Zaawansowane trwałe zagrożenia: to nie jest przeciętne szkodliwe oprogramowanie

Twoja firma niekoniecznie musi być celem, ale Ty nadal jesteś zagrożony!

kaspersky.pl/beready

KASPERSKY lab

Wprowadzenie

1.0

„APT (ang. Advanced Persistent Threat), czyli zaawansowane trwałe zagrożenia i ataki zero–day są wszechobecne i nieubłaganie zmuszają małe i średnie organizacje do zakwestionowania ich obecnego paradygmatu bezpieczeństwa".

Znaną regułą w dziedzinie ochrony informacji jest to, że każdy użytkownik i każde urządzenie musi zmierzyć się z tymi samymi zagrożeniami, płynącymi ze strony szkodliwego oprogramowania. Przez lata złośliwe programy ewoluowały – od narzędzi wykorzystywanych przez cyberwandali do niszczenia danych i czynienia ogólnych strat w systemach ofiar, do narzędzi używanych przy kradzieży tożsamości, kampaniach cyberszpiegowskich i działaniach cyber-wojennych, sponsorowanych przez rządy wrogich państw.

Problem się powiększa, ponieważ wzrasta liczba urządzeń mobilnych na punktach końcowych i coraz częściej działają one poza kontrolą bezpieczeństwa korporacyjnego. Ryzyko jest ogromne – świadczy o tym poziom zaawansowania rozwijającego się szkodliwego oprogramowania, używanego w połączeniu z zaawansowanymi trwałymi zagrożeniami (APT), które infiltruje sieci firmowe, rozpoczynając od punktów końcowych i nośników wymiennych.

Dobrym przykładem nowych zagrożeń jest Flame, cyberszpiegowski robak, który zaatakował irański sektor energetyczny i rozpowszechnił się na całym Bliskim Wschodzie. Wykryty przez Kaspersky Lab robak Flame*[1] nazywany jest „najbardziej wyrafinowaną cyberbronią, jaka została wynaleziona do tej pory". Mimo ścisłego ukierunkowania Flame'a na projekty nuklearne Iranu, eksperci ds. bezpieczeństwa obawiają się, że zagrożenie to rozprzestrzenia się poza swoim pierwotnym obszarem zainteresowań i infekuje systemy korporacyjne na całym świecie. Przed Flamem mieliśmy do czynienia ze Stuxnetem, który został zaprojektowany specjalnie do infekowania i zakłócania systemów SCADA (ang. Supervisory Control and Data Acquisition), kontrolujących wirówki do wzbogacania uranu w irańskich elektrowniach. Szkodliwe oprogramowanie okazało się niezwykle skuteczne w wymuszaniu niekontrolowanej pracy urządzeń, co bezpośrednio wiodło do ich zniszczenia. Na nieszczęście Stuxnet wydostał się poza irańskie instalacje atomowe i rozpoczął infekowanie systemów SCADA w Niemczech, a ostatecznie w innych częściach świata. Zarówno Flame, jak i Stuxnet, są zaawansowanymi trwałymi zagrożeniami – cyberbroniami działań wojennych nowej generacji, sponsorowanymi przez rządy, terrorystów lub majętne syndykaty cyberprzestępcze. Wyposażone w szereg zdolności ukrywających ich działanie, są zaprogramowane do koncentrowania się na własności intelektualnej, planach wojskowych i innych cennych zasobach korporacyjnych. Jednak, największą ofiarą tej wojny będzie prawdopodobnie rynek małych i średnich przedsiębiorstw, który znajdzie się w krzyżowym ogniu, jeśli nie opracuje kompleksowej infrastruktury zabezpieczeń punktów końcowych.

Dobiegły końca dni, w których małe i średnie firmy mogły cieszyć się anonimowością i traktować systemy bezpieczeństwa „po macoszemu". Zagrożenia APT i ataki zero-day są wszechobecne i nieubłaganie zmuszają małe oraz średnie organizacje do zakwestionowania ich obecnego paradygmatu bezpieczeństwa. Bezpieczeństwo sieci jest ważne, ale w żadnym wypadku nie można zaniedbać ochrony punktów końcowych.

Przedsiębiorstwa mają wiele opcji zabezpieczeń, takich jak oferowane przez Kaspersky Lab antywirusowe rozwiązania bezpieczeństwa. Obszerne pakiety zabezpieczające, pozwalają kompleksowo przygotować firmy zarówno na istniejące zagrożenia, jak również na nadciągające, dotychczas nieznane zagadki przyszłości.

W niniejszym artykule przyjrzymy się rosnącej liczbie ataków APT i zagrożeniom zero-day nękającym punkty końcowe, opcjom zabezpieczeń dostępnych dla małych, średnich i dużych firm oraz w jaki sposób Kaspersky Endpoint Security 8 zapewnia doskonałą ochronę przed pospolitymi i zaawansowanymi zagrożeniami.

[1] Flame: Pytania i odpowiedzi, Aleksander Gostiew, VirusList.pl, 30 maja 2012 r.

Ataki APT: to nie jest przeciętne szkodliwe oprogramowanie

2.0

„Cyberprzestępcy wprowadzają wyrafinowane szkodliwe oprogramowanie do arsenału narzędzi używanych przy polowaniach na ściśle spersonalizowane informacje, dotyczące indywidualnych celów. Informacje te są wykorzystywane później w drugim stadium ataku".

Kiedyś zagrożenia bezpieczeństwa dystrybuowane były luzem, zazwyczaj za pośrednictwem wiadomości e-mail. Ofiara zazwyczaj była mamiona wiadomościami od zamorskiego finansisty lub dawno zaginionego krewnego. Mimo że potencjalnie dość szkodliwe, zagrożenia te były bardzo prymitywne, łatwe do wykrycia i możliwe do neutralizacji za pomocą podstawowej infrastruktury bezpieczeństwa IT.

Tego rodzaju ataki są cały czas powszechne. Ostatnio jednak – to, co wywołuje strach, sensację i podnosi dramatyzm – to zagrożenia APT i ataki zero-day.

W ciągu ostatnich kilku lat lista najbardziej znanych ataków APT zaskoczyła nawet najbardziej kreatywnych scenarzystów:

- Operacja Aurora (Google): ten atak (wywodzący się z Chin) w 2009 r. wykorzystywał podatności przeglądarki Internet Explorer do pozyskania kodu źródłowego i innych własności intelektualnych firmy Google i około trzydziestu innych globalnych korporacji.
- RSA: atak, który spowodował naruszenie tokenów firmy (SecurID), pozwolił cyberprzestępcom w 2011 r. zinfiltrować amerykańskich dostawców wojskowych: Lockheed Martin, Northrop Grumman i L3 Communications.
- Incydent w Oakridge National Laboratories: laboratorium Departamentu Energii było zmuszone przejść do trybu offline, gdy administratorzy odkryli, że krytyczne dane wyciekły z serwera za sprawą ataku phishingowego.
- GhostNet: cyberszpiegowska sieć (złożona z 1 295 zainfekowanych hostów w 103 krajach) została skierowana przeciwko zwolennikom wolnego Tybetu i innym celom o wysokiej wartości, wliczając w to: lokalne ministerstwa, komisje spraw zagranicznych, ambasady, organizacje międzynarodowe i organizacje pozarządowe (NGO).
- ShadyRat: ta wysokiej klasy kampania hakerska objęła rządy określonych państw, organizacje non-profit i globalne korporacje. Jej żniwo to 70 ofiar w 14 krajach.

W obecnych czasach zagrożenia APT oraz exploity zero-day idą ramię w ramię i cieszą się niesłabnącym zainteresowaniem mediów. Tak więc czym one naprawdę są i co odróżnia je od zwykłych trojanów czy robaków?

Bezpiecznie jest powiedzieć, że nie są to przeciętne ataki uskuteczniane przez „domorosłych hakerów". Tak jak wskazuje nazwa, zagrożenia APT polegają na zaawansowanej technologii, jak również na wielu metodach i różnych wektorach ataku. Wszystko po to, by dotrzeć do konkretnych organizacji w celu pozyskania określonych, niejawnych informacji.

W odróżnieniu od „dzieciaków skryptowych" bawiących się we wstrzykiwanie SQL – czy średnio zaawansowanych autorów szkodliwego oprogramowania, wynajmujących za ogromne pieniądze botnety w celu dystrybucji swoich „dzieł" – mózgi operacji APT wydają się być wysoce zorganizowanymi syndykatami cyberprzestępczymi, dysponującymi zespołami ekspertów i posiadającymi na wyciągnięcie ręki cały wachlarz technik wywiadowczych i szpiegowskich. Dzięki zdolnościom ukrywania szkodliwej działalności i wykorzystaniu metody powolnego ataku na niskim poziomie, zagrożenia APT stały się naturalnie wybieranym narzędziem dla cyberszpiegów, wrogich rządów, terrorystów i karteli cyberprzestępczych ukierunkowanych na krociowe zyski.

„W głównej fazie ataku APT, do infekcji sieci wykorzystywana jest dowolna liczba wyrafinowanych trojanów, robaków i innych wyspecjalizowanych szkodników".

Oto, jak to typowo przebiega:

Dzięki zagrożeniom APT cyberprzestępcy celują w indywidualne podmioty, wprowadzając do użytku szkodliwe oprogramowanie, które poluje na ściśle spersonalizowane informacje, wykorzystywane w drugiej fazie ataku. Od tego momentu APT polega na starannie przygotowanej socjotechnice i rozpoczyna próby infiltracji organizacji poczynając od jej najsłabszego ogniwa - użytkownika końcowego.

Podczas tej fazy ataku działania są ukierunkowane na kluczowe osoby z dostępem do znanych kont docelowych. Osoby te atakowane są przekonującymi wiadomościami e-mail, które wydają się pochodzić np. z działu zasobów ludzkich lub innego zaufanego źródła. Dzięki jednemu beztroskiemu kliknięciu, cyberprzestępcy dostają swobodny dostęp do najcenniejszych informacji o danej organizacji i nikt nie jest tego świadomy!

W głównej fazie ataku APT, do infekcji sieci wykorzystywana jest dowolna liczba wyrafinowanych trojanów, robaków i innych wyspecjalizowanych szkodników, do systemów wprowadza się wiele backdoorów, które prawdopodobnie pozostaną na komputerach użytkowników i serwerach na zawsze. W tym czasie zagrożenie przenosi się niepostrzeżenie z jednego hosta na drugi – pozostaje cały czas w ukryciu, co pozwala mu wytropić sprecyzowany wcześniej cel.

Cel ataku: luki zero–day

3.0

„Rok 2011 zakończył się z przynajmniej 535 incydentami wycieku danych. Skradziono łącznie 30,4 mln. rekordów danych".

Narzędziami domyślnie wybieranymi do realizacji ataku APT są bezsprzecznie exploity dla luk zero-day. Te tak trafnie nazwane zagrożenia w dosłowny sposób wykorzystują podatności w oprogramowaniu, zanim producent zdąży opublikować odpowiednie poprawki „uszczelniające" aplikację, lub zanim nawet zda sobie sprawę z istnienia takiej, czy innej podatności w swoim produkcie. Czas od pierwszego ataku do wydania poprawki (tzw. „łaty") wyznacza granice „okna zero-day" – swoistego cyberprzestępczego „hulaj dusza, piekła nie ma". Bez obaw przed konsekwencjami cyber-przestępcy czerpią zyski i satysfakcję z ataku, na który pozornie nie ma żadnej znanej obrony.

Szkodliwe oprogramowanie, które wykorzystuje luki zero-day może niepostrzeżenie siać spustoszenie w infrastrukturze organizacji, żerując na zastrzeżonych informacjach, takich jak: kody źródłowe, własności intelektualne, plany wojskowe, dane związane z obroną narodową oraz inne tajemnice rządowe, używane w działalności szpiegowskiej. Kiedy atak zostanie ujawniony, konsekwencje są koszmarem speców od PR-u. Koszmarem przynoszącym milionowe straty – od kosztów związanych z remontami infrastruktury bezpieczeństwa IT, poprzez modernizację sprzętu, a na kosztach postępowania sądowego i odszkodowaniach dla klientów kończąc. Dochodzą do tego niepoliczalne koszty niezbędne do odbudowy reputacji i odzyskania zaufania konsumentów!

Zagrożenia APT i exploity zero-day nie są niczym nowym i znane były lata temu – dużo wcześniej niż stały się zmorą specjalistów ds. bezpieczeństwa. Wiele organizacji nie zdaje sobie sprawy, że zostały trafione atakiem APT lub zero-day – dowiadują się o tym miesiące, a nawet lata później. Zgodnie z raportem firmy Verizon*[2]: 44% wycieków danych, obejmujących własności intelektualne, zostało wykryte dopiero po kilku latach. Christian Science Monitor*[3] ogłosił, że trzy kompanie naftowe – ExxonMobil, Marathon Oil oraz ConocoPhilips – były ofiarami ukierunkowanych cyberataków APT, których początek datuje się na rok 2008. Podczas tych ataków, które prawdopodobnie pochodziły z Chin, cyberprzestępcy zdołali wyprowadzić na zdalny serwer krytyczne informacje branżowe na temat ilości, wartości i miejsc odkrycia ropy naftowej na całym świecie. Jednakże, wspomniane firmy odkryły ataki dopiero wtedy, gdy FBI poinformowało je, że ich zastrzeżone informacje zostały skradzione.

W 2011 r. zagrożenia APT odnalazły swoje miejsce w wielkim łańcuchu pokarmowym bezpieczeństwa informatycznego. Zaawansowane trwałe zagrożenia stały za największymi stratami poniesionymi w 2011 r. przez Sony, Epsilon, HBGary i DigiNotar, oraz doprowadziły do utraty przez RSA ok. 40 milionów tokenów z jednorazowymi hasłami (OTP). Stwierdzono, że naruszenie mechanizmów bezpieczeństwa RSA*[4] kosztowało firmę około 66 milionów dolarów, podczas gdy utrata przez Sony*[5] bazy danych ze 100 milionami wpisów została oszacowana na 170 milionów dolarów amerykańskich. Rok 2011 zakończył się z przynajmniej 535 incydentami wycieku danych, w których skradziono łącznie 30,4 mln. rekordów danych. Zgodnie z informacjami Privacy Rights Clearinghouse*[6], wiele z tych wycieków było spowodowanych niektórymi z najbardziej sensacyjnych ataków. To tylko ułamek znanych naruszeń bezpieczeństwa, ponieważ istnieją tysiące przypadków, które każdego roku przechodzą niezauważone lub pozostają nieudokumentowane.

[2] Raport badań nad wyciekiem danych w roku 2012, Verizon (marzec 2012)
[3] Amerykański przemysł naftowy pod ostrzałem — czy brały w tym udział Chiny? - Mark Clayton, Christian Science Monitor (25 stycznia 2012 r.)
[4] Wtargnięcie do RSA SecureID kosztowało 66 milionów dolarów - Matthew J. Schwartz, InformationWeek (28 lipca 2011 r.)
[5] Wtargnięcie do sieci Sony kosztowało firmę 170 milionów dolarów - Adam Rosenberg, Digital Trends (23 maja 2011 r.)
[6] Wycieki danych: przegląd roczny - Privacy Rights Clearinghouse

Przygotowywanie firm do walki z zaawansowanymi trwałymi zagrożeniami APT

4.0

„Dzięki ukształtowaniu solidnej infrastruktury bezpieczeństwa informacji - tak istotnej dla ochrony krytycznych danych - użytkownicy końcowi mogą się znaleźć daleko od podstawowej linii obrony".

Czy rok 2012 może być jeszcze gorszy? Cóż, badania pokazują, że może...

Ostatnie incydenty wycieków danych ustanowiły silny precedens – przyszłe pokolenia muszą przygotować się na fale coraz bardziej wyrafinowanych cyberzagrożeń tworzonych przez zagraniczne agencje, wrogie rządy, politycznych haktywistów i firmy bez skrupułów kradnące poufne dane konkurencji. Wydarzenia globalne, takie jak Igrzyska Olimpijskie, ciągły niepokój na Bliskim Wschodzie i brak stabilności ekonomicznej w Europie, mogą stać się punktem zapalnym takich działań.
W zależności od tego, komu zada się pytanie, wzrost sponsorowanego przez rządy hakingu jest albo bezpośrednim zagrożeniem, albo przerażającym, monstrualnym problemem. Zgodnie z danymi Asia Times*[7], Kongresowa Komisja Rewizyjna ds. ekonomii i bezpieczeństwa w relacji Stany Zjednoczone – Chiny (USCC) niedawno podzieliła podobne obawy, kiedy dyrektor Inicjatywy Cyberdyplomacji na rzecz Rady Atlantyckiej powiedział, że chińskie zagrożenie jest tak duże, że wojskowy departament obrony przed cyberzagrożeniami nazwał je „największym w historii ludzkości transferem bogactwa, dokonanym przy pomocy kradzieży i piractwa".

W świetle podstępnej działalności i coraz większej globalizacji, APT zawsze oznacza kłopoty. Ponieważ wielu dostawców wojskowych i coraz większa liczba głównych graczy na rynku dużych przedsiębiorstw zyskuje świadomość niebezpieczeństwa i wzmacnia obronę, logicznym krokiem jest przeniesienie koncentracji ataku na mniejsze organizacje. Zazwyczaj te sektory rynku stanowią zabójczą kombinację poufnych informacji na poziomie niewiele niższym niż duże przedsiębiorstwa i agencje rządowe i infrastruktury bezpieczeństwa IT na poziomie małej / średniej firmy. Główną różnicę stanowi stosunkowo niewielki budżet przeznaczony na bezpieczeństwo IT i brak dedykowanych pracowników ochrony, którzy mogliby monitorować zmieniający się krajobraz zagrożeń. Jeżeli dodamy do tego brak świadomości niebezpieczeństwa, wynikający z błędnej percepcji o anonimowości pomniejszych organizacji, klaruje się obraz idealnego celu dla kampanii APT. Biorąc pod uwagę fakt, że hakerzy mogli spokojnie kopać głęboko w sieci takiego giganta jak Lockheed Martin, widać w jak wielkim niebezpieczeństwie jest mały i średni sektor rynku.

Widząc olbrzymi, niszczycielski potencjał ataków APT, wydaje się być słusznym stwierdzenie, że małe i średnie firmy są w beznadziejnej sytuacji, jeżeli chodzi o arsenał środków obrony. Jest to dalekie od prawdy! Wiele ataków na rynek małych i średnich firm może zostać złagodzonych lub zatrzymanych dzięki gruntownej edukacji i regularnym szkoleniom użytkowników końcowych. Wdrożone powinny zostać najlepsze środki zaradcze, takie jak: unikanie klikania odnośników i otwierania załączników pochodzących z nieznanych źródeł; szczegółowe sprawdzanie wszelkich podejrzanych wiadomości i częsta zmiana haseł do kont i serwisów. Rozwiązaniem najlepszym ze wszystkich jest prewencja! Koszt opłacanej z góry profilaktyki jest ułamkiem tego, co organizacje musiałyby wydać na poinfekcyjną kontrolę naprawczą i reperowanie uszkodzeń po ataku, nie wspominając nawet o „lecącym na łeb na szyję" zwrocie z inwestycji - ROI.

Mówi się, że dzięki ukształtowaniu solidnej infrastruktury bezpieczeństwa informacji - tak istotnej dla ochrony krytycznych danych - użytkownicy końcowi mogą się znaleźć daleko od podstawowej linii obrony. Ekspert ds. bezpieczeństwa, Bruce Schneier, określił to słowami: „W konwencjonalnych atakach szkodliwego oprogramowania zabezpieczenie przed napastnikami jest względne; tak długo, jak jesteś lepiej zabezpieczony od innych, agresorzy zaatakują innych, nie ciebie. APT jest inne; napastnik – z jemu tylko znanych powodów – chce dopaść właśnie ciebie. Przed tego rodzaju agresorami ochroni cię tylko najwyższy poziom ochrony. To nie ma znaczenia, jak bezpieczny jesteś w porównaniu swojego otoczenia. Meritum stanowi to, czy jesteś na tyle bezpieczny, aby odeprzeć napastnika".*[8]

[7] Waszyngton poci się na myśl o cybergrożbach ze strony Chin - Benjamin Shobert, Asia Times (29 marca 2012 r.)
[8] Zaawansowane trwałe zagrożenia - Schneier On Security, Bruce Schneier (9 listopada 2011 r.)

Pierwszy i najlepszy krok: zabezpieczyć punkt końcowy

5.0

„Dla tych, którzy uważają, że poczta elektroniczna jest przestarzałym wektorem ataku: przemyślcie sprawę jeszcze raz! Większość ataków APT wykorzystuje sztuczki socjotechniczne rozprzestrzeniane z użyciem poczty elektronicznej lub komunikatorów internetowych!"

Rynek małych i średnich firm musi wzmocnić swoje systemy ochrony, aby być w stanie radzić sobie z zaawansowanymi trwałymi zagrożeniami APT. Standardowe zapory sieciowe i technologia IDS nie wystarczą do zablokowania wyrafinowanych ataków ukierunkowanych.

Sprawy komplikuje fakt, że wiele z tych technologii nie jest odpowiednio monitorowanych i aktualizowanych, mamiąc użytkowników końcowych fałszywym poczuciem bezpieczeństwa, a tak naprawdę dając wolną rękę operatorom ataków APT. Absolutnym minimum dla małych i średnich firm jest wdrożenie silnego zabezpieczenia punktów końcowych – solidnej technologii antywirusowej, kontroli aplikacji, kontroli urządzeń i monitorowania sieci.

Wiele ataków APT opartych jest na mało znanych lub kompletnie nieznanych lukach zero-day. Przedsiębiorstwa potrzebują rozwiązania zabezpieczającego punkty końcowe, które zawiera technologie badania reputacji, do monitorowania podejrzanego zachowania oraz wykrywania i eliminacji tych zagrożeń, które jeszcze nie zostały sklasyfikowane. Filtry reputacji będą również ostrzegać użytkowników końcowych przed podejrzanymi stronami internetowymi, które mogłyby infekować złośliwym oprogramowaniem.

Produkt Kaspersky Endpoint Security 8 łączy w sobie wszystkie funkcje wymagane do blokowania ataków APT w każdym stadium rozwoju. Na to rozwiązanie składa się kombinacja wielokrotnie nagradzanej technologii zwalczania szkodliwego oprogramowania i scentralizowanej kontroli danych, reprezentowanej przez moduły Kontroli aplikacji, Kontroli urządzeń i Filtrowania zawartości sieciowej wraz z wykorzystaniem białych i czarnych list. Technologie heurystyczne produktu ostrzegają użytkownika przed nieznanymi zagrożeniami i jeśli jest to konieczne, pozwalają podjąć natychmiastowe działania w celu wyeliminowania zagrożenia i przywrócenia uszkodzonych danych.

Dla tych, którzy uważają, że poczta elektroniczna jest przestarzałym wektorem ataku: przemyślcie sprawę jeszcze raz! Większość ataków APT wykorzystuje sztuczki socjotechniczne rozprzestrzeniane z użyciem poczty elektronicznej lub komunikatorów internetowych! Kaspersky Endpoint Security 8 zapewnia ochronę również w tym aspekcie: jest kompatybilny z większością programów pocztowych i pozwala na skanowanie plików i odnośników przesyłanych za pośrednictwem komunikatorów internetowych. Dodatkowo, produkt zawiera technologie anty-phishingowe oraz listę fałszywych i phishingowych adresów URL, która jest uaktualniana w czasie rzeczywistym przez Kaspersky Security Network (KSN).

Dodatkowym wzmocnieniem bram pocztowych jest rozwiązanie Kaspersky Anti-Virus Security for Mail Servers, które chroni przed szkodliwymi programami i spamem serwery groupware i wszystkie popularne serwery pocztowe – wliczając w to: Microsoft Exchange, Lotus Notes / Domino, Sendmail, Qmail, Postfix i Exim. Rozwiązanie skanuje wszystkie przychodzące i wychodzące wiadomości oraz załączniki, filtruje wiadomości ze względu na typ załącznika, a całą komunikację pocztową obejmuje skanowaniem w poszukiwaniu wirusów.

Jednak, niewiele (jeżeli w ogóle jakieś) ataków APT zatrzyma się na punktach końcowych – i to samo powinno tyczyć się rozwiązań bezpieczeństwa. Ochrona powinna być rozszerzona na całą sieć, serwery plików, stacje robocze i platformy mobilne. Produkt Kaspersky Security for File Servers zapewnia serwerom plików funkcje skanowania podczas dostępu, zgodnie z terminarzem i skanowania na żądanie wszystkich kluczowych komponentów systemu. Rozwiązanie to wykrywa, usuwa i blokuje złośliwe oprogramowanie i inne zainfekowane obiekty.

„Produkt Kaspersky Endpoint Security 8 udostępnia funkcje zarządzania i bezpieczeństwa, które spełniają wymagania przedsiębiorstw pod kątem ochrony i ceny".

Ponieważ zagrożenia APT mogą uzyskać dostęp do infrastruktury z poziomu każdej stacji roboczej, produkt Kaspersky Anti-Virus for Workstations zapewnia ochronę komputerów stacjonarnych przed wszelkimi rodzajami cyberzagrożeń, wliczając w to: wirusy, oprogramowanie szpiegowskie (spyware) i ataki hakerów. Mocnym punktem produktu jest skaner luk i zagrożeń, który nieustannie monitoruje wszystkie przychodzące i wychodzące pliki, pocztę elektroniczną, ruch internetowy i komunikację sieciową.

Jeszcze kilka lat temu, do osiągnięcia wyznaczonych celów, atak APT nie musiał wybiegać poza platformę Windows – jednak te dni już przeminęły. Ostatnia epidemia szkodliwego oprogramowania dotycząca platformy Mac OS X uświadomiła użytkownikom komputerów Mac ich bezradność i podatność na te same typy ataków, które nękają systemy Windows. W pierwszej połowie tego roku trojan Flashback rzucił cień na użytkowników Maków, pozostawiając z końcem kwietnia 2012 r. około 748 000 zainfekowanych maszyn.*[9]

Produkt Kaspersky Endpoint Security for Mac oferuje solidną ochronę antywirusową, zarówno przed zagrożeniami pokroju Flashbacka, jak i przed innymi zagrożeniami dla komputerów Mac. Produkt posiada: zaawansowane funkcje zwalczania szkodliwego oprogramowania, technologię analizy heurystycznej, możliwość optymalizacji zużycia procesora, możliwość zdalnego wdrożenia, zarządzania detekcją, funkcje kwarantanny i tworzenia kopii zapasowych leczonych obiektów.

Widoczność jest kluczem. Technologie, zapewniające pełną widoczność i możliwości raportowania, dające administratorom zdolność oceny organizacji całego środowiska IT oraz podgląd stanu zabezpieczeń, są kluczowe na linii obrony. Kontrola musi wykraczać poza punkty końcowe i stacje robocze – powinna dotrzeć do serwerów, środowisk zwirtualizowanych i platform mobilnych.

Wszystko spaja ze sobą konsola administracyjna Kaspersky Security Center 9, która oferuje obszerny zestaw narzędzi, pozwalających na: zarządzanie całą gamą różnych aplikacji ochronnych, ustawianie i planowanie profili, integrację z rozwiązaniami Cisco NAC i Microsoft NAP oraz regulację uprawnień urządzeń mobilnych. Nic nie gwarantuje całkowitej ochrony przed infekcjami złośliwym oprogramowaniem, a już na pewno przed potężnymi atakami APT. Celem każdego programu ochronnego powinno być łatwe zmniejszanie zagrożeń bezpieczeństwa przy tak niskim koszcie, jak to możliwe.

Produkt Kaspersky Endpoint Security 8 udostępnia funkcje zarządzania i bezpieczeństwa, które spełniają wymagania przedsiębiorstw pod kątem ochrony i ceny.

[9]Anatomia Flashflake'a. Część 2., VirusList.pl, Siergiej Golowanow (14 czerwca 2012 r.)

Informacje o Kaspersky Lab

Wraz ze wzrostem ilości wyrafinowanego szkodliwego oprogramowania, częstym nieświadomym korzystaniem ze złośliwych aplikacji i pracownikami przynoszącymi do pracy swoje własne urządzenia, coraz ciężej zapanować nad bezpieczeństwem IT w obrębie przedsiębiorstwa.

Dzięki Kaspersky Endpoint Security 8 to Ty ustalasz reguły gry, kontrolujesz aplikacje oraz wykorzystanie sieci i urządzeń. Jeżeli coś złego dzieje się z infrastrukturą IT w Twojej firmie, Kaspersky Lab może pomóc Ci w jej doglądaniu, zarządzaniu i ochronie.

Masz kontrolę. Siedzisz na miejscu kierowcy.

Przygotuj się na to, co nadejdzie!
kaspersky.pl/beready