W dzisiejszych czasach hakerzy coraz rzadziej włamują się do sieci pokonując skomplikowane zabezpieczenia, firewalle, sondy sprawdzające anomalie w sieci. Znacznie łatwiej, szybciej i z dużo mniejszym ryzykiem wykrycia, mogą dostać się do środka organizacji skłaniając użytkownika do kliknięcia na spreparowany link, otwarcie dokumentu lub użycie klucza USB. Użytkownik wtedy uruchamia złośliwy program, który może usunąć bądź zaszyfrować efekty pliki na komputerze bądź wykraść je wysyłając na inny serwer. Dzięki akcjom phisingowym mogą próbować rozesłać automatycznie swój złośliwy kod do milionów użytkowników na całym świecie, tak masowa próba przełamania zabezpieczeń w klasyczny sposób była by niemożliwa.

W grudniu 2012 roku eksperci z firmy o izraelskich korzeniach mającej siedzibę w kalifornijskim mieście Redwood Shores o nazwie Imperva, zajmującej się monitorowaniem bezpieczeństwa danych wraz ze studentami izraelskiego Instytutu Technologii Technion w Hajfie poddali próbie standardowe narzędzia antywirusowe. Zebrali 82 nowe wirusy komputerowe (z własnych honeypotów – czyli pułapek zastawionych w sieci, oraz hackerskich forów internetowych) i uruchomili je pod okiem programów wykrywających zagrożenia, wyprodukowanych przez ponad 40 największych na świecie firm zajmujących się tworzeniem takiego oprogramowania, w tym takich gigantów jak Microsoft, Symantec, McAfee i Kaspersky Lab. Dokonali tego poprzez wysłanie ich do usługi VirusTotal. Wynik: do wykrycia zagrożenia doszło w zaledwie 5% przypadków, co oznaczało, że 95% wirusów nie zostało wykrytych (IMPERVA, 2012)

Raport Anti–Virus Comparative porównujący 18 znanych na rynku aplikacji antywirusowych podaję średnią skuteczności na poziomie 86/100 (Anty-Virus-Comparatives, 2016). Miesięczne raporty firmy AV–Test wskazują na średnią skuteczność około 97 %.

By skutecznie bronić się bronić należy dokonać analizy złośliwego oprogramowania, które dotarło do naszej lub innej organizacji tak by poznać techniki, taktyki i procedury cyberprzestępców Analiza malware to proces wydobywania informacji ze złośliwego oprogramowania za pośrednictwem statycznej i dynamicznej kontroli za pomocą różnych narzędzi, technik i procesów. Jest to metodyczne podejście do odkrywania głównego celu złośliwego oprogramowania poprzez ekstrakcję jak największej ilości danych ze złośliwego oprogramowania, jak to możliwe, gdy jest w stanie spoczynku i w ruchu. Malware w spoczynku to złośliwe oprogramowanie, które nie jest uruchomione w środowisku docelowym, podczas gdy złośliwe oprogramowanie w ruchu to oprogramowanie, które działa w środowisku docelowym. Dane ekstrahuje ze złośliwego oprogramowania poprzez wykorzystanie danych ekstrakcji i narzędzi monitorujących.

Często konieczne jest sprawdzenia dokumentów czy oprogramowania, które otrzymano z niezaufanego źródła czy nie zawiera złośliwych ukrytych funkcji. Analiza podejrzanego oprogramowania konieczna jest z kilku powodów, po pierwsze nie można polegać na oprogramowaniu antywirusowym, po drugie brak często jest narzędzi, wiedzy lub czasu do zaawansowanej analizy za pomocą reverse engineering, wówczas przydatne jest zastosowanie automatycznej analizy malware. Automatyczna analiza polega na uruchomieniu..

W obecnych czasach złośliwe oprogramowanie pojawia się na każdym kroku tak w postaci aplikacji jak i linku czy też dokumentu. Do automatycznej analizy malware najbardziej optymalny jest sandbox. Sandbox (ang. *piaskownica*) to ściśle kontrolowane i

izolowane środowisko (najczęściej wirtualne), w którym programy albo skrypty, co do których nie mamy pewności czy są bezpieczne, mogą zostać bez szkody uruchomione w pamięci (zdetonowane). Dzięki aplikacjom analizującym zawartość pamięci, wywołania systemowe, operacje na dysku lub przesyłane dane możemy stwierdzić czy uruchomione oprogramowanie jest złośliwe i jaki jest naprawdę cel jego działania.

Przykładem otwartego i bezpłatnego a zarazem zaawansowanego i modularnego oprogramowania do automatycznej analizy złośliwego oprogramowania jest Cuckoo Sandbox. W kilka minut po wysłaniu do systemu podejrzanego pliku, dokumentu czy linku Cuckoo potrafi przeanalizować próbkę i zaraportuje jakie operacje były wykonane w wyizolowanym środowisku. Dzięki temu możemy poznać i zrozumieć jak działa malware , jaki ma cel, kontekst i motywacje, nie musimy bazować jedynie na artefaktach pozostawionych w pracującym systemie które pozostawił malware. Cuckoo potrafi automatycznie badać malware uruchomione pod wirtualnych i fizycznych środowiskach MS Windows, Mac OS X, Linux i Android. Standardowo Cuckoo potrafi :

- Analizować różne złośliwe pliki (pliki wykonywalne, dokumenty zawierające eksploity doc, pdf ,xls, aplety Java) a także zainfekowane strony internetowe, w środowiskach wirtualnych Windows, OS X, Linux i Android.
- Śledzenie systemowych wywołań API i ogólne zachowanie plików Tworzenie usuwanie, pobieranie i wysyłanie do sieci Internet.
- Dokonać zrzut i analizę ruchu sieciowego, nawet jeśli jest zaszyfrowany (MITM). Ruch sieciowy może zostać kierowany do otwartej sieci Internet, TOR bądź VPN, można także zasymulować siec internetową pakietem INETSIM.
- Tworzyć zrzuty ekranu podczas wykonywania malware.
- Wykonywać zaawansowaną analizę pamięci zainfekowanego systemu zwirtualizowanego z wbudowanym wsparciem dla pakietu Volatility. (Cuckoo Fundation, 2017)

Cuckoo Sandbox analizuje poniższe typy plików

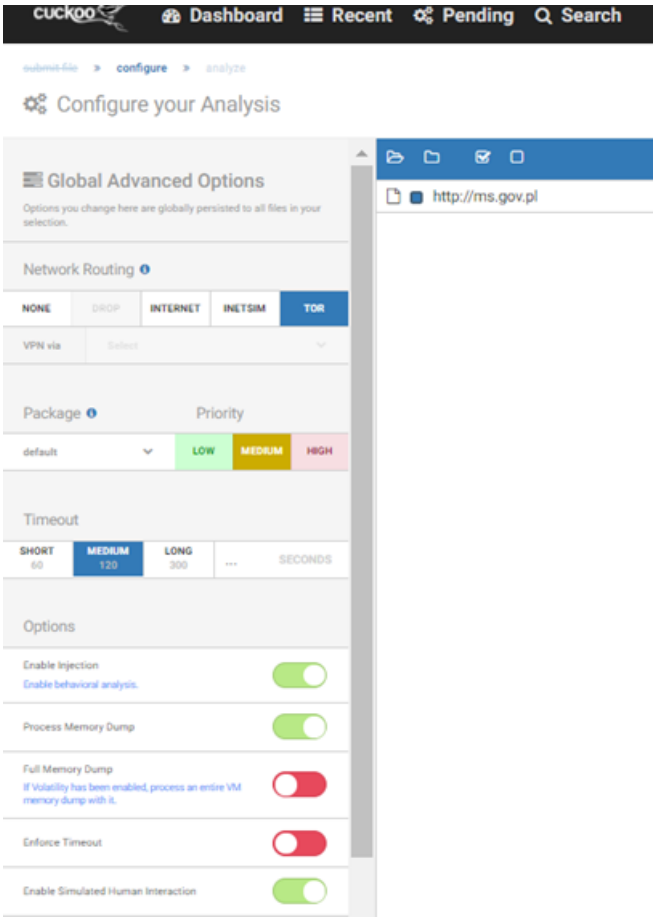
- Wykonywalne pliki Windows
- Pliki DLL
- Dokumenty PDF
- Dokumenty Microsoft Office
- URL’e i pliki HTML
- Skrypty PHP
- Pliki CPL
- Skrypty Visual Basic (VB)
- Pliki ZIP
- Pliki Java JAR
- Pliki Python

Dzięki modułowej konstrukcji Cuckoo można dostosować zarówno etapy przetwarzania analizy i raportowania do swoich potrzeb. Za pomocą wbudowanego API potrafi współpracować z innymi aplikacjami i serwisami służącymi do badania i analizy malware.

Cuckoo Sandbox jest tworzony społecznie przez zespół kilku deweloperów i specjalistów. Za rozwój tego systemu oraz pokrewnych projektów i inicjatyw odpowiedzialna jest Cuckoo Foundation – organizacja typu non profit zarejestrowana w Holandii. Cuckoo Sandbox jest licencjonowany przez Cuckoo Foundation i jest licencjonowany na bazie GNU General Public License wersja 3 — licencja wolnego i otwartego oprogramowania

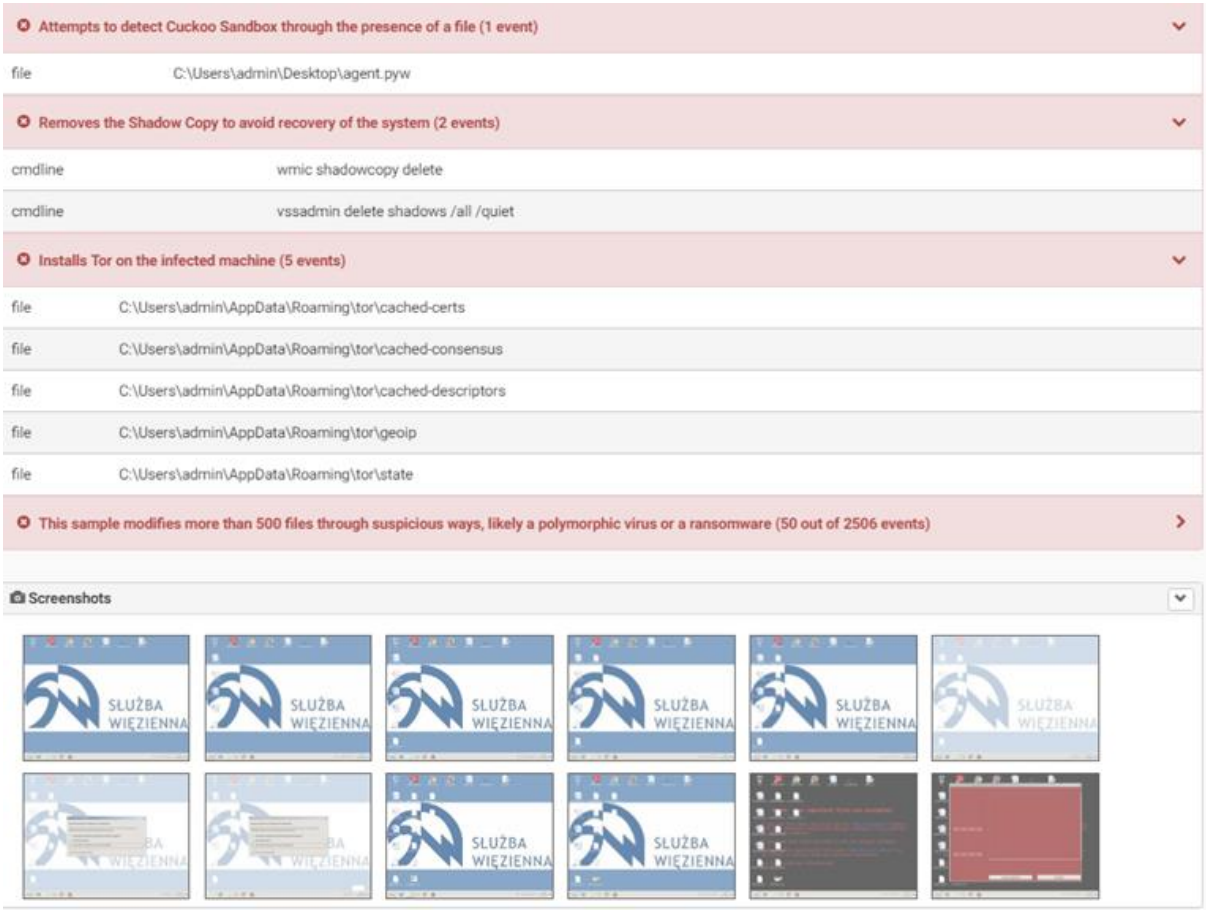
System oczekuje na przesłanie próbki oprogramowania czy linku do witryny internetowej, po przesłaniu przygotowywane jest środowisko oraz wirtualna maszyna, w której zostanie uruchomiona próbka – podczas przesyłania próbki możliwe jest określenie parametrów analizy, jak priorytet typ wirtualnej maszyny (Windows XP, 7, Android, Linux) czy też dostęp do sieci (bezpośredni , VPN, TOR, INETSIM).

Rysunek 1 Wybieranie opcji do analizy



Następnie Cuckoo uruchamia wybraną maszynę wirtualną z punktu przywracania (snapshot), przesyła do maszyny i uruchamia wybraną próbkę. Jeśli jest to próbka .exe to jest wykonywana w systemie operacyjnym maszyny wirtualnej, jeśli jest to dokument to otwierany jest edytor lub przeglądarka (MS Word, Adobe Acrobat Reader) link lub skrypt PHP/HTML uruchamiany jest w przeglądarce internetowej. W dalszej kolejności podczas działania uruchomionego malware tworzone są zrzuty ekranu, informacje o ruchu sieciowym i wszystkie inne o tworzonych czy kasowanych plikach lub wpisach w rejestrze systemu Windows i innych czynnościach zachodzących wewnątrz maszyny wirtualnej. Do tego dochodzą też zrzuty pamięci procesów lub całej pamięci RAM.

Rysunek 2 Fragment wygenerowanego raportu wraz ze zrzutami ekranu (WannaCry)



Po zebraniu wszystkich informacji generowany jest raport w postaci strony HTML, lub dokumentu PDF i tworzone są pliki z danymi zebranymi podczas analizy – utworzone lub pobrane pliki przez badany malware lub jego procesy potomne, szczegółowa analiza ruchu sieciowego oraz jego zrzut w postaci plików PCAP, pełne zrzuty zawartości pamięci RAM. (Bińkowski, 2016)

Rysunek 3 Analiza ruchu sieciowego wygenerowanego przez ransomware WannaCry

TCP 171.25.193.9:80 -> 192.168.56.101:49491	2018789	ET POLICY TLS possible TOR SSL traffic	Misc activity
TCP 69.162.139.9:9001 -> 192.168.56.101:49802	2018789	ET POLICY TLS possible TOR SSL traffic	Misc activity
TCP 178.62.173.203:9001 -> 192.168.56.101:49801	2018789	ET POLICY TLS possible TOR SSL traffic	Misc activity
TCP 62.210.92.11:9001 -> 192.168.56.101:49490	2018789	ET POLICY TLS possible TOR SSL traffic	Misc activity
TCP 193.11.114.43:9001 -> 192.168.56.101:49805	2522572	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 287	Misc Attack
TCP 79.172.193.32:443 -> 192.168.56.101:49806	2523070	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 536	Misc Attack
TCP 5.189.153.185:443 -> 192.168.56.101:49804	2522888	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 445	Misc Attack
TCP 193.11.114.43:9001 -> 192.168.56.101:49805	2018789	ET POLICY TLS possible TOR SSL traffic	Misc activity

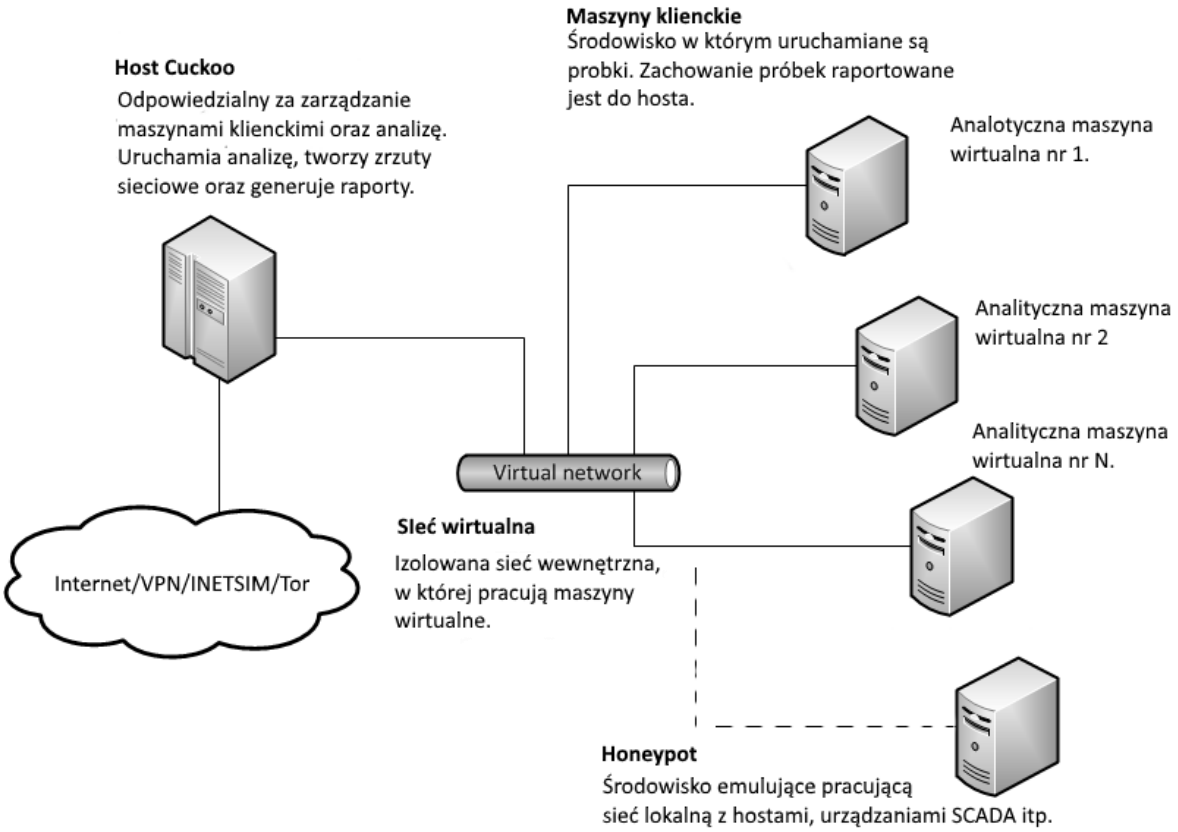
Suricata TLS

Flow	Issuer	Subject	Fingerprint
TLS 1.2 192.168.56.101:49491 171.25.193.9:80	CN=www.ljcq72hz.com	CN=www.cfrarhxu6kogkpse5zj.net	aa:b5:8f:28:a0:b3:2a:dd:20:c1:08:aa:a1:3f:41:7e:cf:52:e2:f8
TLS 1.2 192.168.56.101:49802 69.162.139.9:9001	CN=www.vpbld6o4t2kvtw.com	CN=www.umhe5bmadje.net	8f:c6:e8:48:cf:ac:b5:2b:8c:8a:ed:86:9b:52:43:2e:6c:bb:70:d9
TLS 1.2 192.168.56.101:49801 178.62.173.203:9001	CN=www.j2dtoc22os.com	CN=www.oqnyij75o7wdodycnbv.net	cf:89:20:de:d9:84:8a:51:54:c6:b4:df:0a:d4:21:f6:e8:d4:50:08
TLS 1.2 192.168.56.101:49490 62.210.92.11:9001	CN=www.vrwhayqmb44t5wcon54s.com	CN=www.4qfcsdwinihwnye.net	bf:ba:27:e1:39:4d:d8:d9:d5:01:ed:7c:8d:ed:c7:80:a3:ec:5e:f1
TLS 1.2 192.168.56.101:49804 5.189.153.185:443	CN=www.yehcgnaapl.com	CN=www.ph2phqme6r5tgji5m.net	51:9b:1e:48:ca:38:16:18:9b:4a:dd:01:fb:99:6f:22:3d:24:04:34
TLS 1.2 192.168.56.101:49805 193.11.114.43:9001	CN=www.ha2kxdga5.com	CN=www.siegjfuao6vlbips4ns.net	08:54:4e:4e:40:5b:d0:0e:5b:22:25:b6:4d:12:ea:6b:d9:32:64:17
TLS 1.2 192.168.56.101:49806 79.172.193.32:443	CN=www.s2zwkc4iomeo.com	CN=www.4zc5jd4t3kkc.net	07:43:53:33:b9:b2:60:a4:9e:e0:0b:fa:2b:bd:f9:85:2c:5b:2b:ee

Głównym elementem systemu jest oprogramowanie centralne Cuckoo zainstalowane w systemie Linux – tzw. „Cuckoo Host" bazujące na skryptach Python. Oprogramowanie to zarządza uruchomieniem i analizą przekazanej próbki malware, interfejsem webowym do obsługi aplikacji, a także maszynami typu Guest reprezentującymi wirtualne maszyny lub fizyczne komputery.

Każda analiza uruchamiana jest w czystym i odizolowanym środowisku wirtualnej maszyny lub fizycznego hosta.

Rysunek 4 Architektura systemu Cuckoo Sandbox. Źródło: (Cuckoo Fundation, 2017)



Przed przystąpieniem do instalacji Cuckoo Sandbox warto zauważyć, że wymaga on od użytkownika dobrej znajomości systemu Linux, a także podstawowej wiedzy z zakresu wirtualizacji i obsługi wirtualnych maszyn lub sieci. Dodatkowo przydatna będzie znajomość języka Python a przynajmniej jego składni. Przydatna będzie także wiedza o malware w systemach informatycznych jego zachowaniu i rozprzestrzenianiu.

Sam proces instalacji systemu jest dość skomplikowany i czasochłonny, ponieważ wykorzystuje wiele elementów zewnętrznych. Niestety, system Cuckoo nie zawiera gotowego instalatora, wszystkie więc komponenty należy zainstalować i skonfigurować samodzielnie. Proces instalacji jest w pełni opisany w dokumentacji produktu dostępnej online. W najnowszej wersji autorzy udostępnili możliwość instalacji za pomocą menagera pakietów python – pip.

Do niewątpliwych zalet Cuckoo należy współpraca z rożnymi aplikacjami jak i serwisami internetowymi. Analizowaną próbkę możemy wysłać do serwisu Virustotal, wyniki analizy (sygnatury, adresy, nazwy domen) mogą być przechowywane na serwerze MISP (służącym do zbierania, przechowywania, dystrybucji i udostępniania wskaźników zagrożenia bezpieczeństwa cybernetycznego i analizy incydentów związanych z bezpieczeństwem cybernetycznym i analizy złośliwego oprogramowania) który automatycznie może generować reguły dla firewalla zabezpieczającego naszą sieć. ruch sieciowy może być automatycznie analizowany przez IDS Snort, Suricata bądź przez analizator sieciowy MOLOCH, dane wrażliwe, które nie chcemy wysyłać do ogólnodostępnych serwerów możemy analizować w

farmie antywirusów IRMA. Do współpracy z innymi aplikacjami i serwerami przygotowane jest bardzo dobrze opisane API.

Dokumentacja

http://docs.cuckoosandbox.org/en/latest/

Literatura

IMPERVA https://www.imperva.com/docs/HII_Assessing_the_Effectiveness_of_Antivirus_Solutions.pdf

Anty-Virus-Comparatives https://www.av-comparatives.org/wp-content/uploads/2016/10/avc_rem_2016_en.pdf

Cuckoo Fundation https://cuckoosandbox.org/

Bińkowski, Krzysztof „Automatyczna analiza złośliwego oprogramowania" IT w Administracji Sierpień 2016