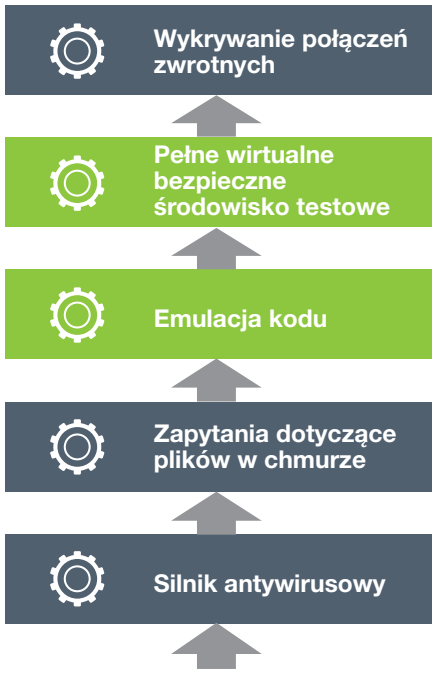
Zaawansowane zagrożenia, zaawansowane rozwiązania — Integracja bezpiecznego środowiska testowego z infrastrukturą zabezpieczeń

W przypadku sprzętu komputerowego angielski termin „sandbox" od dawna oznaczał bezpieczne, odizolowane środowisko, w którym uruchamiano złośliwy kod w celu jego analizy. Zabezpieczenia sieciowe korzystają obecnie z tego rozwiązania — mogą bowiem wówczas emulować i analizować przepływ danych w sieci oraz wykrywać złośliwy kod, który dawniej pozostałby niewykryty przez tradycyjne zabezpieczenia. Wspomniane środowisko umożliwia również emulowanie całych systemów operacyjnych i bezpieczne uruchamianie podejrzanego kodu w celu obserwowania skutków jego działania. W efekcie można zneutralizować zagrożenia wynikające ze złośliwych działań dotyczących m.in. operacji na plikach, nawiązywania połączeń sieciowych, zmian w rejestrze lub konfiguracji systemu. Wczesne wersje takich środowisk były zdolne tylko do skanowania plików wykonywalnych (na przykład plików exe i dll systemu Windows), ale zaawansowane platformy mogą już skanować wiele innych typów plików (m.in. pliki Adobe Flash, JavaScript i pakietu Microsoft Office). Bezpieczne środowiska testowe mogą być obecnie ściśle zintegrowane z pozostałą infrastrukturą zabezpieczeń, umożliwiając przesyłanie obiektów, odbieranie wyników i podejmowanie działań ochronnych z poziomu określonych punktów kontrolnych.

Zwalczanie dzisiejszych zaawansowanych zagrożeń wymaga podejścia wielowarstwowego. Z tego względu rozwiązanie Fortinet FortiSandbox oferuje zaawansowaną kombinację funkcji proaktywnej ochrony, widoczności i kompleksowego raportowania. W celu zapewnienia doskonałej ochrony przed zagrożeniami oferuje również znakomite oprogramowanie antywirusowe i funkcje wykrywania zagrożeń Fortinet, dwupoziomowe bezpieczne środowisko testowe oraz możliwość dodatkowej integracji z korzystającą z chmury społecznością FortiGuard.



RYSUNEK 1. TECHNOLOGIE FORTISANDBOX

Dlaczego zastosowanie bezpiecznego środowiska testowego ma tak duże znaczenie?

Jeśli takie środowisko było stosowane już od dawna, dlaczego dopiero teraz zostało uznane za ważny element infrastruktury zabezpieczeń? Odpowiedź jest prosta: cyberprzestępcy nie spoczywają na laurach i nadal doskonalą swoje umiejętności oraz inwestują w rozwój nowych narzędzi i technik umożliwiających przeprowadzanie ataków. Ponadto nadal szukają nowych sposobów wykorzystania istniejącego oprogramowania i użytkowników do rozprzestrzeniania wirusów i osiągania założonych celów. Dzisiejsze zaawansowane środowiska testowe mogą ułatwić szybkie wykrycie nowych zagrożeń i natychmiastowe ograniczenie skutków znanych zagrożeń.

Bezpieczne środowisko testowe i proaktywne wykrywanie sygnatur

Prowadzone w bezpiecznym środowisku testy mogą być bardzo zasobochłonne, zwłaszcza w przypadku wykonywania ich po wieloetapowych atakach, gdy kod musi być w całości wykonany przed poddaniem go analizie, a zbadanie wszystkich ścieżek realizacji kodu wymagające użycia dodatkowych modułów, które złośliwy kod usiłuje pobrać — bardzo czasochłonne. Fortinet łączy funkcje bezpiecznego środowiska testowego z proaktywnym wykrywaniem sygnatur w celu filtrowania przepływu danych zanim trafią one do tego środowiska. Rozwiązanie takie jest znacznie efektywniejsze niż korzystanie wyłącznie z samego wspomnianego środowiska.

Tradycyjny proces wykrywania sygnatur ma charakter reaktywny, ponieważ sygnatury są jedynie cechami charakterystycznymi znanych zagrożeń. Opatentowany przez Fortinet język *Compact Pattern Recognition Language* (CPRL) to proaktywna technologia wykrywania sygnatur opracowana w wyniku wieloletnich badań prowadzonych przez FortiGuard Labs. Jedna sygnatura CPRL może wykryć ponad 50 tys. nowych wariantów danego złośliwego oprogramowania. Technologia ta obejmuje funkcje odszyfrowywania, rozpakowywania i emulowania kodu na potrzeby zaawansowanej analizy statycznej, co ogranicza ilość kodu wymagającego testów w bezpiecznym środowisku. Proaktywne wykrywanie sygnatur z wykorzystaniem języka CPRL pozwala na łatwiejsze wykrywanie nowych ataków APT (ang. Advanced Persistent Threats) i AET (ang. Advanced Evasion Techniques). W efekcie bezpieczne środowisko testowe może być stosowane już tylko na potrzeby analizy najbardziej zaawansowanych zagrożeń.

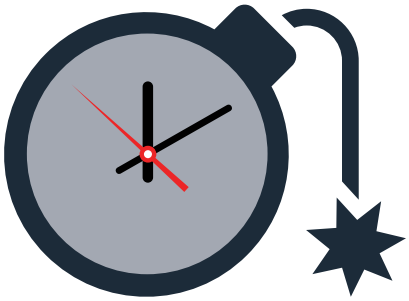
Ataki APT i AET

Ataki typu APT to niestandardowe ataki ukierunkowane, które mogą uniknąć bezpośredniego wykrycia, korzystając z nieznanego (ang. *„zero-day”*) złośliwego oprogramowania lub luk w zabezpieczeniach. Ataki te pochodzą z nowych lub pozornie nieszkodliwych adresów URL lub IP i używają zaawansowanych technik kodowania. Celem takich ataków jest przedostanie się przez zabezpieczenia systemu docelowego i uniknięcie wykrycia przez jak najdłuższy czas. Na potrzeby tych ataków intensywnie stosowane są również techniki inżynierii społecznej, dzięki czemu można zwieść nawet najbardziej wyczulonych na punkcie bezpieczeństwa użytkowników końcowych.

Ataki APT są nawet zdolne do uniknięcia takich zabezpieczeń, jak bezpieczne środowisko testowe.

Bomby logiczne

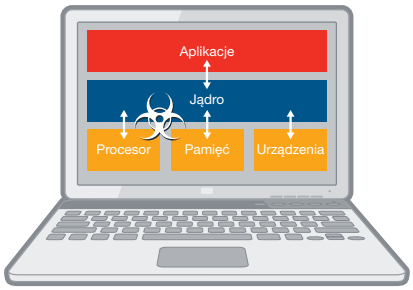
Bomba logiczna to kod, który po instalacji pozostaje w uśpieniu dopóki nie zostanie uruchomiony przez określone zdarzenie (najczęściej stosowane bomby logiczne to bomby czasowe). Bomby logiczne były już używane w głośnych atakach hakerów. W bombie czasowej złośliwa część kodu pozostaje ukryta aż do określonego momentu. Atakujący może umieścić takie złośliwe oprogramowanie w wielu systemach i mieć nadzieję, że pozostanie ono niezauważone do wspomnianego momentu, w którym wszystkie bomby zostaną aktywowane. Uruchomienie niektórych bomb logicznych wymaga działania użytkownika (m.in. kliknięcia przycisku myszy lub ponownego uruchomienia systemu) wskazującego, że bomba znajduje się na komputerze użytkownika, a nie na przykład w bezpiecznym środowisku testowym. Wykrywanie bomb logicznych jest trudne, ponieważ spełnienie warunków logicznych w bezpiecznym środowisku testowym jest mało prawdopodobne bez korzystania z zaawansowanych narzędzi. Oprócz zapewnienia tych narzędzi FortiSandbox umożliwia wykrycie bomb logicznych za pomocą języka CPRL oraz analizy emulacji kodu przed jego rzeczywistym uruchomieniem. Ponadto przeprowadzona w czasie rzeczywistym analiza faktycznych instrukcji działania pozwala na spełnienie warunków logicznych aktywujących bombę bez konieczności czekania na jej aktywację.



RYSUNEK 2. BOMBY LOGICZNE

Rootkity i bootkity

Zaawansowane złośliwe oprogramowanie często zawiera składniki typu rootkit, które za pomocą kodu realizowanego na poziomie jądra pozwalają na przejęcie pełnej kontroli nad systemem. Bezpieczne środowiska testowe mogą nie zapobiegać tej technice ataku, ponieważ funkcje monitorujące wyniki działania kodu mogą również zostać przejęte. Ponadto rootkity infekują system złośliwym oprogramowaniem podczas rozruchu, który zazwyczaj nie jest monitorowany przez wspomniane środowisko. FortiSandbox ponownie rozwiązuje ten problem dzięki zastosowaniu języka CPRL, który pozwala na wykrycie zaawansowanych rootkitów/bootkitów przed ich uruchomieniem i zamaskowaniem.

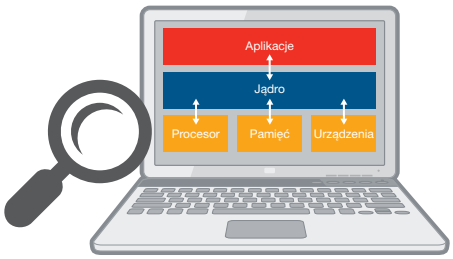


RYSUNEK 3. ROOTKIT

Wykrywanie bezpiecznego środowiska testowego

Kolejną zaawansowaną techniką unikania zabezpieczeń jest wykrywanie bezpiecznego środowiska testowego. Kod APT może sprawdzać, czy został uruchomiony w środowisku wirtualnym, które mogłoby być bezpiecznym środowiskiem testowym,

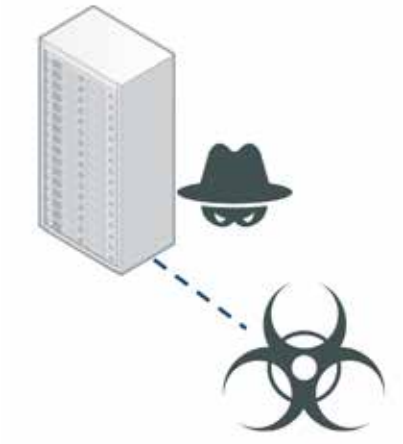
lub szukać cech charakterystycznych znanych mu środowisk testowych. Jeśli kod wykryje, że jest w takim środowisku, nie zadziała złośliwie. Również w tym przypadku język CPRL jest zdolny do szczegółowego zbadania, wykrycia i zarejestrowania kodu rozpoznającego bezpieczne środowisko testowe.



RYSUNEK 4. WYKRYWANIE BEZPIECZNEGO ŚRODOWISKA TESTOWEGO

Sterowanie botnetami

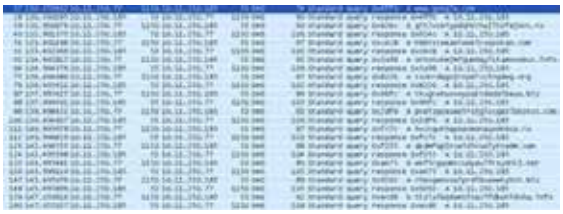
Działania związane ze sterowaniem botnetami zwykle zaczynają się od wprowadzenia składnika zakażającego (*dropper*). Dropper to czysty kod, który przenosi w sobie procedurę połączenia z adresem URL lub IP w celu pobrania pliku w odpowiedzi na określone polecenie. Polecenie takie może zostać przesłane przez atakującego wiele godzin, dni lub tygodni od pierwotnego uruchomienia. Jeśli serwer, z którym łączy się dropper, jest nieaktywny lub uśpiony podczas analizy w bezpiecznym środowisku testowym, nie będzie obserwowane żadne złośliwe działanie. Język CPRL ułatwia wykrycie nietypowych metod wykonywania kodu wskazujących na obecność złośliwego oprogramowania i odbywa się to niezależnie od tego, czy wspomniany serwer jest aktywny. Jednocześnie globalna sieć FortiGuard na bieżąco zbiera informacje o działaniach botnetów w Internecie.



RYSUNEK 5. STEROWANIE BOTNETAMI

Metoda „szybkiego przepływu”

Zaawansowane złośliwe oprogramowanie może stosować metodę szybkiego przepływu (ang. *fast flux*) lub algorytm generowania domen (DGA), aby zmienić adres URL lub IP, z którym w wyniku infekcji zostanie nawiązane połączenie. Ma to na celu uniknięcie wykrycia serwerów sprawujących kontrolę nad systemem na podstawie danych o reputacji. Podczas analizy w bezpiecznym środowisku testowym w trakcie infekcji wyszukiwany jest jeden adres, po pewnym czasie na zainfekowanym komputerze złośliwy kod podejmuje jednak próbę nawiązania połączenia z innym adresem, który został w określonym czasie uaktywniony w celu obsługi złośliwego przepływu danych. FortiGuard śledzi sieci szybkiego przepływu i przesyła zebrane informacje o zagrożeniach do bezpiecznego środowiska testowego do użycia podczas wstępnego skanowania. Rozwiązania Fortinet prowadzą wyszukiwanie na poziomie systemu DNS, a nie tylko na czarnych listach adresów IP, co często ma miejsce w przypadku rozwiązań innych producentów.



RYSUNEK 6. ALGORYTM GENEROWANIA DOMEN

Zaszyfrowane archiwa

Starą, ale nadal przydatną techniką stosowaną przez hakerów jest ukrycie złośliwego oprogramowania w zaszyfrowanym archiwum, którego nie można wypakować bez podania hasła niezbędnego do otwarcia pliku. Za pomocą inżynierii społecznej haker skłania użytkownika do otwarcia archiwum i uruchomienia złośliwego oprogramowania przez podanie hasła. W bezpiecznym środowisku testowym nie jest możliwe automatyczne podanie hasła, złośliwe oprogramowanie nie zostanie zatem uruchomione podczas procesu obserwacji i analizy. Opatentowana przez Fortinet metoda weryfikacji nagłówków skompresowanych archiwów pozwala jednak na wykrywanie cech charakterystycznych złośliwego oprogramowania zamaskowanych w wyniku kompresji.

RYSUNEK 7. ZASZYFROWANE ARCHIWA

Binarne programy pakujące

Binarne programy pakujące maskują złośliwe oprogramowanie przez zaszyfrowanie go w zniekształconych elementach kodu, które trudno przeanalizować przy użyciu tradycyjnych rozwiązań antywirusowych. Kod taki zostaje wypakowany w momencie wykonywania i infekuje hosta. Podobne techniki służą do osadzania złośliwego kodu w językach takich jak JavaScript i używany do obsługi programu Flash język Adobe ActionScript. Dawniej, gdy pamięć była cennym zasobem, technologię tę stosowano do kompresowania kodu wykonywalnego. Obecnie pojemność pamięci nie stanowi problemu, ale binarne programy pakujące są często używane w celu uniknięcia wykrycia przez programy antywirusowe. W przypadku języków JavaScript i ActionScript metoda ta może być w sposób zgodny z prawem stosowana do ochrony przed kopiowaniem. Aparat antywirusowy Fortinet oferuje funkcje odczytywania zaciemnionego kodu i wykrywania wielu binarnych programów pakujących oraz umożliwia wypakowanie złośliwego oprogramowania do formatu macierzystego na potrzeby szczegółowej analizy przy użyciu języka CPRL. Pozwala to na wykrywanie i neutralizowanie zagrożeń w czasie rzeczywistym lub na analizę złośliwego kodu w bezpiecznym środowisku testowym.

RYSUNEK 8. BINARNE PROGRAMY PAKUJĄCE

Replikacja w bezpiecznym środowisku testowym

Po rozwiązaniu problemu unikania bezpiecznego środowiska testowego przez złośliwy kod wartość tego środowiska jest nieoceniona, służy ono bowiem do pełnej replikacji zachowania złośliwego kodu, który narusza zabezpieczenia sieci przedsiębiorstwa. W sytuacji idealnej wynik uzyskany w tym środowisku powinien być taki sam jak wynik wykonania kodu w środowisku produkcyjnym. W praktyce uzyskanie identycznych wyników jest jednak trudne ze względu na występowanie wielu zmiennych. Można to porównać do próby wyhodowania z identycznych nasion dwóch identycznych roślin. Nawet drobne różnice w ilości wody, oświetleniu, temperaturze czy składzie gleby spowodują wówczas uzyskanie różnych efektów.

Luki w zabezpieczeniach i aplikacje

Zaawansowane zagrożenia mogą być ukrywane w dokumentach elektronicznych, co sprawia, że stosowny program (na przykład Word, Excel lub Adobe Reader) uruchamia złośliwy kod. Aby rzetelnie odtworzyć to zachowanie, w bezpiecznym środowisku testowym należy poddać analizie wiele różnych systemów operacyjnych, w których działają różne wersje tych programów. Jest to zatem kosztowna i czasochłonna metoda prób i błędów. W celu rozwiązania tego problemu zwiększa się moc obliczeniową wspomnianych środowisk przez zastosowanie wydajniejszych procesorów, zwiększenie liczby maszyn wirtualnych i dodanie pamięci RAM, ale działania te również są kosztowne i nieefektywne. Lepszym sposobem jest zrównoważenie doboru systemów operacyjnych i programów na podstawie częstości ich używania oraz wybranie do badania działania złośliwego oprogramowania najefektywniejszego środowiska.

Porównanie środowiska 32- i 64-bitowego oraz systemu Windows XP z systemem Windows 7/8/10

Kod 32-bitowy można uruchamiać zarówno w środowisku 32-bitowym, jak i 64-bitowym. Twórcy złośliwego oprogramowania preferują kod 32-bitowy, ponieważ zwiększa to liczbę infekcji. Obecnie większość złośliwego oprogramowania nadal ma postać plików wykonywalnych, w szczególności 32-bitowych plików Portable Executable (PE32). Pliki PE32 można uruchamiać zarówno w systemie Windows XP, jak i Windows 7/8/10, dlatego większość złośliwych działań można zaobserwować w środowisku Windows XP (nieobsługującym kodu 64-bitowego) bez konieczności dalszego testowania w środowisku Windows 7/8/10.

Ponadto poza ograniczoną liczbą przypadków Microsoft nie wspiera już systemu Windows XP. Oznacza to, że nie są już do niego dostępne poprawki i aktualizacje zabezpieczeń, a tym samym rośnie liczba luk w jego zabezpieczeniach. Środowiska Windows XP stały się zatem jeszcze bardziej podatne na różnego rodzaju infekcje. Dobra wiadomość jest taka, że w bezpiecznym środowisku testowym w systemie Windows XP uruchamiać się będzie poprawnie jeszcze więcej złośliwego oprogramowania. Z kolei zła wiadomość jest taka, że z dużym prawdopodobieństwem można założyć, że złośliwe oprogramowanie będzie projektowane z myślą o łatwej zdobyczy, jaką są komputery użytkowników, którzy nie zmienią systemu na Windows 7/8/10. Z dostępnych danych wynika, że komputerów takich jest nadal bardzo dużo.

Mechanizmy zabezpieczeń w systemie Windows 7/8

W systemie Windows 7/8 zastosowano zabezpieczenia, które uniemożliwiają wykonanie złośliwego kodu oraz wirusów ukrytych w dokumentach. Technologia nie jest dostępna w systemie Windows XP, uruchamianie kodu w systemie Windows XP w bezpiecznym środowisku testowym zwiększa zatem wykrywalność, nawet jeśli zagrożenie zostało przygotowane z myślą o systemie Windows 7/8.

System Android

Segment złośliwego oprogramowania na urządzenia przenośne szybko się rozwija, zwłaszcza w odniesieniu do względnie otwartego i pofragmentowanego środowiska systemu Android. O ile naruszenia zabezpieczeń, których źródłem były urządzenia przenośne, miały dotychczas ograniczone oddziaływanie, ryzyko stale wzrasta, w szczególności w niektórych regionach świata. Zdolność do wykrywania zagrożeń, których ścieżka ataku prowadzi przez coraz częściej potrzebne ludziom smartfony i tablety, z biegiem czasu okaże się coraz istotniejsza.

Nie tylko systemy Windows i Android

Aparat antywirusowy Fortinet uruchamiany na urządzeniu FortiSandbox w połączeniu z językiem CPRL w pełni obsługuje 32-bitowy i 64-bitowy kod oraz wiele różnych platform takich jak Windows, Mac OS X, Linux, Android, Windows Mobile, iOS, Blackberry i Symbian.

Zaawansowana integracja

Oferowane przez Fortinet urządzenie FortiSandbox umożliwia łatwą, pełną integrację bezpiecznego środowiska testowego z istniejącą infrastrukturą zabezpieczeń. Rozwiązania różnych producentów mogą być trudne lub niemożliwe do zintegrowania. Może to prowadzić do większych kosztów ogólnego zarządu, większej liczby urządzeń wymagających monitorowania i zarządzania przez personel IT oraz wzrostu złożoności sieci przedsiębiorstwa. Wspomniany personel jest z pewnością już teraz przeciążony pracą, żądanie od niego monitorowania i reagowania na sygnały kolejnego niestandardowego urządzenia o niestandardowym interfejsie użytkownika i sposobie działania zwiększa szanse przeoczenia lub zignorowania zagrożeń.

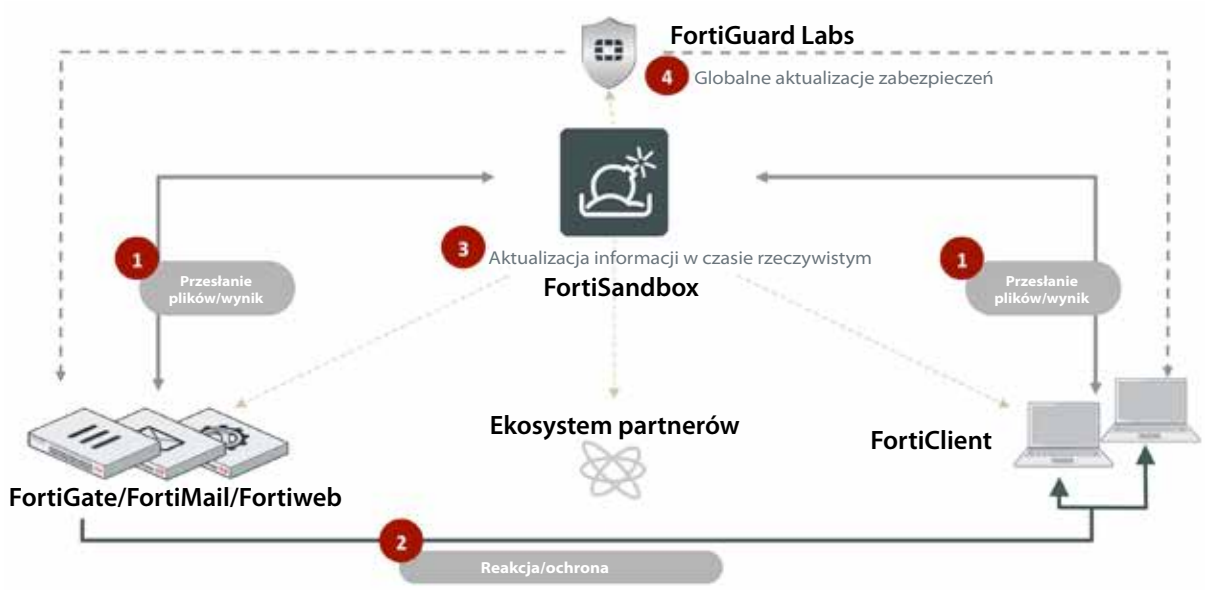
Po minimalnej konfiguracji FortiSandbox może zostać w pełni zintegrowany z istniejącymi urządzeniami FortiGate, FortiMail, FortiWeb i FortiClient. Urządzenia te można następnie skonfigurować tak, aby wysyłały pliki (lub określone podgrupy plików) do analizy do urządzenia FortiSandbox, które w przypadku wykrycia podejrzanego lub złośliwego pliku odeśle odpowiednie dane o prawdopodobieństwie zagrożenia do urządzenia nadawczego w celu podjęcia dalszych działań na podstawie określonych zasad. Ponadto FortiSandbox będzie przechowywać wspomniane dane na wypadek zapytań przesyłanych przez zintegrowane z nim produkty, a nawet tworzyć sygnatury zagrożeń przesyłane później do zintegrowanych z nim urządzeń (obecnie takie sygnatury odbierają urządzenia FortiGate i FortiClient). Pozwoli to lepiej chronić system przed kolejnymi atakami za pośrednictwem dodatkowych punktów wejściowych lub w ramach ruchu wschód–zachód. Ponadto FortiSandbox może przekazywać do innych urządzeń dane o złośliwych adresach URL służących do przeprowadzania ataków, ilekroć takie zagrożenia wykryje.

W efekcie zapobiegnie to pobieraniu wszelkich danych z takiej niebezpiecznej domeny.

Wspomniane funkcje przekazywania i automatycznego odpowiadania na zagrożenia obsługują jednak nie tylko urządzenia Fortinet. Dzięki zastosowaniu domyślnych łączników oraz otwartych, standardowych interfejsów API można również przesyłać takie dane do używanych w danym środowisku urządzeń innych producentów.

Podsumowanie

Twórcy złośliwego oprogramowania znają stosowane zabezpieczenia, maskują zatem swoje ataki oraz korzystają z zaawansowanych metod unikania wykrycia, aby umieścić złośliwy kod w atakowanym systemie. Wykrywanie zagrożeń sprowadza się do zbadania jak największej liczby warstw z uwzględnieniem wszystkich możliwych aspektów ataku. Najlepszym podejściem jest łączne zastosowanie proaktywnych mechanizmów zapobiegania zagrożeniom (na przykład języka Fortinet CPRL) w celu zatrzymania jak największej liczby ataków, w tym ataków AET, które mogą nie zostać wykryte nawet przez najnowsze zaawansowane technologie zabezpieczeń takie jak bezpieczne środowiska testowe z zaawansowanymi technologiami, służącymi do wykrywania najbardziej złożonych ataków niestandardowych. Kluczowe znaczenie ma również powiązanie funkcji zapobiegania zagrożeniom z zaawansowanymi funkcjami wykrywania zagrożeń w ramach sprawnie działającego rozwiązania chroniącego wszystkie potencjalne ścieżki ataku i ułatwiającego odpowiednią reakcję na wykryte zagrożenie. Jeśli dodatkowo wspomniane składniki są udostępniane przez podmiot analizujący zagrożenia taki jak FortiGuard Labs, właściwa reakcja na zagrożenia oraz aktualizacje informacji o zagrożeniach są zagwarantowane, nawet jeśli zagrożenia stale się zmieniają. Programem minimum powinno być jednak znalezienie takich rozwiązań i podmiotów, które w ramach współdziałania i wymiany informacji mogą zapewnić, że nawet niejednorodne infrastruktury zabezpieczeń zostaną odpowiednio wzmocnione i pozbawione luk.



RYSUNEK 9. ZINTEGROWANE BEZPIECZNE ŚRODOWISKO TESTOWE

Polska
ul. Złota 59/6F
Budynek Lumen II (6 piętro)
00-120 Warszawa
Polska

SIEDZIBA GŁÓWNA
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
Stany Zjednoczone
Tel.: +1 408 235 7700
www.fortinet.com/sales

BIURO SPRZEDAŻY — REGION EMEA
905 rue Albert Einstein
Valbonne
06560, Alpes-Maritimes, France
Tel.: +33 4 8987 0500

BIURO SPRZEDAŻY — REGION APAC
300 Beach Road 20-01
The Concourse
Singapur 199555
Tel.: +65 6513 3730

BIURO SPRZEDAŻY — AMERYKA ŁACIŃSKA
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel.: 011-52-(55) 5524–8428

22 marca 2016 r.