy, który dysponuje ogromnymi funduszami i wielką determinacją by wykorzystać nowe zdobycze nauki do nielegalnych celów. Nielegalne organizacje potrafią pozyskać utalentowane osoby oraz technologię, by stworzyć systemy do masowego okradania i wykorzystywania ludzi i organizacji niezależnie od ich geograficznego położenia.

Przykładem takiej działalności są sieci BotNet tworzone z milionów komputerów zainfekowanych złośliwym oprogramowaniem. Oprogramowanie zmusza zainfekowane komputery (zwane dalej "zombie") do zbierania danych o użytkowniku komputera i wykonywania poleceń **głównego komputera sterującego (CnC - Command And Control)**. Oczywiście za tym procederem stoją ludzie i to na ich rozkaz miliony komputerów atakują banki, firmy czy nawet całe państwa lub wykradają tożsamości właścicieli zagrożonych komputerów. Kilkumilionowa armia zombie, do wynajęcia do niemal dowolnego celu, dostępna dla każdego za zaledwie kilka tysięcy dolarów.

Początek może być banalny, wystarczy jeden komputer w sieci z zainstalowanym systemem operacyjnym, którego podłączamy do internetu w celu ściągnięcia dodatkowych aktualizacji lub programu antywirusowego. Już po kilku sekundach nasz komputer może być zainfekowany "koniem trojańskim" co praktycznie oznacza że nie jest już nasz. Od tego momentu agent na naszym komputerze zaczyna ciężką pracę. Przede wszystkim przeszukuje całą dostępną sieć w poszukiwaniu kolejnych ofiar na które może przenieść swoje kopie. Wykorzystuje luki systemowe które jeszcze nie zostały naprawione przez producentów oprogramowania lub nie zostały zaimplementowane przez administratorów. W trakcie skanowania i kopiowania wielokrotnie mutuje, by nie dopuścić do jego wykrycia. W tym samym czasie uszkadza elementy systemu operacyjnego oraz programy antywirusowe, by nie dopuścić do jego usunięcia (blokuje serwisy automatycznych poprawek, uszkadza silniki znanych programów antywirusowych, wielokrotnie się kopiuje i mutuje zapewniając sobie redundantne uruchomienie wraz z uruchomieniem komputera) dodatkowo próbują łamać hasła kont wyciąganych z usług katalogowych by zdobyć uprawnienia do dalszego rozprzestrzeniania się w sieci. To oczywiście nie koniec jego pracy, a zaledwie dopiero początek. Już po kilku minutach w naszej sieci firmowej możemy mieć kilkadziesiąt lub nawet kilkaset komputerów zombie które zaczynają przestępczy proceder.

Największa obecna sieć komputerów zombie zbudowana jest z ponad 10’000’000 (Conficker) komputerów i pomimo otwartej wojny producentów programów antywirusowych i systemów operacyjnych ta liczba stale rośnie. Kolejne znane sieci mają także miliony hostów (Zeus 3,5 mln… Koobface 2,9 mln) takich sieci jest kilkadziesiąt i ciągle powstają kolejne. Obecnie popularne są sieci wielkości kilku tysięcy agentów, by precyzyjniej nimi zarządzać oraz chronić przed wykryciem.

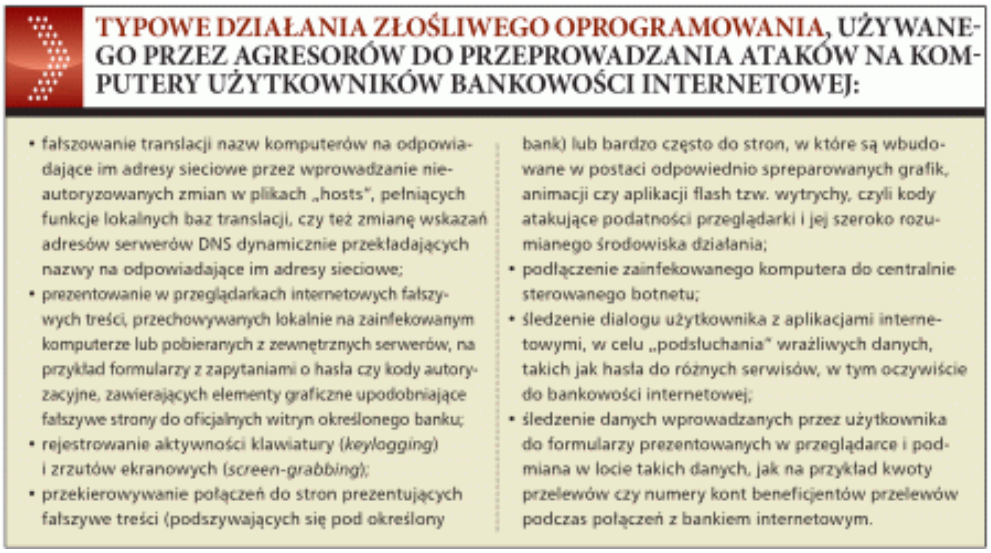
Głównym celem do jakiego można "zatrudnić" BotNet jest rozsyłanie wiadomości SPAM. Wg. danych Kasperskiego, przeciętny SPAMer zarabia rocznie od 50 do 100 tysięcy dolarów rocznie, wykorzystując BotNet, nie dość że dysponuje milionami prawdziwych adresów pobranych z zainfekowanych maszyn, to jednocześnie dysponuje niewykrywalna maszyną do wysyłania wiadomości.



Pasted from <http://en.wikipedia.org/wiki/Botnet>

Osoba zainteresowana wysłaniem miliardów wiadomości płaci za fragment sieci, by ta na chwilę wysyłki stała się gigantyczną machiną do wysyłania wiadomości e-mail. Serwery są nie do zablokowania, ponieważ nigdy wcześniej nie pełniły takiej funkcji a kolejna wysyłka może się odbywać już z zupełnie innej części świata. Po wykonaniu zadania, sieć powraca do swoich podstawowych funkcji oraz oczekuje na kolejne rozkazy. Rozkazy wydawane są zazwyczaj za pomocą sieci ogólnodostępnych serwerów IRC, ale każdy z BotNetów ma swoje własne i tylko im znane metody komunikacji. Często komputery zombie same poszukują rozkazów w znanych im miejscach (CnC) a metody komunikacji omówię poniżej.

BotNet gotowy do działania wykonuje też bardziej wyrafinowane przestępstwa a kolejnym z popularnych jest kradzież tożsamości. Wartościowa tożsamość w przestępczym świecie to przede wszystkim karty kredytowe oraz kody dostępowe go bankowości elektronicznej. Po przechwyceniu takiej tożsamości, karty i konta bankowe niemal natychmiast są czyszczone z pieniędzy. Ilość skradzionych w ten sposób tożsamości szacuje się na dziesiątki milionów. Do wykrywania ich zostały stworzone specjalne jednostki rządowe na całym świecie. Oprócz informacji bezpośrednio prowadzących do pieniędzy, sieć agentów zbiera nazwy użytkowników portali społecznościowych, kont e-mail oraz inne informacje na które jest popyt na czarnym rynku. Wykorzystanie tych informacji może być przeróżne, od wrzucania reklam na forach, po kradzież domen i tożsamości internetowych.



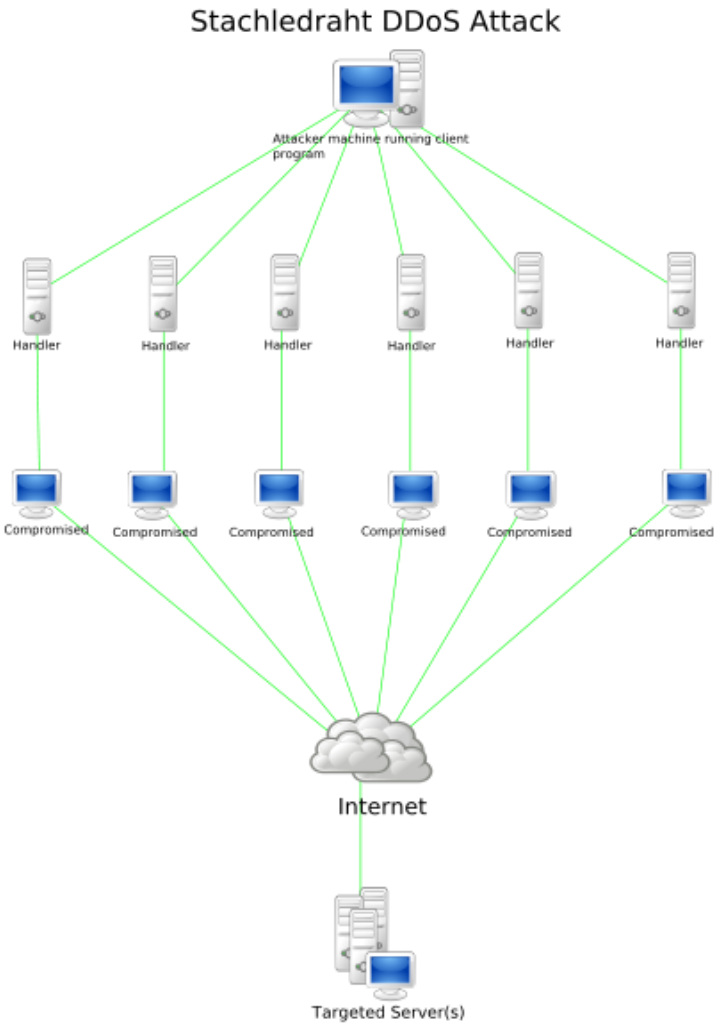
TYPOWE DZIAŁANIA ZŁOŚLIWEGO OPROGRAMOWANIA, UŻYWANEGO PRZEZ AGRESORÓW DO PRZEPROWADZANIA ATAKÓW NA KOMPUTERY UŻYTKOWNIKÓW BANKOWOŚCI INTERNETOWEJ:

- fałszowanie translacji nazw komputerów na odpowiadające im adresy sieciowe przez wprowadzanie nieautoryzowanych zmian w plikach „hosts", pełniących funkcje lokalnych baz translacji, czy też zmianę wskazań adresów serwerów DNS dynamicznie przekładających nazwy na odpowiadające im adresy sieciowe;
- prezentowanie w przeglądarkach internetowych fałszywych treści, przechowywanych lokalnie na zainfekowanym komputerze lub pobieranych z zewnętrznych serwerów, na przykład formularzy z zapytaniami o hasła czy kody autoryzacyjne, zawierających elementy graficzne upodobniające fałszywe strony do oficjalnych witryn określonego banku;
- rejestrowanie aktywności klawiatury (*keylogging*) i zrzutów ekranowych (*screen-grabbing*);
- przekierowywanie połączeń do stron prezentujących fałszywe treści (podszywających się pod określony bank) lub bardzo często do stron, w które są wbudowane w postaci odpowiednio spreparowanych grafik, animacji czy aplikacji flash tzw. wytrychy, czyli kody atakujące podatności przeglądarki i jej szeroko rozumianego środowiska działania;
- podłączenie zainfekowanego komputera do centralnie sterowanego botnetu;
- śledzenie dialogu użytkownika z aplikacjami internetowymi, w celu „podsłuchania" wrażliwych danych, takich jak hasła do różnych serwisów, w tym oczywiście do bankowości internetowej;
- śledzenie danych wprowadzanych przez użytkownika do formularzy prezentowanych w przeglądarce i podmiana w locie takich danych, jak na przykład kwoty przelewów czy numery kont beneficjentów przelewów podczas połączeń z bankiem internetowym.

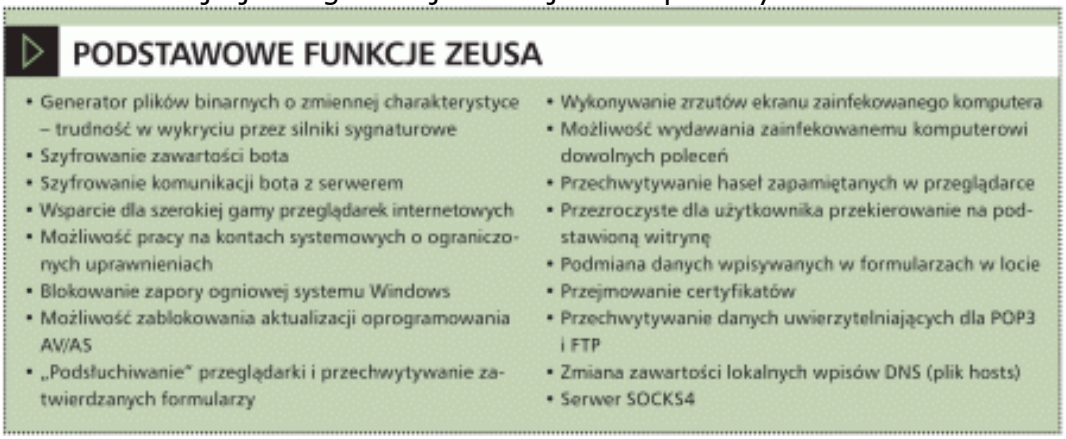
Pasted from <http://www.networld.pl/artykuly/352274_3/E.banking.na.celowniku.html>

Tak ogromne sieci to także olbrzymie zagrożenie dla firm a nawet państw.
W kwietniu 2007 roku odbył się pierwszy cyberatak na cały kraj. Estonia została zaatakowana przez Rosyjskie grupy hackerskie. Atak DoS wymierzony w urzędy, banki oraz większe firmy sparaliżował całkowicie pracę państwa dodatkowo całkowicie odcinając je od internetu. Wg. Estońskiej minister obrony to był najbardziej przerażający atak jakiego doświadczyła. Na jednej z konferencji mówiła, że w momencie tradycyjnego ataku, wystarczy oszacować siły wroga i wysłać tyle czołgów, żołnierzy i statków ile potrzeba (lub ile się posiada), w przypadku cybeataku nie wiadomo kto atakuje, czego chce ile to może potrwać a już przede wszystkim nie wiadomo jak się bronić. Od czasu tego ataku na całym świecie ataki cyber złoczyńców zostały dodane do podstawowych zagrożeń w dokumentacji ciągłości działania firm, urzędów i krajów (plany BCP) a odpowiednie procedury zapobiegania wchłonęły grube miliony z budżetów firm i organizacji. Panika jest tym większa, że obserwatorzy uważają, że Estonia była tylko próbą/pokazem sił. Dodając do tego możliwość prowokacji politycznych (atak na jedno państwo z obszaru drugiego, ale sterowany przez osoby z trzeciego…) pozwala nakreślać zupełnie nowe przerażające scenariusze kolejnych wojen światowych.
Przy tak rażącej sile jaką dysponują przestępcy, powszechne są też groźby ataków DoS i płatne odstąpienie od ataku. Właściciele serwerów lub korporacje niemal zawsze decydują się na przekazanie żądanej sumy.

Atak DoS lub w tym przypadku DDoS (Distributed Denial of Service) polega na zablokowaniu dostępu do usługi (np.. strony www) za pomocą jej wielokrotnego odpytywania. Nie było by w tym nic groźnego gdyby nie skala ataku. Większość serwerów jest w stanie wyświetlić stronę kilku tysiącom użytkowników na sekundę (to i tak już duża skala …np.. strony bankowe), w sytuacji, gdy komputerów próbujących wejść na tą stronę są miliony, nie ma żadnego zabezpieczenia przed takim atakiem. Efektem jest napis informujący o braku dostępności serwisu, lub brak jakiejkolwiek informacji. Brak działania strony internetowej dla firm to wymierne straty, liczone w milionach w przypadku takich gigantów jak Amazon.com czy chociażby onet.pl. Poniższy schemat pokazuje uproszczoną organizacje ataku. Atakujący wykorzystuje pośredników (Handlers ..np Servery IRC) do wydawania rozkazów armii zombie. Każdy z pośredników może obsługiwać nawet miliony komputerów zombie. Po otrzymaniu rozkazu wszystkie te komputery zaczynają go wykonywać (np.. Próbując wejść na stronę banku RBS) efektem jest zalew (flood) informacji od dziesiątek milionów klientów. Niemal żaden obecny system nie jest w stanie oprzeć się takiemu zalewowi. Próba obsłużenia każdego z zapytań, powoduje coraz dłuższe odpowiedzi, a w końcu ich brak. Taki atak może trwać nawet kilka dni.



Przykładowe funkcje jednego z najbardziej niebezpiecznych botnetów:



PODSTAWOWE FUNKCJE ZEUSA

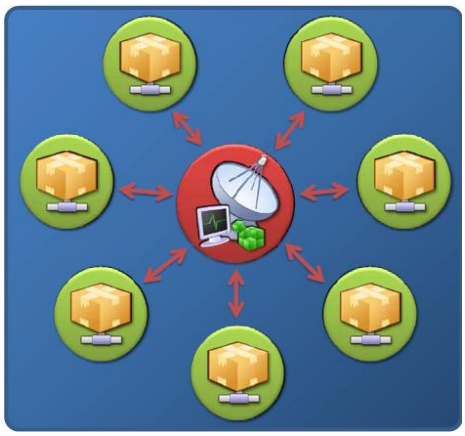
- Generator plików binarnych o zmiennej charakterystyce – trudność w wykryciu przez silniki sygnaturowe
- Szyfrowanie zawartości bota
- Szyfrowanie komunikacji bota z serwerem
- Wsparcie dla szerokiej gamy przeglądarek internetowych
- Możliwość pracy na kontach systemowych o ograniczonych uprawnieniach
- Blokowanie zapory ogniowej systemu Windows
- Możliwość zablokowania aktualizacji oprogramowania AV/AS
- „Podsłuchiwanie" przeglądarki i przechwytywanie zatwierdzanych formularzy
- Wykonywanie zrzutów ekranu zainfekowanego komputera
- Możliwość wydawania zainfekowanemu komputerowi dowolnych poleceń
- Przechwytywanie haseł zapamiętanych w przeglądarce
- Przezroczyste dla użytkownika przekierowanie na podstawioną witrynę
- Podmiana danych wpisywanych w formularzach w locie
- Przejmowanie certyfikatów
- Przechwytywanie danych uwierzytelniających dla POP3 i FTP
- Zmiana zawartości lokalnych wpisów DNS (plik hosts)
- Serwer SOCKS4

Pasted from <http://www.networld.pl/artykuly/352274_3/E.banking.na.celowniku.html>

Sieci komputerów Zombie muszą oczywiście być bardzo odporne zarówno na problemy komunikacyjne (same sobie mogą blokować funkcjonowanie) wydajnościowe a dodatkowo muszą być trudne do wytropienia i sparaliżowania. Mają więc szereg mechanizmów powodujących, że największe firmy zajmujące się bezpieczeństwem informatycznym są bezradne w powstrzymywaniu ataków BotNet.
Wpływa na to nie tylko komunikacja między agentami i centrami zarządzania, ale również złożoność technik ukrywania źródła ataku.

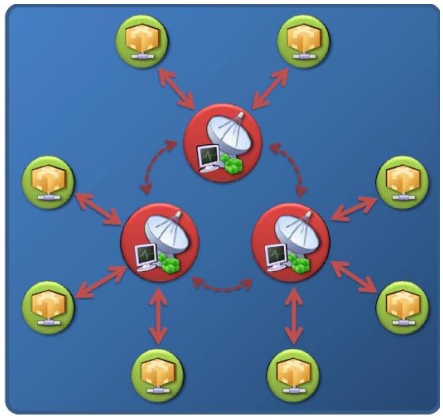
Komunikacja - opiszę szereg najbardziej popularnych topologii, oczywiście im większa sieć lub bardziej „czarne" jest jej działanie, stopień złożoności i liczba wykorzystanych mechanizmów jest większa.

Gwiazda (Star)



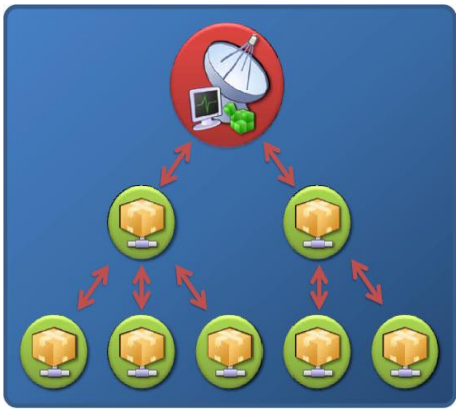
To najprostsza z topologii z tylko jednym centralnym CoC. Z oczywistych względów jest mało popularna. Łatwo jest ustalić i zablokować CoC wykorzystywana jest więc w sytuacjach gdy CoC nie musi być już potrzebne po wydaniu odpowiednich rozkazów. Zaletą jest oczywiście szybka komunikacja, gdy wrogi program "osiądzie" na komputerze ofiary i wykonuje tzw. "phone home" aby zarejestrować się jako aktywny element sieci. Może od razu otrzymać rozkazy i czekać do chwili ich planowego wykonania.

MuliServer



Rozszerzenie Gwiazdy i powielenie komputera centralnego. CoC komunikują się ze sobą informując siebie wzajemnie o swojej aktywności. Tworzą klaster. Klient podłącza się do najbliższego dostępnego CoC. Rozwiązanie bazuje na architekturze DNS i na własnym kodzie CoC. Zalety to oczywiście większa odporność CoC w przypadku próby ich blokowania oraz optymalizacja geograficzna komunikacji klientów z CoC.

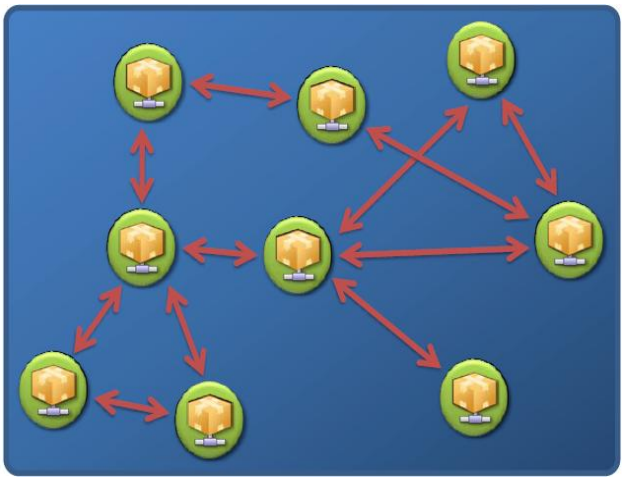
Hierarchiczna



Bardzo popularna i skuteczna metoda zarządzania sieciami (nie tylko sieciami, wiele usług IT funkcjonuje w ten sposób). Główny CoC mianuje kolejne systemy, które pośredniczą w przekazywaniu rozkazów do sieci zombie. Ta hierarchia jest niemal wymuszona przy wielomilionowych sieciach. Oczywiście możliwe są też hybrydy rozwiązań z redundantnym CoC i tysiącami pośrednich (Handlers) komputerów. Taka sieć może funkcjonować nawet w sytuacji, gdy jej duża część zostanie zablokowana (np.. Wszystkie hosty w USA przestają wykonywać rozkazy). Dzięki takiej strukturze, jest w stanie

nieustannie się powiększać i sprawnie funkcjonować nawet przy regularnym ponoszeniu strat.
Jedyną wadą jest minimalna bezwładność sieci, poprzez opóźnienia pośredników.

Losowa



Ostania opisywana topologia jest niemal nie do zniszczenia. Jest struktura jest dynamiczna i w czasie może przybierać różną postać dopasowując się do obecnej roli lub broniąc się przed uszkodzeniami. Możliwe jest też, że siec zawiera wiele różnych modeli komunikacji jednocześnie (np.. Dynamiczne Master-slave, Peer to peer). Główną cechą jest jednak brak scentralizowanego CoC, a rozkaz może być przekazana przez dowolnego zaufanego agenta sieci. Taki rozkaz jest natychmiast przekazywany do wszystkich komputerów zombie z którymi jest możliwa komunikacja. Problemem jest duża bezwładność sieci oraz możliwość wykrycia jej członków poprzez obserwację ruchu sieciowego jednego z agentów.

Jak agent znajduje CoC.

Kluczowym elementem komunikacji w większości topologii jest szybka lokalizacja CoC przez agenta. Oczywiście CoC nie może mieć stałego adresu, bo został by od razu namierzony i zablokowany. Bez odnalezienia CoC komputer zombie jest bezużyteczny więc funkcjonuje kilka mechanizmów umożliwiających odnalezienie właściwego CoC. Agent wykonuje swoją pracę i regularnie sprawdza dostępność CoC i nowych instrukcji, aby w jak najkrótszym czasie reagować na polecenia. Główne mechanizmy odnajdywania to tzw. Fluxing który występuje w dwóch typach.

IP Flux

Metoda polega na stałej zmianie adresów IP na serwerach DNS (co kilkaset milisekund). Metoda inaczej zwana Fast-Flux w bardzo krótkim czasie pod FQDN (pełną nazwę DNS) podstawić setki różnych adresów IP komputerów z różnych części świata.
Dwa typy Fast-Flux, to Single-flux i Double-flux.

Single-Flux - charakteryzuje się tysiącami adresów powiązanych z jedną nazwą domenową. Adresy te są błyskawicznie rejestrowane i derejestrowane na serwerach DNS korzystając z mechanizmu Round Robin (Multi Master) lub bardzo krótkich czasów TTL (Time to Live) wynoszących nawet milisekundy.

Double-Flux - ten mechanizm zawiera w sobie poprzedni, dodatkowo jednak wymienia jeszcze adresy serwerów DNS obsługujących daną domenę, by jeszcze trudniej było namierzyć CoC.

Domain Flux

Mechanizm Domain Fluxjest odwrotnością IP flux i polega na stałej podmianie nazwy FQDN (pełnej nazwy domenowej) na pojedyńczy adres IP lub adres atruktury CnC. Mechanizmy wykorzystywane przez tą metodę to Domain Wildcerding oraz Domain Generation Algoritm.

Domain Wildcarding - odnosi się do podstawowej funkcjonalności DNS, do użycia znaku wieloznaczności (*). Wystarczy, że zarejestrowana domena nadrzędna wskazuje na ten sam adres IP ze wszystkich swoich hostów. Dodatkowo nazwy hostów mogą być generowane losowo i funkcjonować tylko przez ułamki sekund (np.. Di2nd9**.test.pl**; u2n3fr8gtr**.test.pl**; dkdjq93**.test.pl**)
Taki zabieg często jest wykorzystywany do rozsyłania SPAMu, a fakt że host rozsyłający nigdy wcześniej nie istniał utrudnia blokowanie takiego nadawcy przez filtry antyspamowe.

Domain Generation Algoritm - to jedno z najnowszych dodatków bot agentów. Każdego dnia, generują one listę wielu adresów FQDN i umieszcza ją w swoim CnC. Żaden serwer pośredniczący nie musi znać tych nazw, a CnC może bez trudu komunikować się ze swoimi agentami. Ze względu, że lista jest aktualna tylko przez jeden dzień jeszcze trudniej niż w pozostałych przypadkach jest ustalić prawdziwy adres agenta.

Blind Proxy Redirection

Zarówno IP Flux jak i Domain Flux zapewniają duży poziom nadmiarowości oraz zdolności odtworzeniowych całej infrastruktury CnC oraz sieci agentów. Bywa jednak, że operatorzy botnetów dodają dodatkową warstwę abstrakcji, by jeszcze podnieść bezpieczeństwo i niezawodność swojej armii zombie. Ta warstwa to Blind Proxy Redirection.
Poprzez częste przekierowania całej komunikacji można sprawnie utrudnić namierzenie sieci opartej na metodach IP Flux. Do tego celu zostają zatrudnieni agenci, którzy przechwytują (proxy) cały ruch związany z poszukiwaniem domen/ip oraz ruch CnC i przekazują go dalej ukrywając prawdziwe adresy źródła zapytań. Poprzez rozproszenie agentów oraz częstą zmianę ich funkcji (lub zniszczenie po wykonanej pracy) niemal niemożliwym jest ustalenie prawdziwej lokalizacji CnC oraz pozostałych elementów sieci IP Flux.

Oczywiście zastosowanie tych wszystkich technik to spore wyzwanie dla operatora sieci botNet. Jest to stała walka z licznymi organizacjami oraz firmami, dbającymi (zarabiającymi) o bezpieczeństwo komputerów oraz zarządzanych przez nich sieci. Sama technologia stawia jednak systemy agentowe wyżej w tej rywalizacji. Poprzez wszystkie mechanizmy zabezpieczające, samoodtworzeniowe, samopowielające oraz sprawne techniki ukrywania, sprawiają, że BotNety są niemal nie do zniszczenia, można co najwyżej chwilowo zmniejszać ich zasięg i próbować zabezpieczać się przed tymi znanymi obecnie.
Kryminaliści stojący za procederem sieci, są jednak przebiegli i wyrafinowani a techniki agentowe wraz z zaawansowanymi technikami mutacji kodu i losowości powodują, że w tym wyścigu zbrojeń będą zawsze wygrywać.

Sieci bot net się popularyzują jak również komercjalizują, w linkach pod tekstem zamieściłem adresy stron, na których można się dowiedzieć nie tylko jak działają

BotNety, ale również gdzie zakupić ich funkcjonalność. Ponad to dostępne są już zestawy typu „sam zbuduj swój botnet" dostępne w Internecie jak również udostępniane z prasą fachową (np.: „Hackin9"). Można oczywiście wykorzystywać tą broń co celów testowania penetracyjnego własnej infrastruktury ale oczywiście nie tylko. Dostępne są również dedykowane serwery, na których możemy umieścić swoje własne CnC oraz szczegółowe poradniki jak zacząć zarabiać na własnych botnetach. Wszystko to wskazuje na fakt, że niedługo sieć Internet będzie musiała przejść gruntowną zmianę architektury, by odciąć się zupełnie od możliwości zabicia jej przez powszechne mechanizmy BotNetów.
Jedyną bronią, która mam nadzieje zostanie wprowadzona, będzie zmiana podejścia do wykrywania wrogich sieci, z funkcji monitorująco alarmującej na agresywną samodzielną. Z defensywnej na ofensywną. Wyobrażam sobie sieć „dobrych" agentów, przemierzających Internet w celu wykrycia, uszkodzenia i całkowitej eliminacji sieci BotNet. Ale to już kolejny scenariusz wojen agendowych na razie jeszcze fikcyjny.

Linkownia:

BotNet
http://en.wikipedia.org/wiki/Botnet
Jak działa Conficker
http://webhosting.pl/Jak.dziala.Conficker
CyberAtak na Estonię
http://wyborcza.biz/biznes/1,101562,4140556.html
Zeus:
http://www.securitystandard.pl/news/356873/Botnet.Zeus.coraz.grozniejszy.html
Więcej o DoS:
http://en.wikipedia.org/wiki/Denial-of-service_attack
Jak się komunikują BotNety:
http://www.damballa.com/downloads/r_pubs/WP%20Botnet%20Communications%20Primer%20(2009-06-04).pdf
Interes na BotNet:
http://www.egospodarka.pl/32762,Sieci-botnet-dochodowy-interes,1,12,1.html