AV-TEST LAB

THE INDEPENDENT ANTIVIRUS TESTS

Test bezpłatnych skanerów antywirusowych

Sprawdzanie skuteczności tak zwanych skanerów antywirusowych na żądanie pod kątem detekcji zagrożeń to bardzo specyficzny test.

We współczesnym świecie, zarówno użytkownik indywidualny jak i korporacyjny bardzo często stosuje przedstawione w tym raporcie aplikacje. Ich rola nadal pozostaje niezmienna – pozwala upewnić się co do stanu bezpieczeństwa urządzenia.

wrzesień 2016

Konspekt

Sprawdzanie skuteczności tak zwanych skanerów antywirusowych na żądanie pod kątem detekcji zagrożeń to bardzo specyficzny test. We współczesnym świecie, zarówno użytkownik indywidualny jak i korporacyjny bardzo często stosuje przedstawione w tym raporcie aplikacje. Ich rola nadal pozostaje niezmienna — pozwala upewnić się co dostanu bezpieczeństwa urządzenia.

Kluczowym zadaniem skanerów na żądanie jest wykrycie oraz całkowite usunięcie zagrożenia lub pozostałości po nim — a w niektórych przypadkach leczenie zainfekowanego systemu, który może mieć wpływ na bezpieczeństwo i komfort pracy z komputerem.

Wszystkie z przetestowanych przez AVLab skanerów umożliwiają wskazanie lokalizacji, które powinny zostać sprawdzone pod kątem zainfekowanych plików w oparciu o zaimplementowane technologie skanujące danego producenta. W teście nie brano pod uwagę dostępnych skanerów, które oferują jedynie tak zwane szybkie skanowanie, nie uwzględniając preferencji użytkownika co do weryfikowania bezpieczeństwa konkretnej lokalizacji lub partycji.

W wykrywaniu kilku tysięcy zainfekowanych plików najlepszym poziomem detekcji charakteryzowały się aplikacje: Arcabit Skaner Online, Emsisoft Emergency Kit, ESET Online Scanner oraz Trend Micro HouseCall. Pozostałe programy, chociaż uzyskały certyfikat potwierdzający ich skuteczność, to nie zapewniały detekcji na tak wysokim poziomie, jak te skanery, które otrzymały najwyższe wyróżnienie „BEST+++” wykrywając ponad 99% z 7089 próbek.

W przedziale wykrywalności 98-99 procent z 7089 użytych do testu różnych wirusów znalazły się skanery: Dr.Web CureIt!, Kaspersky Virus Removal Tool, Panda Cloud Cleaner oraz Sophos Clean.

Czas skanowania wszystkich plików przez poszczególne aplikacje był bardzo zróżnicowany i wahał się od kilku minut do kilkudziesięciu, co i tak nie przekładało się na większą ilość detekcji. Najdłuższym czasem skanowania charakteryzowały się programy: Panda Cloud Cleaner, Comodo Cleaning Essentials (niekiedy aplikacja ta żądała ponownego uruchomienia systemu, aby kontynuować skanowanie) oraz Windows Defender.

Emsisoft Emergency Kit, Dr. Web Cureit!, Malwarebytes Anti-Malware i ClamWin Free Antivirus to programy, które najszybciej uporały się ze sprawdzeniem kolekcji próbek. Chociaż należy przyznać, że z różnym skutkiem.

Najwyższe wyróżnienie BEST+++ otrzymały programy:

Emsisoft Emergency Kit, Trend Micro HouseCall, Arcabit Skaner Online, ESET Online Scanner

Metodologia

Skaner antywirusowy na żądanie to specyficzne oprogramowanie, więc zastosowana przez AVLab metodologia testu wykracza poza typowe skanowanie kolekcji próbek. Oprócz badania faktycznej skuteczności detekcji tysięcy próbek złośliwego oprogramowania, w teście brano pod uwagę usuwanie szkodliwych plików i kluczy rejestru po zainfekowaniu systemu operacyjnego.

Aby sprawdzić wykrywalność najpopularniejszych darmowych skanerów antywirusowych oferowanych jako bezpłatne narzędzia od kilku producentów, przygotowano obraz wirtualnego systemu Windows 10 Professional x64 z najnowszymi aktualizacjami. System w każdym dniu testów był przywracany do stanu początkowego. Dzięki takiemu rozwiązaniu, wszystkie produkty zostały przebadane w identycznym środowisku testowym.

Materiał badawczy do pierwszej części testu w łącznej ilości 7089 próbek pozyskano we współpracy z niezależnymi badaczami. Analogicznie — w drugiej części testu — wybrano 6 konkretnych zagrożeń, które nie wchodziły w skład materiału badawczego wykorzystanego do pierwszej części testu.

AVLab pozyskując próbki do testów nie współpracuje z żadnym producentem oprogramowania zabezpieczającego. Dzięki temu nie zachodzi podejrzenie, że testowany program wykrywa zagrożenia dostarczone przez własnego producenta.

W czasie badania wszystkie programy były zainstalowane na domyślnych ustawieniach, mogły korzystać z Internetu, a w przypadku dwóch aplikacji: Dr. Web Cureit i Kaspersky Removal Tool, każdego dnia pobierano nowszą wersję programu (automatyczna aktualizacja zagrożeń nie jest w nich dostępna).

cz. 1 (skanowanie kolekcji wirusów)

1. Dla każdego testowanego programu odtwarzano obraz systemu operacyjnego, dzięki czemu wiernie odwzorowano środowisko pracy dla każdej aplikacji.
2. Każdego dnia testu dobierano niepowtarzające się próbki zagrożeń.
3. Przed wskazaniem do skanowania folderu z zainfekowanymi plikami, aktualizowano sygnatury do najnowszej wersji lub pobierano nowe wersje aplikacji (jeśli było to konieczne) z wbudowanymi sygnaturami.

cz. 2 (leczenie zainfekowanego systemu)

1. Do tej części testu dobrano różnego rodzaju zagrożenia oraz poddano ich manualnej analizie, aby sprawdzić, jakie obszary systemowe są infekowane.
2. Na odtworzonym obrazie systemu z pierwszej części testu, każda próbka została sekwencyjnie uruchomiona, po czym wykonywano restart systemu operacyjnego. Jeśli było to wymagane, udzielano zezwolenia na uruchomienie malware z uprawnieniami administratora.
3. Testowane programy miały za zadanie wykryć zainfekowany plik (dropper) lub utworzone w wyniku infekcji zmiany w systemie.
4. Jeśli było to wymagane, zezwalano na restart systemu operacyjnego w czasie pracy skanera antywirusowego na żądanie.

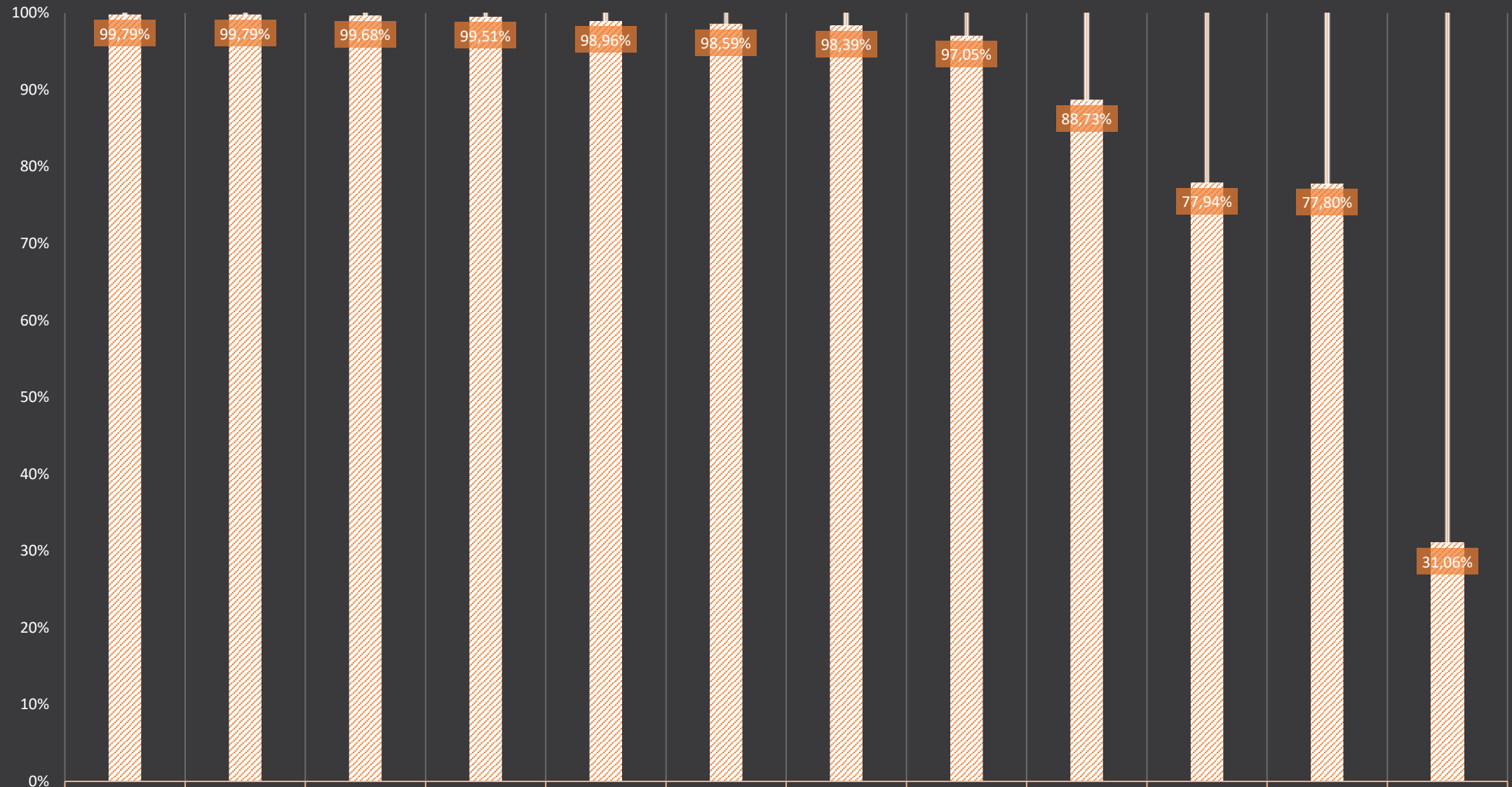
Testowane programy

Przedstawione wersje poniższych aplikacji zapisano ostatniego dnia testu.

Arcabit Skaner Online	*1.0.4*
*ClamWin Free Antivirus **	*0.99.1*
Comodo with Cleaning Essentials	*2.5.242177.201*
Dr.Web CureIt!	*11.1.2*
Emsisoft Emergency Kit	*11.9.0.6508*
ESET Online Scanner	*2.0.12.0*
Kaspersky Virus Removal Tool	*15.0.19.0*
Malwarebytes Antimalware Free	*2.2.1.1043*
Panda Cloud Cleaner	*1.1.9*
Sophos Clean (dawniej HitmanPro)	*3.7.13.262*
Trend Micro HouseCall	*(1.62)*
*Windows Defender **	*4.10.14393.0*

* CLAMWIN FREE ANTIVIRUS I WINDOWS DEFENDER ZAPEWNIAJĄ OCHRONĘ W CZASIE RZECZYWISTYM, JEDNAK NIE BRANO TEGO PO UWAGĘ. OCHRONA NA CZAS SKANOWANIA ZOSTAŁA WYŁĄCZONA.

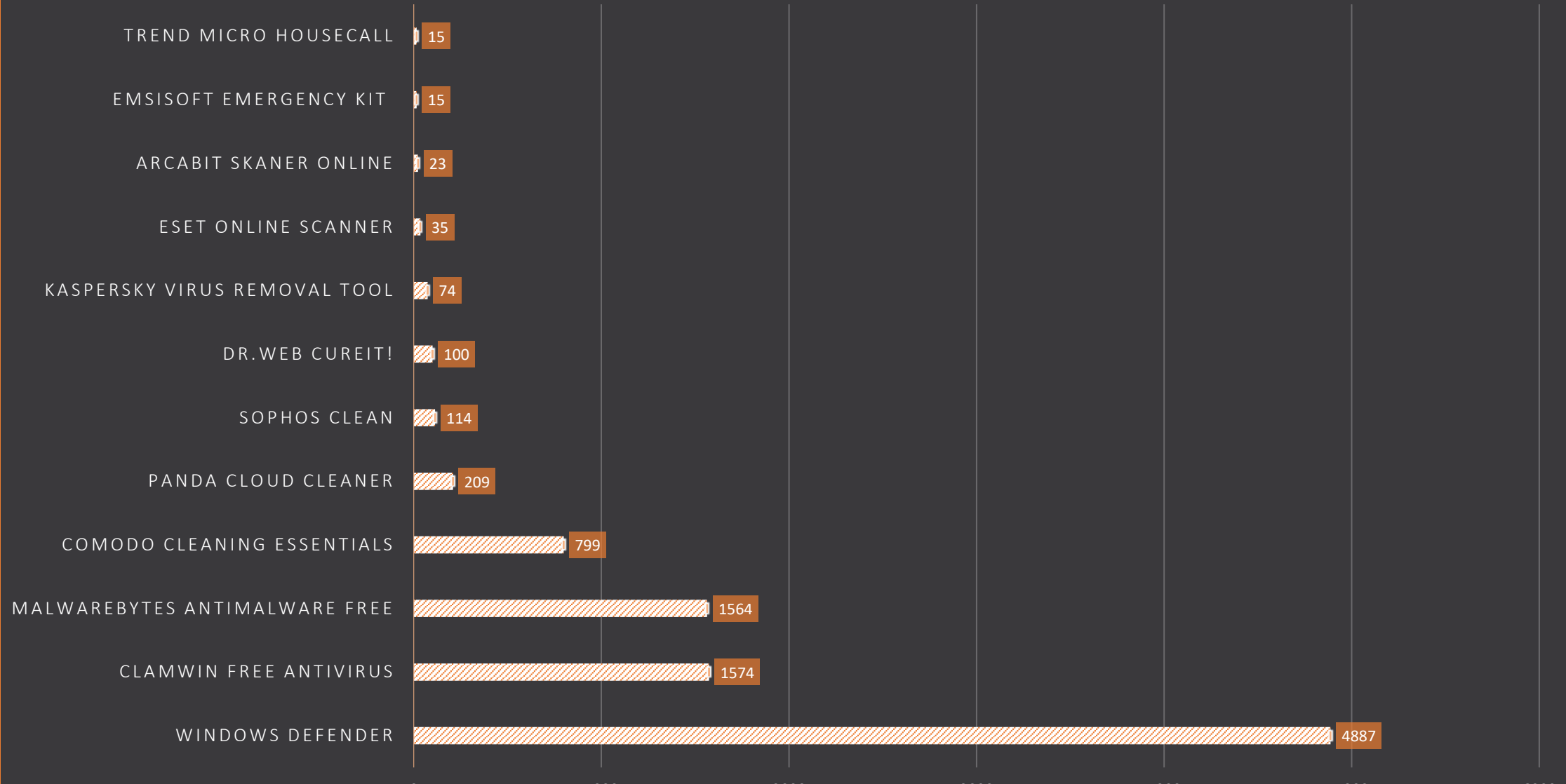
ILOŚĆ WYKRYTYCH ZAGROŻEŃ Z POŚRÓD 7089 PRZESKANOWANYCH PLIKÓW
(WIĘCEJ = LEPIEJ)



	Emsisoft Emergency Kit	Trend Micro HouseCall	Arcabit Skaner Online	ESET Online Scanner	Kaspersky Virus Removal Tool	Dr.Web CureIt!	Sophos Clean	Panda Cloud Cleaner	Comodo Cleaning Essentials	Malwarebytes Anti-Malware	ClamWin Free Antivirus	Windows Defender
Wynik	99,79%	99,79%	99,68%	99,51%	98,96%	98,59%	98,39%	97,05%	88,73%	77,94%	77,80%	31,06%

		Dzień 1	*Dzień 2*	*Dzień 3*	*Dzień 4*	*Dzień 5*	*Dzień 6*	*Dzień 7*	*Suma*
	Ilość malware	1039	883	1044	1006	917	915	1285	7089
	Ilość wykrytych zagrożeń								
Arcabit Skaner Online		1035	882	1039	1000	914	913	1283	7066
ClamWin Free Antivirus		895	717	831	760	748	618	946	5515
Comodo Cleaning Essentials		958	713	862	953	803	859	1142	6290
Dr.Web CureIt!		1023	873	1026	981	904	915	1267	6989
Emsisoft Emergency Kit		1035	882	1039	1004	916	914	1284	7074
ESET Online Scanner		1030	880	1036	1001	914	913	1280	7054
Kaspersky Virus Removal Tool		995	881	1040	1002	912	910	1275	7015
Malwarebytes Antimalware Free		832	630	755	783	693	772	1060	5525
Panda Cloud Cleaner		1016	740	1016	1000	914	912	1282	6880
Sophos Clean		1034	844	1019	988	899	914	1277	6975
Trend Micro HouseCall		1037	879	1043	1004	915	913	1283	7074
Windows Defender		247	314	421	348	265	218	389	2202

ILOŚĆ NIEWYKRYTYCH ZAINFEKOWANYCH PLIKÓW
(MNIEJ = LEPIEJ)



	Windows Defender	ClamWin Free Antivirus	Malwarebytes Antimalware Free	Comodo Cleaning Essentials	Panda Cloud Cleaner	Sophos Clean	Dr.Web CureIt!	Kaspersky Virus Removal Tool	ESET Online Scanner	Arcabit Skaner Online	Emsisoft Emergency Kit	Trend Micro HouseCall
Wynik	4887	1574	1564	799	209	114	100	74	35	23	15	15

	próbka A	*próbka B*	*próbka C*	*próbka D*	*próbka E*	*próbka F*
Arcabit Skaner Online	+	+	+	+	+	+
ClamWin Free Antivirus	-	+	+	+	+	+
Comodo Cleaning Essentials	+	+	+	+	+	+
Dr.Web CureIt!	+	+	+	+	+	+
Emsisoft Emergency Kit	+	+	+	+	+	+
ESET Online Scanner	+	+	+	+	+	+
Kaspersky Virus Removal Tool	+	+	+	+	+	+
Malwarebytes Antimalware Free	+	+	+	+	+	+
Panda Cloud Cleaner	+ *	+	+	+	+	+
Sophos Clean	+ *	+	+	+	+	+
Trend Micro HouseCall	+	+	+	+	+	+
Windows Defender	-	+	-	-	+	-

+ próbka została wykryta lub system operacyjny został wyleczony

- próbka dla testowanego rozwiązania była całkowicie niewykrywalna

* NIEKIEDY USUNIĘCIE ZAGROŻENIA WYMUSZAŁO ZE STRONY SKANERA RESTARTU SYSTEMU OPERACYJNEGO. W TYCH DWÓCH PRZYPADKACH INFEKCJĘ UDAŁO SIĘ USUNĄĆ JEDYNIE W TRYBIE RATUNKOWYM.

próbka A:

backdoor Kelihos — powoduje, że zainfekowana stacja robocza może zostać wykorzysta do rozsyłania spamu, wykradania poufnych informacji, pobierania i uruchamia innych zainfekowanych plików, w tym trojanów. Zainfekowany bot, aby komunikować się z innymi komputerami zombie, wykorzystuje połączenie P2P. W zdecentralizowanej sieci, zainfekowana maszyna może działać jako klient lub serwer C2 przyjmując i wysyłając polecenia z serwera kontrolno-zarządzającego.

próbka B:

backdoor Careto — obejmuje niezwykle wyrafinowane szkodliwe oprogramowane składające się z rootkita i bootkita. Z zaobserwowanych przez badaczy wariantów wynika, że wszystkie wersje tego malware przeznaczone są dla 32 i 64 bitowych systemów Mac OS X, Linux, Windows oraz (prawdopodobnie) Androida i iOS (z niepotwierdzonych informacji także BlackBerry OS). Backdoor Careto (alias Maska) ze względu na swoje możliwości, najprawdopodobniej powstał na zlecenie jednego z rządów państw.

Backdoor Careto może przechwycić ruch sieciowy, wciskane klawisze, rozmowy Skype, klucze PGP, potrafi analizować ruch WiFi, monitorować wszystkie operacje na plikach, gromadzić listę dokumentów z zainfekowanego systemu, w tym klucze szyfrowania, konfiguracje VPN, klucze SSH i pliki PROW. Backdoor Careto pod względem wyrafinowania jest jednym z najbardziej zaawansowanych zagrożeń APT.

próbka C:

keylogger Ardamax — komercyjny spyware, którzy został wykorzystany w jednej ze socjotechnicznych kampanii „na komornika" wycelowanej w obywateli Polski. Za pomocą tego narzędzia możliwe jest automatyczne wysyłanie zebranych logów i danych na dowolny adres e-mail lub konto FTP.

Keylogger Ardamax potrafi: rejestrować naciskane klawisze, zapisywać historię odwiedzanych stron WWW, nagrywać obraz z kamery i dźwięk za pomocą mikrofonu, przechwytywać skopiowany do schowka systemowego tekst, monitorować komunikatory AIM, Windows Live Messenger, ICQ, Skype, Yahoo Messenger, Google Talk, Miranda i QiP. Zapisane w ten sposób informacje mogą zostać wysłane na wskazany adres e-mail lub konto FTP.

próbka D:

trojan Emotet — w celu ukrycia się przed programami antywirusowymi przechowuje swoje pliki w rejestrze systemowym. Trojan Emotet o modułowej budowie zawiera: własny instalator, moduł bankowy, moduł bota antyspamowego, moduł do kradzieży kontaktów z popularnych klientów poczty (posiada zdolność auto-dystrybucji, potrafi wykradać adresy z klientów poczty i wysyłać ten sam spam do ofiar z listy kontaktów), moduł do ataków DDoS (Nitol DDoS bot).

Trojan Emotet zawiera listę popularnych adresów bankowych. Jeśli zainfekowany użytkownik odwiedza jeden ze zdefiniowanych adresów URL, Emotet rejestruje wszystkie dane przesyłane pomiędzy użytkownikiem a stroną internetową — nawet, jeśli strona jest szyfrowana protokołem HTTPS.

próbka E:

trojan downloader — jak sama nazwa wskazuje, trojan downloader zawiera szkodliwy lub potencjalne niechciane oprogramowanie, które pobiera i instaluje w zaatakowanym systemem. Pobrany w ten sposób dropper instaluje docelowego wirusa, który może być następnie wykorzystany do różnych celów.

Droppery często wykorzystywane są do przenoszenia znanych trojanów, ponieważ znacznie łatwiej jest napisać droppera niż zupełnie nowego trojana, którego program antywirusowy nie będzie w stanie wykryć.

W teście wykorzystano trojana, który tworzy na dysku kilka plików. Jeden z nich pobiera dodatkowe złośliwe oprogramowanie.

próbka F:

trojan Poweliks — wykorzystuje podatności w zabezpieczeniach programu Microsoft Word i przy pomocy spreparowanego dokumentu Word, który dystrybuowany jest za pośrednictwem poczty e-mail, instaluje dodatkowy kod, który jest skryptem PowerShell zakodowanym w Base64 wywołując i wykonując niskopoziomowy program (schellcode) napisany w asemblerze. W końcowym etapie, schellcode wykonuje binarny ładunek, który próbuje się połączyć z zakodowanymi adresami IP, aby otrzymać dalsze polecenia z serwera C&C

Trojan Poweliks może być wykorzystany do pobierania i wykonywania plików. Wszystkie swoje działania przechowuje w rejestrze — nie tworzy żadnego pliku na dysku twardym, więc jego wykrycie wymaga detekcji zainfekowanego dokumentu Word lub ochrony / przeskanowania rejestru.

99% >	BEST+++
97-98%	BEST++
95-96%	GOOD+
94-80%	AVERAGE
79%	NOT RECOMMENDED

Emsisoft Emergency Kit
Trend Micro HouseCall
Arcabit Skaner Online
ESET Online Scanner

Kaspersky Virus Removal Tool
Dr.Web CureIt!
Sophos Clean
Panda Cloud Cleaner

Comodo Cleaning Essentials
Malwarebytes Anti-Malware Free
ClamWin Free Antivirus

Windows Defender

Kontakt w sprawie testów dla producentów: kontakt@avlab.pl

Przyznane certyfikaty do pobrania w wysokiej rozdzielczości https://avlab.pl/dla-prasy

Informacje o AVLab

AVLab skupia w jednym miejscu miłośników rozwiązań zabezpieczających. Nasze działania obejmują testowanie programów i dzielenie się wynikami z naszych analiz ze wszystkimi użytkownikami Internetu. Nie jesteśmy kontrolowani i/lub powiązani w jakikolwiek sposób z żadnym producentem lub dystrybutorem oprogramowania zabezpieczającego.

Testy AVLab są niezależne i odbywają się w warunkach zbliżonych do rzeczywistości. Nie należy kierować się naszymi wynikami, jako ostateczną decyzją w wyborze aplikacji bezpieczeństwa. W celu dokonania ostatecznego wyboru, sugerujemy zapoznać się także z testami innych niezależnych laboratoriów, które korzystają z różnych metod i technik testowania oprogramowania. Ponadto, decyzje w wyborze zależą od osobistych preferencji, dostępności niezbędnych funkcji, skuteczności, wykrywalności, wpływu na wydajność systemu, wyglądu interfejsu, ceny, łatwości użytkowania, kompatybilności, języka, wsparcia technicznego i wielu innych cech.

avlab.pl