ECLIPSE: zautomatyzowany systemy reakcji na nowe zagrożenia sieciowe

Krzysztof Cabaj*, Marek Słomnicki**, Krzysztof Szczypiorski**
* Instytut Informatyki PW, **Instytut Telekomunikacji PW
{K.Cabaj, M.Slomnicki, K.Szczypiorski}@elka.pw.edu.pl

Abstrakt

Obecna sytuacja w dziedzinie bezpieczeństwa sieciowego zmieniła sposób postępowania z zainfekowanymi (skompromitowanymi) maszynami. Aktualnie, kiedy robaki internetowe infekują tysiące maszyn w ciągu minut, reakcja na takie zagrożenie oparta jedynie na ludzkiej percepcji jest za wolna. W chronionych sieciach trzeba wdrożyć automatyczne systemy zajmujące się reakcją na tego typu naruszenia bezpieczeństwa. Potrzebny jest sposób jak najszybszego wykrycia oraz odizolowania zainfekowanej maszyny, w celu zabezpieczenia i ochrony innych zasobów. Nie można zapomnieć także o utraconym zaufaniu do organizacji, jeśli wyjdzie na jaw, że jest ona w posiadaniu zainfekowanych maszyn.

W pracy zostanie omówiony aktualnie wdrażany na Politechnice Warszawskiej autorski system wykrywania robaków internetowych powiązany z systemem reakcji w razie wykrycia zainfekowanej maszyny o nazwie **ECLIPSE** – **E**nhanced **C**ommunication p**L**atform for **I**ntrusion **P**revention **S**yst**E**m. System powstał na Wydziale Elektroniki i Technik Informacyjnych PW i jest obecnie zaimplementowany w ramach testów w jednym z domów studenckich.

Wstęp

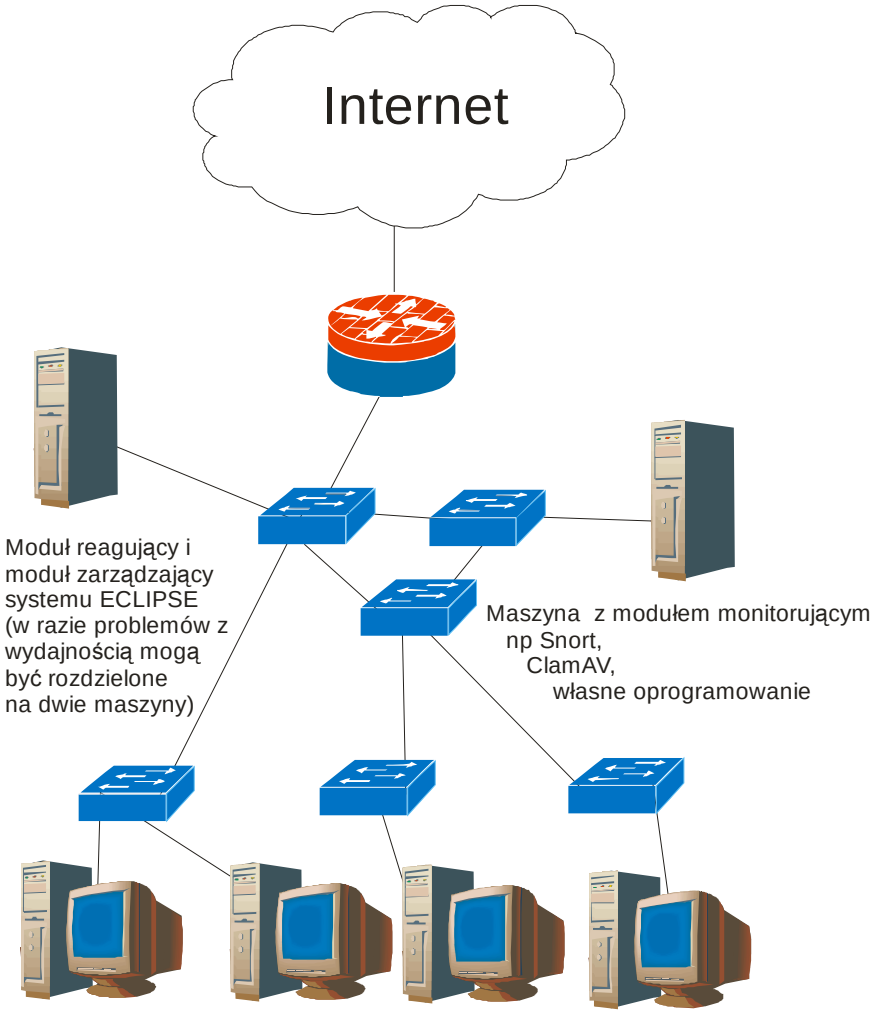
Przez ostatnie kilka lat zupełnie zmieniły się zagrożenia w sieciach komputerowych. Coraz więcej incydentów związanych z naruszeniem bezpieczeństwa spowodowanych jest **zautomatyzowanymi zagrożeniami**, a nie z bezpośrednim działaniem hakerów. Robaki internetowe, wirusy rozsyłające swój kod za pomocą poczty elektronicznej, czy różnego typu oprogramowanie szpiegujące coraz częściej atakują chronione sieci. Prędkość, z jaką infekują nowe ofiary powoduje, że ręczna reakcja operatorów systemów bezpieczeństwa jest zbyt wolna. Jedynie automatycznie czy też półautomatycznie działające systemy są w stanie sprostać nowym zagrożeniom. Oczywiście wraz z rozwojem oraz zmianą zagrożeń ewoluują także systemy bezpieczeństwa. Coraz częściej zamiast zapór ogniowych i systemów IDS instaluje się systemy IPS. Systemy te mają na celu automatycznie reagować na incydenty i od razu blokować podejrzaną aktywność, aby nie dopuścić do infekcji. Jednak aktualnie dostępne na rynku rozwiązania nie spełniają wystarczająco swojej roli. Po pierwsze ruch podlega analizie jedynie w kilku wybranych miejscach sieci. W wielu przypadkach, z powodów finansowych jest to styk sieci chronionej, danej instytucji a Internetu. Po drugie aktualne systemy blokują podejrzaną aktywność tylko w wybranych punktach, tam gdzie zainstalowany jest system IPS. Zainfekowana maszyna nie zostaje usunięta z sieci a jedynie blokowana na urządzeniu. Najczęściej polega to na filtrowaniu całego ruch z tej maszyny, przechodzącego przez system IPS. Takie działanie nie odciąża sieci, która musi przenosić duże ilości niepotrzebnego ruchu a także stanowi niebezpieczeństwo dla innych maszyn znajdujących się w sieci.

Zaprojektowany, aktualnie wdrażany i testowany, a prezentowany w tej pracy system należy do następnej generacji systemów bezpieczeństwa mających rozwiązać opisane wcześniej problemy.

System nie tylko ma większe możliwości analizy ruchu sieciowego, ale co ważniejsze i niespotykane w aktualnych systemach trwale usuwa zainfekowane maszyny z sieci. Usunięcie maszyny polega na przełączeniu najbliższego zainfekowanej maszynie portu sieciowego w tryb shutdown. System ten jest całkowicie związany z architekturą sieciową i jest implementacją wizji systemu IPS zanurzonego w infrastrukturze (infrastructure IPS).

Opis systemu ECLIPSE

Zaprojektowany przez nas system ma spełniać **dwa główne zadania**. **Po pierwsze wykrywać**, a po **drugie szybko usuwać z chronionej sieci niepożądane maszyny**. Decyzję o odłączeniu maszyny można podejmować na wiele sposobów. Ponieważ istnieje duża dowolność doboru metody wykrywania naruszeń, zaprojektowany system ECLIPSE może współdziałać z wieloma, już wdrożonymi systemami bezpieczeństwa. W tym celu można zastosować znane od wielu lat rozwiązania takie jak systemy antywirusowe (AV) czy systemy wykrywania włamań (IDS). Jednak takie podejście nie różni się od aktualnie wdrażanych systemów IPS. Ciekawym zagadnieniem, opisanym w dalszej części pracy, jest wykorzystanie do wykrywania naruszeń całej infrastruktury budującej chronioną sieć.



O wiele ciekawszym wydaje się problem związany z odnalezieniem i odłączeniem podejrzanej maszyny z chronionej sieci. Zagadnienie to jest w szczególności niebanalne dla dużych sieci komputerowych budowanych w oparciu o całkowicie przełączany w warstwie drugiej szkielet sieci.

System ECLIPSE składa się z trzech podstawowych modułów. Najważniejszy moduł - moduł reagujący, odpowiedzialny jest za znalezienie i odłączenie podejrzanej maszyny. Moduł ten przyjmuje zlecenia od modułów monitorujących mających na celu odłączenie od sieci maszyny o określonym adresie IP czy MAC. Jak było opisane wcześniej zlecenia o wyłączeniu mogą być wygenerowane przez inne, także zewnętrzne systemy. Ostatnim modułem systemu jest moduł zarządzający. Ponieważ system aktualnie jest w trakcie wdrażania moduł ten jest aktualnie w fazie intensywnego rozwoju. Jego zadaniem jest prezentacja w wygodnej dla administratora formie wszystkich zdarzeń związanych z działaniem systemu oraz umożliwienie konfiguracji. Przykładowo za jego pomocą można kontrolować adresy kluczowych dla działania instytucji maszyn, które nigdy nie mogą być automatycznie odłączone.

Część reagująca

Część reagująca wydaje się być najciekawszym rozwiązaniem w systemie ECLIPSE, które nie zostało jak dotąd zaimplementowane w żadnym komercyjnym czy OpenSource'owym systemie. Maszyna, która zostanie przez system sklasyfikowana jako zainfekowana, czy skompromitowana zostaje całkowicie usunięta z sieci. Usunięcie polega na wyłączenie interfejsu najbliższego jej podłączeniu do sieci. W wypadku, gdy taka maszyna jest podłączona bezpośrednio za pomocą zarządzanego urządzanie zostanie wyłączona jedynie ona. W wypadku podłączenia maszyny przez urządzanie niezarządzalne lub niewłączone do systemu ECLIPSE np. koncentrator (hub) zostaje cały odłączony.

Wydaje się, że odłączenie zainfekowanej maszyny nie jest problemem. Oczywiście zagadnienie to jest banalne, jeśli mówimy o małych sieciach z jednym przełącznikiem. Jednak przy większych instalacjach z dziesiątkami przełączników tworzących szkielet i tysiącami maszyn nie jest to już zadanie proste. Aby zrozumieć problem, jakim jest odłącznie np. zainfekowanej maszyny trzeba opisać jak budowane są współczesne duże sieci komputerowe. Coraz częściej stosuje się instalacje ze szkieletem przełączanym w warstwie drugiej. Oznacza to, że większość urządzeń aktywnych w sieci to przełączniki (switche). W takich instalacjach w przypadku skrajnym może występować jeden router (instalacje typu router-on-the-stick). Taka budowa sieci jest efektem dwóch czynników. Po pierwsze przełączniki jako urządzenia warstwy 2 zawsze były szybsze, wiąże się to z mniejszą liczbą operacji potrzebnych do analizy adresów MAC w przeciwieństwie do analizy adresów warstwy 3 np. IP. Z tego powodu częściej są to urządzenia oparte na specjalizowanych szybszych układach elektronicznych (ASIC). Po drugie wzrost prędkości i zasięgów technologii używanych w sieciach lokalnych. Nowsze wersje używanego Ethernetu takie jak Gigabit Ethernet czy 10Gigabit Ethernet wyeliminowały potrzebę używaniu specjalnych technologii sieciowych do zapewnienia odpowiednich przepustowości jak i zasięgów. W zastosowaniach czysto komputerowych, technologia ta często wyeliminowała ATM. Dodatkowo zastosowanie przełączników z zaimplementowanym protokołem drzewa rozpinającego (STP) pozwala na budowę sieci z redundantnymi połączeniami. Dzięki temu można dzisiaj budować sieci, które szybko reagują na uszkodzenia łączy czy urządzeń. Sieć Ethernet z protokołem rapidSTP jest w stanie zareagować na uszkodzenie w czasie około 15 s. Wszystkie te czynniki spowodowały problemy z identyfikacją miejsca, urządzenia i portu gdzie maszyna o danym adresie MAC czy IP jest podłączona do sieci.

Szybkie odłączenie określonej maszyny od sieci nie jest zadaniem trywialnym. Sprawę oczywiście komplikuje liczba urządzeń, które trzeba przeszukać. Jednak większym problemem mogą być zmieniające się dynamicznie aktywne połączenia. W razie uszkodzenia łącza uruchamiana jest na przełącznikach procedura budowy drzewa rozpinającego, mająca na celu wyeliminowanie pętli i umożliwienie transmisji za pomocą nadmiarowych łączy. Wynikiem działania algorytmu mogą być

zmiany topologii. Z tego powodu w naszym projekcie staraliśmy się maksymalnie zmniejszyć ilość informacji dotyczących architektury sieci, jakie trzeba podać w celu poprawnej pracy systemu. Administrator nie musi wprowadzać do systemu całego opisu sieci wraz ze wszystkimi połączeniami. Do poprawnej pracy potrzebne są jedynie adresy IP urządzeń i dane pozwalające na zalogowanie się do nich. Wszystkie inne informacje na temat sieci, między innymi jej aktualna topologia, są automatyczne zbierane z urządzeń. Takie podejście pozwala na szybkie reakcje spowodowane zmianami w architekturze, oraz maksymalnie odciąża administratora.

W momencie wykrycia podejrzanej, np. zainfekowanej robakiem maszyny, największe znaczenie ma czas, w jakim system zlokalizuje ją i wyłączy. Trzeba pamiętać, iż część zainfekowanych maszyn rozpoczyna skanowanie z prędkością, która powoduje duże obciążenie urządzeń sieciowych oraz może powodować zapełnienie buforów i uniemożliwienie transmisji nowych danych na przeciążonych łączach. Dlatego warto, aby system działał w całkowicie odizolowanej od użytkowników sieci zarządzania. W celu przyspieszenia działania moduł reagowania działa w dwóch trybach. Tryb podstawowy polega na natychmiastowym zlokalizowaniu urządzenia i portu, do którego podłączona jest maszyna o określonym adresie MAC. W celu wyszukania odpowiedniego portu rozpoczyna się odpytanie kolejnych urządzeń czy w swoich tablicach adresów MAC nie znajduje się wyszukiwany. Jeśli nie, procedura jest powtarzana dla kolejnego urządzenia. Teoretycznie może być to dowolny, wybrany losowo przełącznik. Jednak wybieranie urządzeń ze szkieletu zwiększa prawdopodobieństwo znalezienia adresu za pierwszym razem. W momencie wykrycia adresu na urządzeniu mogą być podjęte czynności dwojakiego rodzaju. Jeśli port skojarzony z tym adresem jest podłączony z innym przełącznikiem procedura zostaje powtórzona na kolejnym przełączniku. W innym wypadku następuje wyłączenie portu. Drugi tryb pracy modułu ma na celu zwiększenie prędkości znajdowania maszyn. Cyklicznie przeglądane są wszystkie urządzenia i tworzona jest baza aktualnie używanych maszyn wraz z ich adresami i dokładną informacją na temat miejsca podłączenia. Dzięki temu trybowi pracy, jeśli maszyna została włączona wcześniej i wysyłała jakieś dane zostaje znaleziona praktycznie natychmiast. Jeśli podanego adresu nie ma w bazie, następuje wyszukanie go za pomocą pierwszej opisanej powyżej procedury.

Część monitorująca

Ta część systemu odpowiedzialna jest za wykrywanie zainfekowanych maszyn, które powinny zostać natychmiast odłączone od sieci. Jak opisaliśmy wcześniej system reagujący może współpracować z różnymi systemami bezpieczeństwa. W instalacji pilotażowej w jednym z akademików Politechniki Warszawskiej opisywany system współpracował z systemem wykrywania włamań Snort oraz skanerem antywirusowym ClamAV. Jednak przy takim podejściu działanie całości systemu przypominało klasyczne systemy IPS. Różnica dotyczyła jedynie tego, iż zainfekowana czy skompromitowana maszyna była odłączana fizycznie, a nie blokowana np. na zaporze ogniowej.

Zmiany trendów związanych z bezpieczeństwem wymagają zupełnie innego podejścia do projektowania. Dzisiaj aspekty związane z bezpieczeństwem sieci muszą być brane pod uwagę już podczas jej projektowania. W takim projekcie urządzenia zapewniające bezpieczeństwo nie są dodatkiem do urządzeń służących tylko i wyłącznie przesyłaniu danych. Każde urządzenie aktywne w sieci staje się elementem systemu bezpieczeństwa. Możemy mówić o rozwiązaniach typu IPS zanurzony w infrastrukturze. W prezentowanym poniżej rozwiązaniu zostaną opisane możliwości wykorzystania funkcji inteligentnych przełączników oraz routerów jako sensorów systemu ECLIPSE. W opisywanym poniżej rozwiązaniu, moduł system ECLIPSE służy do wykrywania maszyn zainfekowanych robakami internetowymi.

Stwierdzenie czy dana maszyna jest zainfekowana, odbywa się na podstawie wystąpienia pewnych czynników, charakterystycznych dla infekcji robakiem internetowym. Zastosowaliśmy podejście polegające na wykrywaniu anomalii a nie sygnaturowe. Dzięki temu system powinien być w stanie wykryć nie tylko aktualnie znane, ale także nowe robaki.

Na podstawie analizy działania większości robaków ustaliliśmy zestaw zachowań świadczących o infekcji. W aktualnym rozwiązaniu wybraliśmy najprostsze zdarzenia mogące świadczyć o infekcji. Wybór ten ma na celu wykorzystanie jak największej liczby urządzeń jako sensorów. Takie podejście pozwala wykryć szybko każdą zainfekowaną maszynę, ponieważ każda transmisja podlega analizie. W naszym rozwiązaniu bazujemy na możliwościach urządzeń sieciowych do wykrywania i blokowania określonego ruchu. Wykorzystujemy do tego celu listy kontroli dostępu. Za ich pomocą wykrywamy próby komunikacji, które nie powinny być wywołane przez normalną pracę użytkowników. Aby zrozumieć, w jaki sposób prosta lista kontroli dostępu może wykryć infekcje należy przyjrzeć się, w jaki sposób wybierane są przez robaka adresy maszyn do skanowania i ewentualnej infekcji.

Większość znanych robaków generuje adresy potencjalnych ofiar bazując na adresie aktualnie zainfekowanej maszyny. Najczęściej generowanie nowych adresów polega na zastąpieniu ostatnich oktetów adresu losowymi wartościami. Działanie takie jest podyktowane tym, że maszyny o „bliskich" adresach mogą posiadać identyczne oprogramowanie. Mimo prostoty założenia takie podejście świetnie sprawdza się w wielu instytucjach powodując bardzo szybkie, masowe infekcje wielu maszyn. Przykładowo robak Sasser wybierał adresy w następujący sposób (`http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html`). W 25% przypadków pozostawiał 2 pierwsze oktety adresu IP bez zmiana a losował dwa ostatnie. W 23% przypadków pozostawiał jedynie pierwszy oktet a losował 3 oktety. W pozostałych 52% przypadków cały adres był wybierany losowo.

Korzystając z tej wiedzy możemy próbować wykrywać zainfekowane maszyny, jako takie, które próbują komunikować się z nieprzydzielonymi adresami w naszej puli adresowej. Oprócz tego możemy za podejrzane uznać wszelkie próby komunikacji protokołu TCP na adresy IP, które w chronionej sieci odpowiadają adresom sieci i adresom rozgłoszeniowym. Za podejrzane można uznać także wszelką komunikacje do sieci o adresacji prywatnej (RFC1918), która nie jest używana w naszej sieci.

Technicznie wykrycie tego typu zdarzeń polega na utworzeniu odpowiednich list kontroli dostęp na urządzeniach sieciowych. Dzisiaj praktycznie jest to możliwe na każdym routerze i coraz częściej możliwe jest to na nowszych, „inteligentniejszych" przełącznikach. Listy służące do wykrywania infekcji powinny logować wykryte zdarzenia. Na podstawie analizy logów podejmowana jest decyzja o wyłączeniu określonej maszyny. W celu działania systemu w czasie rzeczywistym logi z urządzeń wysyłane są w formacie zgodnym z programem syslog do modułu systemu ECLIPSE zajmującego się analizują zdarzeń związanych z bezpieczeństwem. W razie wystąpienia zdarzenia polegającego na zablokowaniu transmisji przez wspomniana listę kontroli dostępu maszyna, która spowodowała wygenerowanie tego zdarzenia, zostaje uznana za zainfekowana. Automatycznie rozpoczyna się procedura odłączenia jej od sieci.

Opisana powyżej metoda jest możliwa do zastosowania w praktycznie każdej sieci. W wypadku, gdy dla sieci jest zdefiniowana odpowiednia polityka bezpieczeństwa ilość sprawdzanych, podejrzanych zdarzeń może zostać zwiększona. Często przez współczesne robaki internetowe wykorzystywane są protokoły IRC oraz TFTP. W sieci organizacji, której pracownicy nie potrzebują wykorzystywać tych protokołów pojawienie się ich można uznać jako objaw infekcji. W takim wypadku można dodać do list kontroli dostępu wpisy wykrywające połączenia na porty skojarzone z tymi protokołami. Niestety nie można tego zastosować w sieci akademickiej gdzie użycie tych protokołów jest całkowicie legalne.

Poniżej znajduje się przykładowa lista kontroli dostępu dla sieci klasy C 192.168.1.0 która została podzielona na 4 podsieci. Oprócz tych adresów żadne inne adresy prywatne nie są używane w monitorowanej sieci. Przyjęliśmy zasadę, że podejrzany ruch od razu będzie blokowany. Na początku wykrywamy wszystkie próby połączeń na adresy prywatne klas A i B.

```
access-list 102 deny ip any 10.0.0.0 0.255.255.255 log
access-list 102 deny ip any 172.16.0.0 0.7.255.255 log
```

Dalej wyłapujemy wszystkie odwołania do adresów IP będących adresami poszczególnych podsieci oraz adresami rozgłoszeniowymi dla nich. Tym razem wybraliśmy jedynie protokół TCP. Często pakiety UDP wysyłane na adresy rozgłoszeniowe są całkowicie legalne. Przykładowo tego typu pakiety wysyłają maszyny działające pod kontrolą systemu Microsoft Windows.

```
access-list 102 deny tcp any host 192.168.1.0 log
access-list 102 deny tcp any host 192.168.1.63 log
access-list 102 deny tcp any host 192.168.1.64 log
access-list 102 deny tcp any host 192.168.1.127 log
access-list 102 deny tcp any host 192.168.1.128 log
access-list 102 deny tcp any host 192.168.1.191 log
access-list 102 deny tcp any host 192.168.1.192 log
access-list 102 deny tcp any host 192.168.1.255 log
```

W dalszej części tej listy wyłapujemy wszystkie próby komunikacji na niezaalokowane przez nas adresy. Niestety w tym miejscu trzeba wpisać wszystkie adresy. Pomocne może być zastosowanie skanera sieciowego (przykładowo programu nmap) i odpowiedniego skryptu.

```
access-list 102 deny ip any host 192.168.1.33 log
access-list 102 deny ip any host 192.168.1.58 log
access-list 102 deny ip any host 192.168.1.97 log
…
```

Poniższe dwa zapisy służą wyłapaniu transmisji do innych sieci o adresacji prywatnych. Na początku zezwalamy na całą komunikacje do sieci 192.168.1.0 – wszystkie nielegalne adresy zostały już wcześniej w przedstawionej liście wykryte i zablokowane. Dalej blokujemy dostęp do wszystkich pozostałych 254 sieci klasy C. Oczywiście na końcu nie możemy zapomnieć o zezwoleniu innego ruchu, który według naszych wcześniejszych założeń uważamy za całkowicie legalny.

```
access-list 102 permit ip 192.168.1.0 0.0.0.255
access-list 102 deny ip 192.168.0.0 0.0.255.255 log
access-list 102 permit any any
```

Przedstawiona, powyżej lista kontroli dostępu może znaleźć zastosowanie w praktycznie dowolnej sieci. Za jej pomocą są wyłapywane wszelkie podejrzane próby transmisji. W sieciach gdzie polityka bezpieczeństwa jest wdrożona można dodać jeszcze inne zdarzenia. W zależności od restrykcyjności polityki może być ich mniej lub więcej. Przykładowo poniżej znajdują się dwie reguły, które wykrywają często przez robaki wykorzystywane protokoły IRC i TFTP

```
access-list 102 deny tcp any any range 6666 6677 log
access-list 102 deny udp any any eq 69
```

Przyszłość systemu

Aktualnie po znalezieniu maszyny port za pomocą, którego jest podłączona zostaję wyłączony (zostaje przełączony w tryb shutdown). W dalszych pracach planujemy rozwiązanie mniej drastyczne, i oszczędzające czas administratorów. Podejrzana maszyna zostanie przeniesiona do odpowiedniego

VLAN'a w którym możliwe jedynie będzie pobranie narzędzi służących do wyczyszczenia maszyny oraz aktualnych łat i szczepionek dla systemów antywirusowych. Po wyczyszczeniu systemu, zaktualizowaniu całego oprogramowania oraz sygnatur systemów antywirusowych maszynę będzie można poddać zdalnemu sprawdzeniu. Jeśli okaże się, że jest ona „czysta" będzie następowało automatyczne włączenie jej do normalnego użytkowania. Oczywiście rozwiązanie to można stosować przy założenie odpowiedniego poziomu wiedzy użytkowników oraz dla systemów nieprzetwarzających kluczowych dla danej organizacji danych.

Podsumowanie

Zaprezentowany w niniejszej pracy system jest odpowiedzią na ewoluujące niebezpieczeństwa występujące w dzisiejszych sieciach teleinformatycznych. Ponieważ coraz częściej spotykamy się ze zautomatyzowanymi zagrożeniami, także systemy chroniące muszą działać (przynajmniej częściowo) bez udziału człowieka. Odłączenie zainfekowanej, czy też będącej pod kontrolą włamywacza maszyny całkowicie chroni pozostałe zasoby. Poza tym takie działanie znacznie odciążą całą infrastrukturę sieciową w wypadku nagłej infekcji wielu maszyn. Ma to szczególne znaczenie dla dużych sieci podczas ataków nowych robaków, kiedy to ilość ruchu generowanego przez zainfekowane maszyny całkowicie rujnuje zasoby sprzętowe. Przeciążona sieć nie pozwala na przesłanie jakichkolwiek danych oraz komend, także tych potrzebnych do analizy zagrożenia i powrotu do normalnego działania systemu teleinformatycznego.

Mamy nadzieje, że system ECLIPSE w dużym stopniu może pomóc zabezpieczać sieci eliminując zainfekowane maszyny. Pragniemy, aby zastosowanie sytemu ECLIPSE częściowo przyćmiło zagrożenie, jakim wciąż pozostają robaki internetowe.