AV-TEST CYBERSECURITY FOUNDATION

Produkt Roku 2024

Rekomendowane rozwiązania do zabezpieczania Windows

Na podstawie testów
Advanced In-The-Wild Malware Test w roku 2023

marzec 2024

amtso
The cybersecurity industry's testing standard community

MEMBER

Na Skróty

I	Przyznajemy nagrody.
II	Testowani producenci.
III	Jak dokonujemy analizy w 3 krokach.
IV	Dane statystyczne z testów.
V	Indywidualne karty producentów.

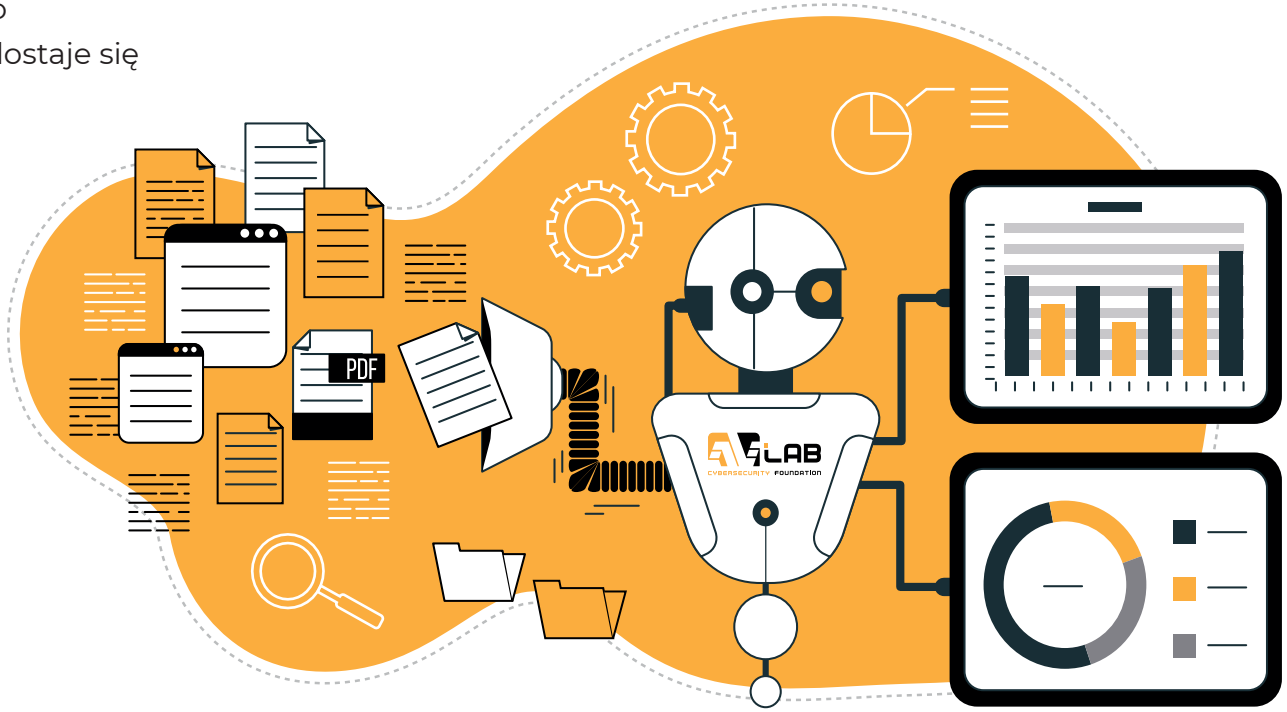
Podsumowanie testów Advanced In-The-Wild Malware Test

Celem niniejszego podsumowania jest nagrodzenie tych producentów, których oprogramowanie w roku 2023 uczestniczyło w badaniach inicjowanych przez Fundację AVLab dla Cyberbezpieczeństwa. Przyznanie specjalnej nagrody Produkt Roku 2024 to dobra okazja, aby zachęcić ludzi na stanowiskach menadżerskich IT, szefów ds. technologii i bezpieczeństwa, którzy muszą wdrażać odpowiednie standardy i procedury do zapewnienia cyfrowego bezpieczeństwa przy wykorzystaniu najlepszych rozwiązań.

Przygotowując całoroczne podsumowanie chcemy nagrodzić producentów w dwóch kategoriach. W pierwszej przyznajemy certyfikat Produkt Roku 2024 będący potwierdzeniem nad wyraz dobrej ochrony systemu operacyjnego Windows w ujęciu kompleksowym. Mianowicie testowane rozwiązania w tej serii testów sprawdzamy na szkodliwym oprogramowaniu pochodzącym z Internetu na ustawieniach domyślnych albo z włączonymi dodatkowymi funkcjami bezpieczeństwa, jeżeli uważamy, że powinny zostać aktywowane.

Kolejnym wyróżnieniem jest certyfikat TOP Remediation Time przyznany za szybkie zwalczanie złośliwego oprogramowania, które w symulowany sposób dostaje się do systemu i jest w nim uruchamiane.

Mając na uwadze ten aspekt seria Advanced In-The-Wild Malware Test jest bardzo rygorystyczna, ponieważ pokazuje prawdziwą charakterystykę testowanego produktu ochronnego przeciwko realistycznym zagrożeniom, które poprzez spam, komunikatory lub strony internetowe dostaje się na komputery. Nagroda TOP Remediation Time odzwierciedla szybki czas reakcji na malware poprzez całkowitą neutralizacją całego „cyklu życia" malware od momentu wejścia próbki do systemu aż po usunięcie złośliwej aktywności.



Kryteria przyznania nagród

Produkt Roku 2024 oraz TOP Remediation Time

Do zdobycia certyfikatu potwierdzającego kompleksową skuteczność ochrony, jak i szybką oraz całkowitą neutralizację cyklu życia malware, testowane rozwiązanie musiało spełnić określone warunki:

1. Uczestniczyć co najmniej w 3 edycjach badania Advanced In-The-Wild Malware Test.

2. Uzyskać co najmniej 3 x certyfikat EXCELLENT **(99% blokowania próbek in-the-wild)**

3. Aby dodatkowo otrzymać certyfikat TOP Remediation Time **oprogramowanie musiało zneutralizować wszystkie zagrożenia w rozpatrywanych edycjach testu. Jeżeli rozwiązanie było testowanie więcej niż trzy razy braliśmy pod uwagę trzy wyniki z najszybszym wskaźnikiem Remediation Time.**

Testowani producenci w roku 2023 roku

Acronis

avast

Avira

Bitdefender

COMODO
Creating Trust Online®

EMSISOFT

eset

F-Secure

G DATA

Immunet

kaspersky

Malwarebytes

norton

Quick Heal
Security Simplified

SOPHOS

ThreatDown
Powered by Malwarebytes

TREND MICRO

WEBROOT
SecureAnywhere

xcitium
The Power of Zero. Unleashed.

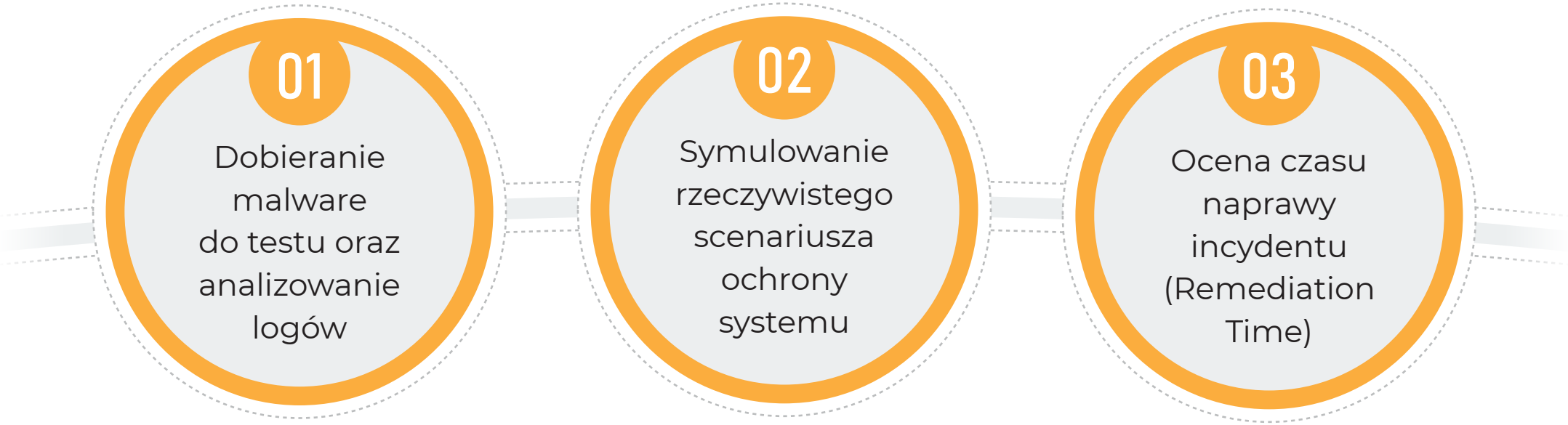
ZONEALARM
By Check Point

Nie jest to pełna lista, ponieważ niektórzy producenci biorą udział w testach anonimowo, chcąc poprawić technologie zabezpieczające. Firmy, które są zainteresowane przetestowaniem swoich rozwiązań i chciałyby się dowiedzieć, co mogą ulepszyć w oprogramowaniu, zapraszamy do kontaktu.

Jak testujemy – w pigułce

Advanced In-The-Wild Malware Test to długoterminowa analiza, której podstawowym celem jest weryfikowanie skuteczności testowanych rozwiązań przed złośliwym oprogramowaniem w czasie rzeczywistym. W tym teście rozpatrujemy biznesowe wersje produktów bezpieczeństwa, które są często wyposażone w zaawansowane moduły EDR-XDR używane do automatycznego polowania na zagrożenia wraz z funkcjonalnością usuwania skutków ataków. Testujemy także wersje dla użytkowników indywidualnych. W dużym skrócie po zainstalowaniu oprogramowania bezpieczeństwa w systemie Windows odtwarzamy zachowanie człowieka podczas korzystania z Internetu w przeglądarce. Jest to najczęściej spotykany scenariusz, gdzie każdy może paść ofiarą socjotechniki i nieumyślnego pobrania do systemu złośliwego oprogramowania.

Do testu dobierane są prawdziwe próbki szkodliwego oprogramowania in-the-wild pochodzące z rzeczywistych adresów URL, dlatego test jest najkorzystniejszy dla wszystkich odbiorców oraz producentów, którzy biorą udział w badaniu. Ujawniony zostaje szereg technicznych danych na temat metod wykrywania i blokowania zagrożeń. Dzięki systemom Windows uruchomionym w normalnym trybie graficznym test ocenia realną ochronę produktu przy uwzględnieniu naprawy każdego incydentu.



Jak dokonujemy analizy w 3 krokach – metodologia w skrócie

Na wyniki testów z serii Advanced In-The-Wild Malware Test składają się 3 duże procedury, które następują po sobie:

1. Dobieranie malware do testu oraz analizowanie logów

Na bieżąco gromadzimy złośliwe oprogramowanie w postaci prawdziwych adresów URL z Internetu. Wykorzystujemy szerokie spektrum próbek z różnych źródeł, a są to publiczne feedy i honeypoty. Test obejmuje najbardziej aktualny i zróżnicowany zestaw zagrożeń.

Każda próbka zanim trafi do testu przechodzi szereg czynności sprawdzających. Jedną z nich jest porównywanie sumy SHA256 z istniejącymi w bazie danych. Dzięki temu w naszych testach nigdy nie dochodzi do sytuacji testowania na tym samym malware.

Analizowane próbki potencjalnego złośliwego oprogramowania przechodzą weryfikację w Windows na podstawie setek reguł – najczęściej stosowanych technik przez autorów malware (tzw. LOLBin). Monitorujemy procesy systemowe, połączenia sieciowe, rejestr Windows oraz inne zmiany dokonywane w systemie operacyjnym, aby dowiedzieć się, co tak naprawdę zaświadczało o szkodliwości danej próbki podczas jej analizy.

Algorytm postępowania z malware

Sprawdzenie każdego potencjalnie złośliwego pliku dokonujemy na podstawie algorytmu:

SZEREG CZYNNOŚCI SPRAWDZAJĄCYCH

POTENCJALNIE ZŁOŚLIWY PLIK

1 **Czy plik jest online?**
Zagrożenie musi być dostępne do pobrania.

2 **Czy próbka jest unikalna?**
Porównujemy SHA256 z istniejącymi w bazie danych.

3 **Czy plik może być uruchomiony w Windows?**

4 **Statyczne skanowanie:**
korzystamy z reguł Yara oraz silnika antywirusowego mks_vir, aby upewnić się, czy plik jest prawdziwym zagrożeniem.

5 **Dynamiczne skanowanie:**
plik jest uruchamiany w systemie Windows, aby sprawdzić złośliwą aktywność z wykorzystaniem narzędzia Sysmon.

MALWARE ZAKWALIFIKOWANE DO TESTU

BRAK ZŁOŚLIWEJ AKTYWNOŚCI, PLIK ODRZUCONY

* Wiele zagrożeń zakwalifikowanych do testu jest dystrybuowanych pozornie bezpiecznym protokołem HTTPS. Autorom złośliwych stron nie sprawia żadnej trudności, aby szybko i za darmo zaimplementować certyfikat SSL w celu zwiększenia zaufania domeny. Dodatkowo niektóre z plików są umiejscowione na legalnych serwerach WWW. Aktorzy żerują na reputacji danej domeny, aby oszukać podstawowe mechanizmy zabezpieczające.

2. Symulowanie rzeczywistego scenariusza ochrony systemu

W tym kroku każda potwierdzona próbka złośliwego oprogramowania jest w tym samym czasie pobierana przez przeglądarkę z rzeczywistego adresu URL do systemów Windows, gdzie zainstalowane są rozwiązania bezpieczeństwa. Jest to bardzo ważny etap testowania, ponieważ każde oprogramowanie ochronne powinno mierzyć się z tym samym zagrożeniem dokładnie w tym samym czasie.

W badaniu symulujemy rzeczywisty scenariusz wtargnięcia zagrożenia do systemu na skutek pobrania pliku z adresu URL. Może to być strona internetowa przygotowana przez oszusta albo link wysłany ofierze przez komunikator, mail, dokument. Następnie link jest otwierany w Mozilla Firefox.

ŹRÓDŁO ATAKU **WYODRĘBNIANIE ADRESU URL** **POBIERANIE MALWARE**

Wynik na próbce malware może być zakwalifikowany do jednego z następujących poziomów

PRE-LAUNCH

Dotyczy wykrywania malware przed uruchomieniem w systemie.

POST-LAUNCH

Dotyczy analizy, kiedy wirus dostał się do systemu, został uruchomiony i wykryty przez testowane rozwiązania.

FAIL

Malware nie zostało zablokowane i zainfekowało system.

a.

Jeśli link do pliku jest szybko identyfikowany i blokowany w przeglądarce albo tuż po zapisaniu na dysku przez testowany produkt, to wówczas przypisujemy dla próbki wynik tzw. PRE-LANUCH, gdzie dane zagrożenie jest zatrzymywane na wczesnym etapie, jeszcze przed uruchomieniem.

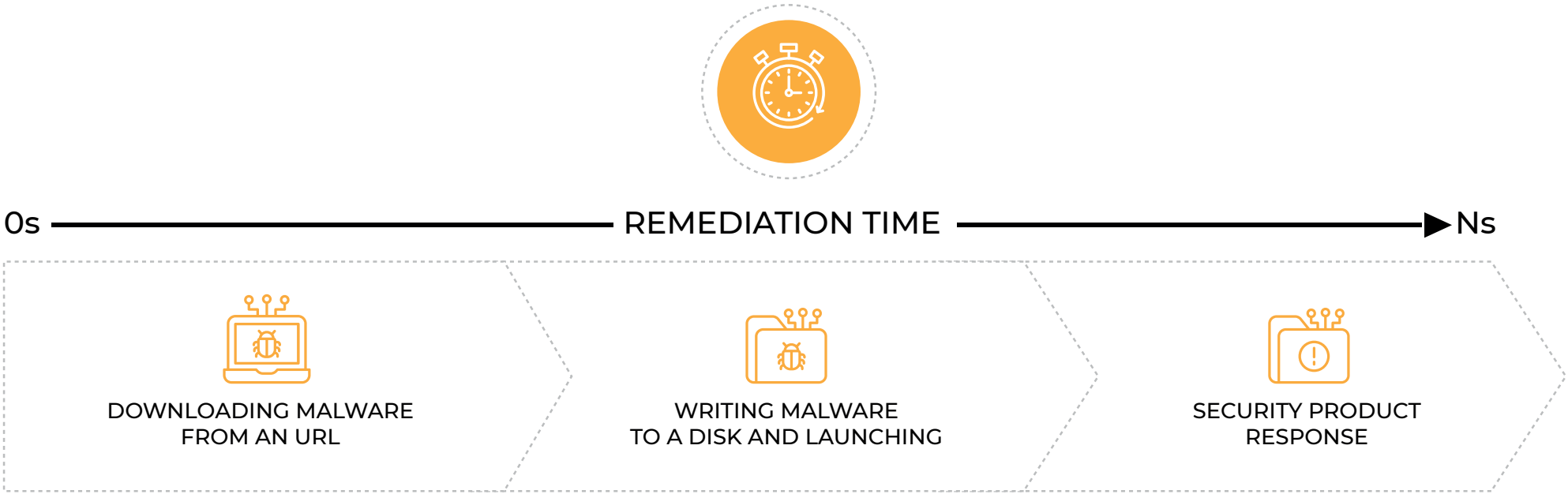
b.

Jeżeli malware zostanie pobrane, dopuszczone do uruchomienia, ale skutecznie zatrzymane, to przypisujemy poziom POST-LANUCH, oceniając realną skuteczność produktu przeciwko znanym zagrożeniom i przed zagrożeniami 0-day.

O ile poziom Pre-Lanuch wskazuje na zatrzymanie malware, które zostało szybko wykryte i zablokowane, zanim aktywowało swój złośliwy ładunek, o tyle poziom Post-Lanuch zwykle odnosi się do zagrożenia wychwyconego dowolną technologią producenta (lokalną albo w chmurze) już po detonacji pliku w systemie. Należy podkreślić, że na tym poziomie najlepiej radzą sobie te rozwiązania, które dysponują zróżnicowaną ochroną w postaci wielu warstw zabezpieczeń.

3. Ocena czasu naprawy incydentu (Remediation Time)

W dalszej kolejności, na podstawie uzyskanych logów oprócz detekcji i blokowania zagrożeń 0-day, obliczamy czas automatycznego naprawiania skutków incydentu dla danej próbki malware. Nazywamy to „Automatic Average Remediation Time". Testowane produkty konfigurujemy w taki sposób, aby usuwanie skutków ataku z naprawą systemu było realizowane automatycznie, nie pytając użytkownika o decyzję, ponieważ nie to jest celem testowania.



Aby oszacować czas „Automatic Average Remediation Time" przyjmujemy, że incydent rozpoczyna się od pobrania pliku z adresu URL i trwa do czasu zakończenia dynamicznej analizy, której czas to 7 do 9 minut. Po tym czasie, jeżeli nie zarejestrujemy żadnej aktywności produktu bezpieczeństwa na aktywność malware, ów analiza kończy się wynikiem negatywnym (Fail). Finalnie dla każdej próbki malware od momentu jej uruchomienia odmierzamy czas potrzebny do wykrycia wskaźników infekcji (ang. Indicators of Compromise) po automatyczną naprawę incydentu.

Dane statystyczne z testów *

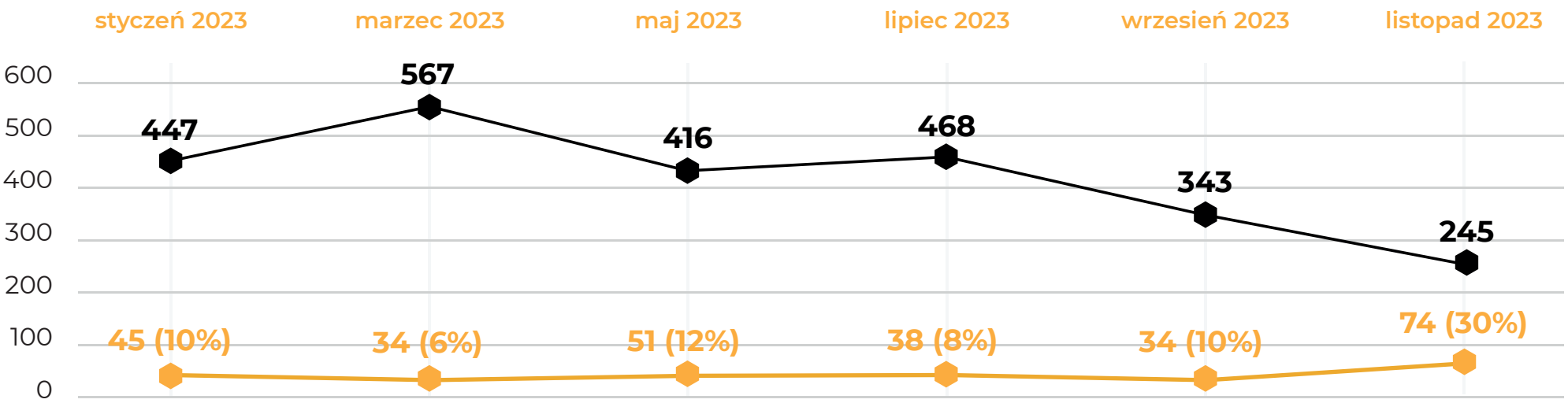
* Opracowano na podstawie informacji zwrotnych przeskanowanych plików za pomocą silnika naszego partnera technologicznego, firmy mks_vir Sp. z o.o.

Podstawowe informacje o szkodliwym oprogramowaniu

Uwzględniając dane telemetryczne z testowanych rozwiązań, okazało się, że łącznie w roku 2023 wykorzystaliśmy 2468 próbek niepowtarzającego się złośliwego oprogramowania.

Malware w liczbach

Średnio 12,6% wszystkich próbek w każdej edycji stanowiło zagrożenie nieznane w dniu analizy, co odpowiada plikom o zerowej reputacji (0-day). Zauważyliśmy, że złośliwe oprogramowanie najczęściej występowało pod postacią fałszywych plików-faktur lub innego rodzaju dokumentów, które mogą podszywać się pod znane firmy i instytucje. Bardzo wysoko w statystykach znajduje się trojan z rodziny RedLine używany przez cyberprzestępców do kradzieży danych i do kontrolowania komputerów użytkowników. W danych telemetrycznych z testu kolejno odnotowujemy trojany-downloadery, takie jak Zusy i Zard, które są najczęściej rozprzestrzeniane przez spamerskie kampanie email. W roku 2023 trojany zdominowały listę TOP10 najczęściej występującego złośliwego oprogramowania.

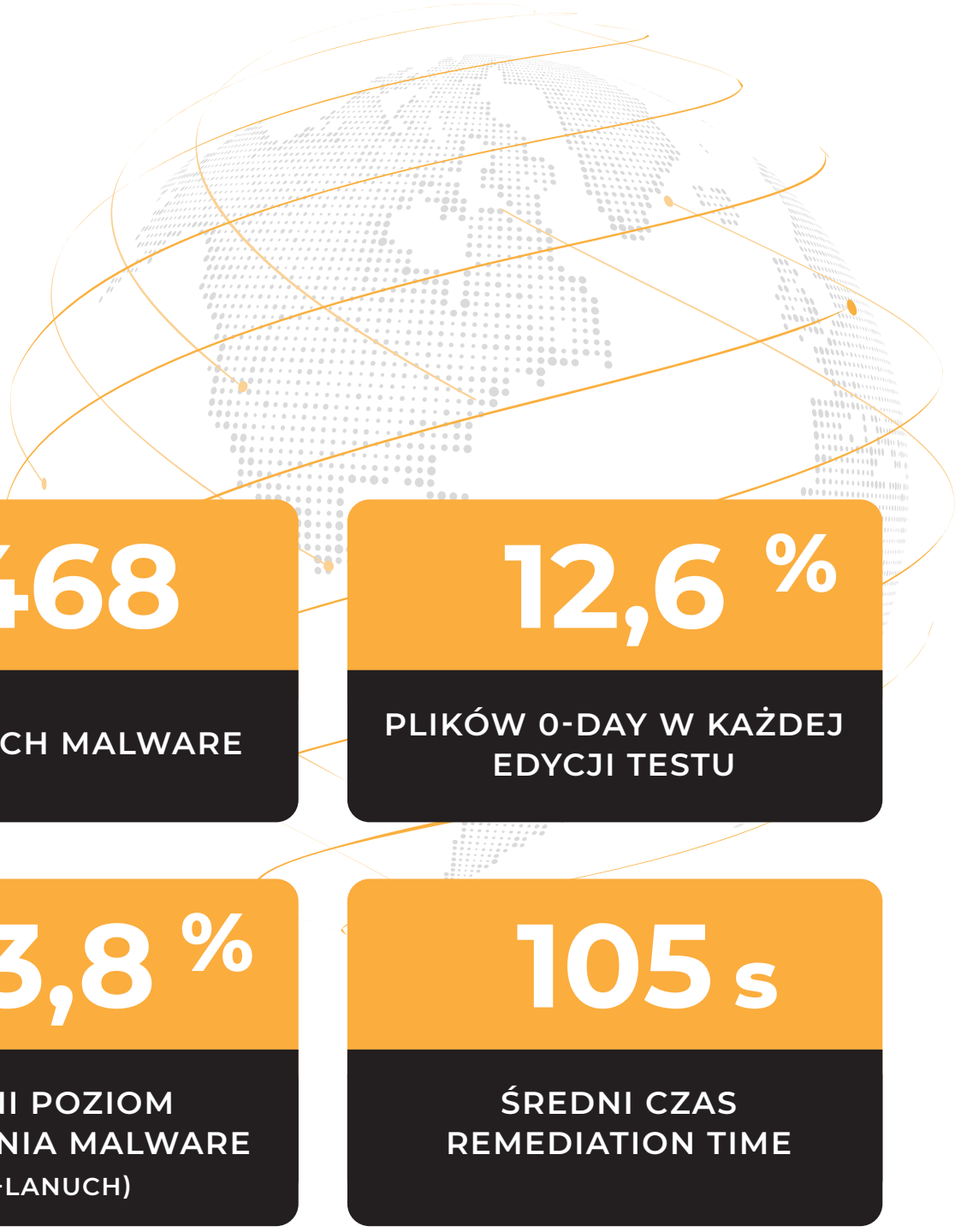


2468 Całkowita liczba potwierdzonych próbek malware w poszczególnych edycjach testu

276 Ilość plików 0-day użytych do przeprowadzenia testu

Pozostałe informacje

Z TESTÓW W 2023



6

EDYCJI BADANIA

2468

UNIKALNYCH MALWARE

12,6 %

PLIKÓW 0-DAY W KAŻDEJ EDYCJI TESTU

72,6 %

ŚREDNI POZIOM DETEKCJI MALWARE (PRE-LANUCH)

23,8 %

ŚREDNI POZIOM BLOKOWANIA MALWARE (POST-LANUCH)

105 s

ŚREDNI CZAS REMEDIATION TIME

avast | Free Antivirus

Oprogramowanie do ochrony stacji roboczej uczestniczyło we wszystkich edycjach testu. Łącznie w całym roku zablokowało 2468 rzeczywistych próbek malware. Daje to maksymalny wynik 100% wszystkich zneutralizowanych zagrożeń in-the-wild.

- Ponad 87% zagrożeń zostało zablokowanych w przeglądarce albo tuż po zapisaniu na dysku bez uruchamiania złośliwego oprogramowania.
- Ponad 12% próbek złośliwego oprogramowania zostało zablokowanych po uruchomieniu.
- Uwzględniając trzy najlepsze wyniki oprogramowanie Avast potrzebowało średnio 13 sekund na automatyczną i bezbłędną naprawę incydentów bezpieczeństwa.

Na podstawie uzyskanych danych telemetrycznych potwierdzamy, że oprogramowanie AVAST Free Antivirus ani razu nie naraziło systemu operacyjnego oraz znajdujących się na dysku danych na potencjalny wyciek wskutek uruchomienia złośliwego oprogramowania w testowym systemie.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	94,85%	5,15%	-	100%	22s
MARCH	92,12%	6,88%	-	100%	4s
MAY	81,79%	18,21%	-	100%	43s
JULY	81,41%	18,59%	-	100%	43s
SEPTEMBER	81,79%	18,21%	-	100%	57s
NOVEMBER	90,61%	9,39%	-	100%	13s
AVERAGE	87,10%	12,74%	-	100%	13s

PRE-LAUNCH: poziom dotyczy wykrywania próbek złośliwego oprogramowania przed ich uruchomieniem w systemie

POST-LAUNCH: poziom dotyczy analizy, kiedy wirus dostał się do systemu, został uruchomiony i wykryty przez testowane rozwiązania

FAIL: malware nie zostało zablokowane i zainfekowało system

RT [REMEDIATION TIME]: średnia na podstawie 3 najlepszych czasów neutralizacji zagrożeń

COMODO
Creating Trust Online®

Internet Security Pro

Oprogramowanie do ochrony stacji roboczej uczestniczyło we wszystkich edycjach testu. Łącznie w całym roku zablokowało 2468 rzeczywistych próbek malware. Daje to maksymalny wynik 100% wszystkich zneutralizowanych zagrożeń in-the-wild.

- Ponad 42% zagrożeń zostało zablokowanych już w przeglądarce albo tuż po zapisaniu na dysku bez uruchamiania złośliwego oprogramowania.
- Ponad 57% próbek złośliwego oprogramowania zostało zablokowanych po uruchomieniu.
- Uwzględniając trzy najlepsze wyniki oprogramowanie Comodo potrzebowało średnio 13 sekund na automatyczną i bezbłędną naprawę incydentów bezpieczeństwa.

Na podstawie uzyskanych danych telemetrycznych potwierdzamy, że oprogramowanie COMODO Internet Security Pro ani razu nie naraziło systemu operacyjnego oraz znajdujących się na dysku danych na potencjalny wyciek wskutek uruchomienia złośliwego oprogramowania w testowym systemie.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	21,48%	78,52%	-	100%	175s
MARCH	33,33%	66,67%	-	100%	158s
MAY	45,67%	54,33%	-	100%	170s
JULY	65,38%	34,62%	-	100%	75s
SEPTEMBER	45,95%	54,05%	-	100%	135s
NOVEMBER	43,27%	56,73%	-	100%	269s
AVERAGE	42,51%	57,49%	-	100%	123s

PRE-LAUNCH: poziom dotyczy wykrywania próbek złośliwego oprogramowania przed ich uruchomieniem w systemie

POST-LAUNCH: poziom dotyczy analizy, kiedy wirus dostał się do systemu, został uruchomiony i wykryty przez testowane rozwiązania

FAIL: malware nie zostało zablokowane i zainfekowało system

RT [REMEDIATION TIME]: średnia na podstawie 3 najlepszych czasów neutralizacji zagrożeń

EMSISOFT

Enterprise Security + EDR

Oprogramowanie do ochrony stacji roboczej uczestniczyło we wszystkich edycjach testu. Łącznie w całym roku zablokowało 2467 rzeczywistych próbek malware. Daje to prawie maksymalny wynik wszystkich zneutralizowanych zagrożeń in-the-wild.

- Prawie 59% zagrożeń zostało zablokowanych w przeglądarce albo tuż po zapisaniu na dysku bez uruchamiania złośliwego oprogramowania.
- Ponad 41% próbek złośliwego oprogramowania zostało zablokowanych po uruchomieniu.
- Uwzględniając trzy najlepsze wyniki oprogramowanie Emsisoft potrzebowało średnio 106 sekund na automatyczną i bezbłędną naprawę incydentów bezpieczeństwa.

Na podstawie uzyskanych danych telemetrycznych potwierdzamy, że oprogramowanie EMSISOFT nie naraziło systemu operacyjnego i danych na potencjalny wyciek w sposób rażący na skutek uruchamiania złośliwego oprogramowania w testowym systemie. Jeden zgłoszony incydent został natychmiast przeanalizowany przez wyspecjalizowany zespół analityków i szybko wyeliminowany.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	62,75%	37,25%	-	100%	254s
MARCH	59,08%	40,92%	-	100%	242s
MAY	54,81%	45,19%	-	100%	181s
JULY	57,69%	42,31%	-	100%	167s
SEPTEMBER	57,51%	42,49%	-	100%	139s
NOVEMBER	59,59%	40,00%	0,41% (1 sample)	99,59%	13s
AVERAGE	58,57%	41,36%	0,07%	99,93%	106s

PRE-LAUNCH: poziom dotyczy wykrywania próbek złośliwego oprogramowania przed ich uruchomieniem w systemie

POST-LAUNCH: poziom dotyczy analizy, kiedy wirus dostał się do systemu, został uruchomiony i wykryty przez testowane rozwiązania

FAIL: malware nie zostało zablokowane i zainfekowało system

RT [REMEDIATION TIME]: średnia na podstawie 3 najlepszych czasów neutralizacji zagrożeń

Smart Security Premium

Oprogramowanie do ochrony stacji roboczej uczestniczyło w 3/6 edycjach testu. Łącznie w całym roku zablokowało 1056 rzeczywistych próbek malware. Daje to maksymalny wynik 100% wszystkich zneutralizowanych zagrożeń in-the-wild.

- Prawie 86% zagrożeń zostało zablokowanych już w przeglądarce albo tuż po zapisaniu na dysku bez uruchamiania złośliwego oprogramowania.
- Ponad 14% próbek złośliwego oprogramowania zostało zablokowanych po uruchomieniu.
- Uwzględniając trzy najlepsze wyniki oprogramowanie Eset potrzebowało średnio 31 sekund na automatyczną i bezbłędną naprawę incydentów bezpieczeństwa.

Na podstawie uzyskanych danych telemetrycznych potwierdzamy, że oprogramowanie ESET Smart Security Premium ani razu nie naraziło systemu operacyjnego oraz znajdujących się na dysku danych na potencjalny wyciek wskutek uruchomienia złośliwego oprogramowania w testowym systemie.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	not tested	-	-	-	-
MARCH	not tested	-	-	-	-
MAY	not tested	-	-	-	-
JULY	82,26%	17,74%	-	100%	50s
SEPTEMBER	81,79%	18,21%	-	100%	34s
NOVEMBER	93,88%	6,12%	-	100%	8s
AVERAGE	85,98%	14,02%	-	100%	31s

PRE-LAUNCH: poziom dotyczy wykrywania próbek złośliwego oprogramowania przed ich uruchomieniem w systemie

POST-LAUNCH: poziom dotyczy analizy, kiedy wirus dostał się do systemu, został uruchomiony i wykryty przez testowane rozwiązania

FAIL: malware nie zostało zablokowane i zainfekowało system

RT [REMEDIATION TIME]: średnia na podstawie 3 najlepszych czasów neutralizacji zagrożeń

F-Secure | Total

Oprogramowanie do ochrony stacji roboczej uczestniczyło w 4/6 edycjach testu. Łącznie w całym roku zablokowało 1628/1632 rzeczywistych próbek malware. Daje to prawie maksymalny wynik wszystkich zneutralizowanych zagrożeń in-the-wild.

- Ponad 82% zagrożeń zostało zablokowanych już w przeglądarce albo tuż po zapisaniu na dysku bez uruchamiania złośliwego oprogramowania.
- Ponad 17% próbek złośliwego oprogramowania zostało zablokowanych po uruchomieniu.
- Uwzględniając trzy najlepsze wyniki oprogramowanie F-Secure potrzebowało średnio 13 sekund na automatyczną i bezbłędną naprawę incydentów bezpieczeństwa.

Na podstawie uzyskanych danych telemetrycznych potwierdzamy, że oprogramowanie F-SECURE nie naraziło systemu operacyjnego i danych na potencjalny wyciek w sposób rażący na skutek uruchamiania złośliwego oprogramowania w testowym systemie.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	not tested	-	-	-	-
MARCH	83,25%	16,05%	0,71% (1 sample)	99,29%	27s
MAY	not tested	-	-	-	-
JULY	79,49%	20,51%	-	100%	13s
SEPTEMBER	83,53%	16,47%	-	100%	21s
NOVEMBER	84,08%	15,92%	-	100%	6s
AVERAGE	82,59%	17,24%	0,18%	99,82%	13s

PRE-LAUNCH: poziom dotyczy wykrywania próbek złośliwego oprogramowania przed ich uruchomieniem w systemie

POST-LAUNCH: poziom dotyczy analizy, kiedy wirus dostał się do systemu, został uruchomiony i wykryty przez testowane rozwiązania

FAIL: malware nie zostało zablokowane i zainfekowało system

RT [REMEDIATION TIME]: średnia na podstawie 3 najlepszych czasów neutralizacji zagrożeń

Total Security

Oprogramowanie do ochrony stacji roboczej uczestniczyło w 4/6 edycjach testu. Łącznie w całym roku zablokowało 1472 rzeczywistych próbek malware. Daje to maksymalny wynik 100% wszystkich zneutralizowanych zagrożeń in-the-wild.

- Ponad 94% zagrożeń zostało zablokowanych już w przeglądarce albo tuż po zapisaniu na dysku bez uruchamiania złośliwego oprogramowania.
- Prawie 6% próbek złośliwego oprogramowania zostało zablokowanych po uruchomieniu.
- Uwzględniając trzy najlepsze wyniki oprogramowanie G Data potrzebowało średnio 16 sekund na automatyczną i bezbłędną naprawę incydentów bezpieczeństwa.

Na podstawie uzyskanych danych telemetrycznych potwierdzamy, że oprogramowanie G DATA Total Security ani razu nie naraziło systemu operacyjnego oraz znajdujących się na dysku danych na potencjalny wyciek wskutek uruchomienia złośliwego oprogramowania w testowym systemie.

AV LAB CYBERSECURITY FOUNDATION
PRODUCT OF THE YEAR 2024
ADVANCED IN-THE-WILD MALWARE TEST

TOP REMEDIATION TIME
AV LAB CYBERSECURITY FOUNDATION
CERTIFIED 2024

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	not tested	-	-	-	-
MARCH	not tested	-	-	-	-
MAY	93,99%	6,01%	-	100%	81s
JULY	88,03%	11,97%	-	100%	14s
SEPTEMBER	100%	0%	-	100%	0s
NOVEMBER	95,1%	4,9%	-	100%	33s
AVERAGE	94,28%	5,72%	-	100%	16s

PRE-LAUNCH: poziom dotyczy wykrywania próbek złośliwego oprogramowania przed ich uruchomieniem w systemie

POST-LAUNCH: poziom dotyczy analizy, kiedy wirus dostał się do systemu, został uruchomiony i wykryty przez testowane rozwiązania

FAIL: malware nie zostało zablokowane i zainfekowało system

RT [REMEDIATION TIME]: średnia na podstawie 3 najlepszych czasów neutralizacji zagrożeń

kaspersky | Plus

Oprogramowanie do ochrony stacji roboczej uczestniczyło w 4/6 edycjach testu. Łącznie w całym roku zablokowało 1472 rzeczywistych próbek malware. Daje to maksymalny wynik 100% wszystkich zneutralizowanych zagrożeń in-the-wild.

- Ponad 96% zagrożeń zostało zablokowanych już w przeglądarce albo tuż po zapisaniu na dysku bez uruchamiania złośliwego oprogramowania.
- Ponad 3% próbek złośliwego oprogramowania zostało zablokowanych po uruchomieniu.
- Uwzględniając trzy najlepsze wyniki oprogramowanie Kaspersky potrzebowało średnio 16 sekund na automatyczną i bezbłędną naprawę incydentów bezpieczeństwa.

Na podstawie uzyskanych danych telemetrycznych potwierdzamy, że oprogramowanie KASPERSKY Plus ani razu nie naraziło systemu operacyjnego oraz znajdujących się na dysku danych na potencjalny wyciek wskutek uruchomienia złośliwego oprogramowania w testowym systemie.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	not tested	-	-	-	-
MARCH	not tested	-	-	-	-
MAY	97,84%	2,16%	-	100%	164s
JULY	97,65%	2,35%	-	100%	82s
SEPTEMBER	97,11%	2,89%	-	100%	287s
NOVEMBER	94,69%	5,31%	-	100%	122s
AVERAGE	96,82%	3,18%	-	100%	123s

PRE-LAUNCH: poziom dotyczy wykrywania próbek złośliwego oprogramowania przed ich uruchomieniem w systemie

POST-LAUNCH: poziom dotyczy analizy, kiedy wirus dostał się do systemu, został uruchomiony i wykryty przez testowane rozwiązania

FAIL: malware nie zostało zablokowane i zainfekowało system

RT [REMEDIATION TIME]: średnia na podstawie 3 najlepszych czasów neutralizacji zagrożeń

Malwarebytes | Premium

Oprogramowanie do ochrony stacji roboczej uczestniczyło we wszystkich edycjach testu. Łącznie w całym roku zablokowało 2468 rzeczywistych próbek malware. Daje to maksymalny wynik 100% wszystkich zneutralizowanych zagrożeń in-the-wild.

- Prawie 85% zagrożeń zostało zablokowanych już w przeglądarce albo tuż po zapisaniu na dysku bez uruchamiania złośliwego oprogramowania.
- Ponad 15% próbek złośliwego oprogramowania zostało zablokowanych po uruchomieniu.
- Uwzględniając trzy najlepsze wyniki oprogramowanie Malwarebytes potrzebowało średnio 183 sekund na automatyczną i bezbłędną naprawę incydentów bezpieczeństwa.

Na podstawie uzyskanych danych telemetrycznych potwierdzamy, że oprogramowanie MALWAREBYTES Premium ani razu nie naraziło systemu operacyjnego oraz znajdujących się na dysku danych na potencjalny wyciek wskutek uruchomienia złośliwego oprogramowania w testowym systemie.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	95,79%	4,21%	-	100%	294s
MARCH	89,59%	10,41%	-	100%	219s
MAY	89,42%	10,58%	-	100%	209s
JULY	83,96%	16,03%	-	100%	138s
SEPTEMBER	78,03%	21,97%	-	100%	286s
NOVEMBER	70,61%	29,39%	-	100%	202s
AVERAGE	84,57%	15,43%	-	100%	183s

PRE-LAUNCH: poziom dotyczy wykrywania próbek złośliwego oprogramowania przed ich uruchomieniem w systemie

POST-LAUNCH: poziom dotyczy analizy, kiedy wirus dostał się do systemu, został uruchomiony i wykryty przez testowane rozwiązania

FAIL: malware nie zostało zablokowane i zainfekowało system

RT [REMEDIATION TIME]: średnia na podstawie 3 najlepszych czasów neutralizacji zagrożeń

MICROSOFT Defender

Oprogramowanie do ochrony stacji roboczej uczestniczyło w 3/6 edycjach testu. Łącznie w całym roku zablokowało 1420/1430 rzeczywistych próbek malware. Daje to wynik ponad 99% zneutralizowanych zagrożeń in-the-wild.

- Ponad 18% zagrożeń zostało zablokowanych już w przeglądarce albo tuż po zapisaniu na dysku bez uruchamiania złośliwego oprogramowania.
- Ponad 81% próbek złośliwego oprogramowania zostało zablokowanych po uruchomieniu.
- Uwzględniając trzy wyniki rozwiązanie Microsoftu potrzebowało średnio 119 sekund na automatyczną naprawę incydentów bezpieczeństwa.

Na podstawie uzyskanych danych telemetrycznych stwierdzamy, że oprogramowanie MICROSOFT Defender mogło narazić system operacyjny oraz znajdujące się na dysku dane na potencjalny wyciek wskutek uruchomienia złośliwego oprogramowania w testowym systemie.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	18,79%	80,76%	0,45% (2 samples)	99,55%	115s
MARCH	15,7%	83,6%	0,7% (4 samples)	99,29%	122s
MAY	19,95%	79,09%	0,96% (4 samples)	99,04%	121s
JULY	not tested	-	-	-	-
SEPTEMBER	not tested	-	-	-	-
NOVEMBER	not tested	-	-	-	-
AVERAGE	18,15%	81,15%	0,7%	99,29%	119s

PRE-LAUNCH: poziom dotyczy wykrywania próbek złośliwego oprogramowania przed ich uruchomieniem w systemie

POST-LAUNCH: poziom dotyczy analizy, kiedy wirus dostał się do systemu, został uruchomiony i wykryty przez testowane rozwiązania

FAIL: malware nie zostało zablokowane i zainfekowało system

RT [REMEDIATION TIME]: średnia na podstawie 3 najlepszych czasów neutralizacji zagrożeń

ThreatDown
Powered by Malwarebytes

Endpoint Protection + EDR

Oprogramowanie do ochrony stacji roboczej uczestniczyło we wszystkich edycjach testu. Łącznie w całym roku zablokowało 2468 rzeczywistych próbek malware. Daje to maksymalny wynik 100% wszystkich zneutralizowanych zagrożeń in-the-wild.

- Prawie 86% zagrożeń zostało zablokowanych już w przeglądarce albo tuż po zapisaniu na dysku bez uruchamiania złośliwego oprogramowania.
- Ponad 14% próbek złośliwego oprogramowania zostało zablokowanych po uruchomieniu.
- Uwzględniając trzy najlepsze wyniki oprogramowanie ThreatDown potrzebowało średnio 167 sekund na automatyczną i bezbłędną naprawę incydentów bezpieczeństwa.

Na podstawie uzyskanych danych telemetrycznych potwierdzamy, że oprogramowanie THREATDOWN Endpoint Protection ani razu nie naraziło systemu operacyjnego oraz znajdujących się na dysku danych na potencjalny wyciek wskutek uruchomienia złośliwego oprogramowania w testowym systemie.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	97,09%	2,91%	-	100%	289s
MARCH	89,42%	10,58%	-	100%	221s
MAY	89,66%	10,34%	-	100%	180s
JULY	81,84%	18,16%	-	100%	157s
SEPTEMBER	80,35%	19,65%	-	100%	189s
NOVEMBER	77,55%	22,45%	-	100%	163s
AVERAGE	85,99%	14,01%	-	100%	167s

PRE-LAUNCH: poziom dotyczy wykrywania próbek złośliwego oprogramowania przed ich uruchomieniem w systemie

POST-LAUNCH: poziom dotyczy analizy, kiedy wirus dostał się do systemu, został uruchomiony i wykryty przez testowane rozwiązania

FAIL: malware nie zostało zablokowane i zainfekowało system

RT [REMEDIATION TIME]: średnia na podstawie 3 najlepszych czasów neutralizacji zagrożeń

Quick Heal
Security Simplified

Total Security

Oprogramowanie do ochrony stacji roboczej uczestniczyło w 4/6 edycjach testu. Łącznie w całym roku zablokowało 1472 rzeczywistych próbek malware. Daje to maksymalny wynik 100% wszystkich zneutralizowanych zagrożeń in-the-wild.

- Ponad 82% zagrożeń zostało zablokowanych już w przeglądarce albo tuż po zapisaniu na dysku bez uruchamiania złośliwego oprogramowania.
- Prawie 18% próbek złośliwego oprogramowania zostało zablokowanych po uruchomieniu.
- Uwzględniając trzy najlepsze wyniki oprogramowanie Quick Heal potrzebowało średnio 38 sekund na automatyczną i bezbłędną naprawę incydentów bezpieczeństwa.

Na podstawie uzyskanych danych telemetrycznych potwierdzamy, że oprogramowanie QUICK HEAL Total Security ani razu nie naraziło systemu operacyjnego oraz znajdujących się na dysku danych na potencjalny wyciek wskutek uruchomienia złośliwego oprogramowania w testowym systemie.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	not tested	-	-	-	-
MARCH	not tested	-	-	-	-
MAY	91,59%	8,41%	-	100%	36s
JULY	78,85%	21,15%	-	100%	24s
SEPTEMBER	76,59%	23,41%	-	100%	55s
NOVEMBER	81,22%	18,78%	-	100%	59s
AVERAGE	82,06%	17,94%	-	100%	38s

PRE-LAUNCH: poziom dotyczy wykrywania próbek złośliwego oprogramowania przed ich uruchomieniem w systemie

POST-LAUNCH: poziom dotyczy analizy, kiedy wirus dostał się do systemu, został uruchomiony i wykryty przez testowane rozwiązania

FAIL: malware nie zostało zablokowane i zainfekowało system

RT [REMEDIATION TIME]: średnia na podstawie 3 najlepszych czasów neutralizacji zagrożeń

WEBROOT by opentext™

Antivirus

Oprogramowanie do ochrony stacji roboczej uczestniczyło we wszystkich edycjach testu. Łącznie w całym roku zablokowało 1471/1472 rzeczywistych próbek malware. Daje to prawie maksymalny wynik 100% wszystkich zneutralizowanych zagrożeń in-the-wild.

- Ponad 48% zagrożeń zostało zablokowanych już w przeglądarce albo tuż po zapisaniu na dysku bez uruchamiania złośliwego oprogramowania.
- Prawie 52% próbek złośliwego oprogramowania zostało zablokowanych po uruchomieniu.
- Uwzględniając trzy najlepsze wyniki oprogramowanie Webroot potrzebowało średnio 36 sekund na automatyczną i bezbłędną naprawę incydentów bezpieczeństwa.

Na podstawie uzyskanych danych telemetrycznych potwierdzamy, że oprogramowanie WEBROOT Antivirus nie naraziło systemu operacyjnego i danych na potencjalny wyciek w sposób rażący na skutek uruchamiania złośliwego oprogramowania w testowym systemie.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	44,3%	55,7%	-	100%	125s
MARCH	43,03%	56,97%	-	100%	25s
MAY	51,92%	47,84%	0,24% (1 sample)	99,76%	100s
JULY	63,68%	36,32%	-	100%	54s
SEPTEMBER	41,04%	58,96%	-	100%	30s
NOVEMBER	44,9%	55,1%	-	100%	180s
AVERAGE	48,15%	51,82%	0,24%	99,96%	36s

PRE-LAUNCH: poziom dotyczy wykrywania próbek złośliwego oprogramowania przed ich uruchomieniem w systemie

POST-LAUNCH: poziom dotyczy analizy, kiedy wirus dostał się do systemu, został uruchomiony i wykryty przez testowane rozwiązania

FAIL: malware nie zostało zablokowane i zainfekowało system

RT [REMEDIATION TIME]: średnia na podstawie 3 najlepszych czasów neutralizacji zagrożeń

xcitium

The Power of Zero. Unleashed.

ZeroThreat Advanced + EDR

Oprogramowanie do ochrony stacji roboczej uczestniczyło we wszystkich edycjach testu. Łącznie w całym roku zablokowało 2468 rzeczywistych próbek malware. Daje to maksymalny wynik 100% wszystkich zneutralizowanych zagrożeń in-the-wild.

- Prawie 86% zagrożeń zostało zablokowanych już w przeglądarce albo tuż po zapisaniu na dysku bez uruchamiania złośliwego oprogramowania.
- Ponad 14% próbek złośliwego oprogramowania zostało zablokowanych po uruchomieniu.
- Uwzględniając trzy najlepsze wyniki oprogramowanie Xcitium potrzebowało średnio 79 sekund na automatyczną i bezbłędną naprawę incydentów bezpieczeństwa.

Na podstawie uzyskanych danych telemetrycznych potwierdzamy, że oprogramowanie XCITIUM ani razu nie naraziło systemu operacyjnego oraz znajdujących się na dysku danych na potencjalny wyciek wskutek uruchomienia złośliwego oprogramowania w testowym systemie.

	PRE	POST	FAIL	COMBINED PROTECTION	AVERAGE RT
JANUARY	2,24%	97,76%	-	100%	136s
MARCH	7,94%	92,06%	-	100%	110s
MAY	15,14%	84,86%	-	100%	107s
JULY	5,13%	94,87%	-	100%	21s
SEPTEMBER	3,18%	96,82%	-	100%	119s
NOVEMBER	23,67%	76,33%	-	100%	179s
AVERAGE	9,55%	90,45%	-	100%	79s

PRE-LAUNCH: poziom dotyczy wykrywania próbek złośliwego oprogramowania przed ich uruchomieniem w systemie

POST-LAUNCH: poziom dotyczy analizy, kiedy wirus dostał się do systemu, został uruchomiony i wykryty przez testowane rozwiązania

FAIL: malware nie zostało zablokowane i zainfekowało system

RT [REMEDIATION TIME]: średnia na podstawie 3 najlepszych czasów neutralizacji zagrożeń

AVLab
CYBERSECURITY FOUNDATION

Fundacja AVLab dla Cyberbezpieczeństwa jako niezależna organizacja stoi na straży ochrony prywatności i bezpieczeństwa w Internecie. Budujemy świadomość użytkowników z zakresu ochrony cyfrowej. Wydajemy opinie, techniczne analizy oraz testy rozwiązań informatycznych w sferze cyberbezpieczeństwa. Naszym najmocniejszym atutem są wnikliwe i szczegółowe recenzje, przygotowywanie raportów związanych z prywatnością i ochroną urządzeń końcowych, a w szczególności testy bezpieczeństwa, dzięki którym jesteśmy rozpoznawalni na całym świecie, jako jedno z najpopularniejszych laboratoriów testujących.

Jesteśmy stowarzyszeni w grupie roboczej non-profit AMTSO (Anti-Malware Testing Standards Organization). W ramach pełnionych funkcji w międzynarodowych środowisku ekspertów pracujemy nad poprawą transparentności, obiektywności oraz jakości przeprowadzanych testów oprogramowania ochronnego.

Aby poznać szczegóły techniczne producenci mogą kierować swoje zapytania na adres: kontakt@avlab.pl

amtso
The cybersecurity industry's testing standard community
MEMBER