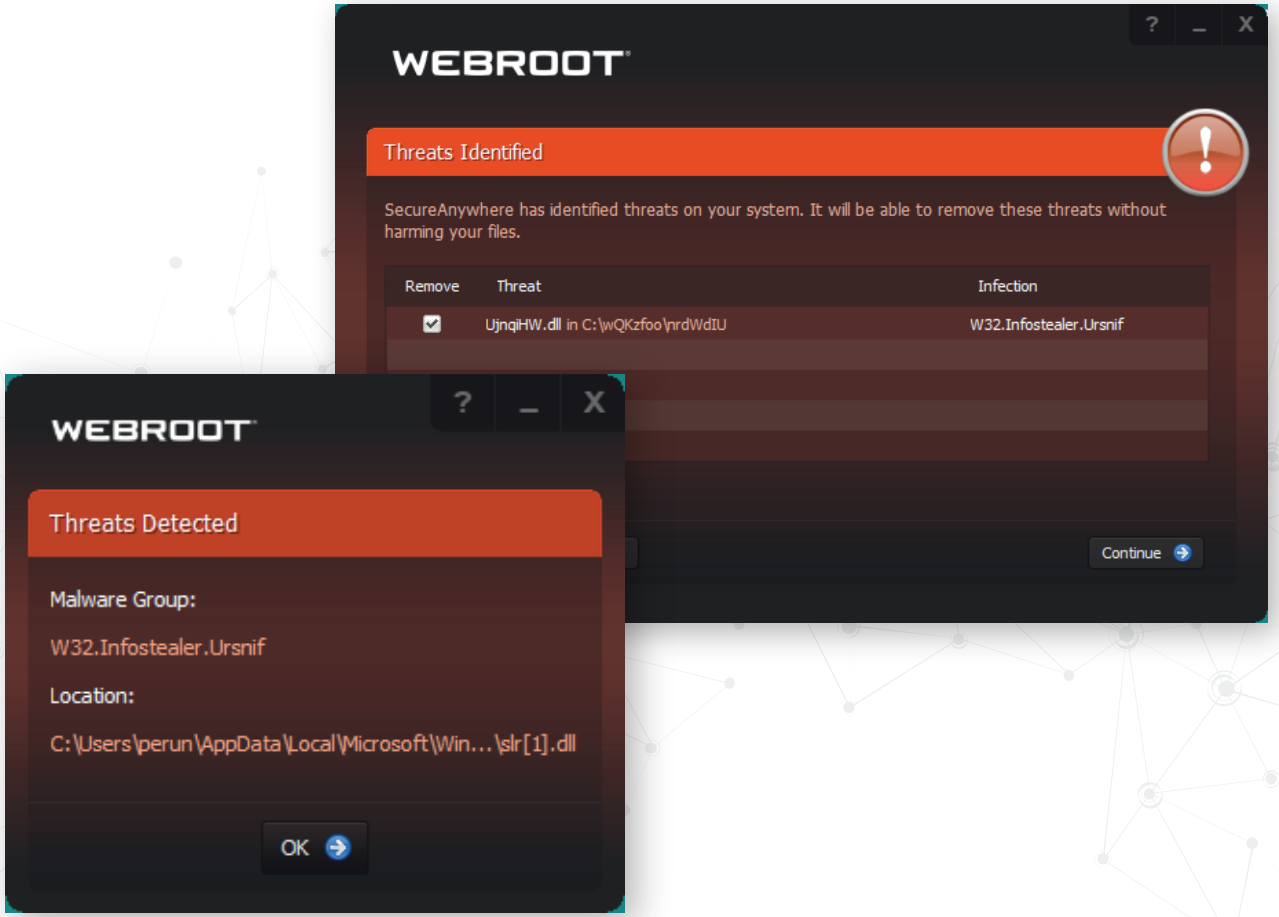
THE INDEPENDENT ANTIVIRUS TESTS



Nazwa produktu: WEBROOT Endpoint Protection
Data testu: kwiecień 2020

WEBROOT® Smarter Cybersecurity™

Najlepsze antywirusy na podstawie testów ochrony przed atakami bezplikowymi, ransomware i makrowirusami

Główne założenia testu

Chcieliśmy sprawdzić skuteczność zabezpieczeń popularnych programów do ochrony komputerów osobistych i stacji roboczych przed najczęściej rejestrowanymi zagrożeniami i cyberatakami od początku 2020 roku.

W ostatnim kwartale cyberprzestępcy dali do zrozumienia, że aby uniknąć wykrycia przez tradycyjne narzędzia ochronne, łączy się popularne rodziny złośliwego oprogramowania z nowoczesnymi technikami atakowania. Według raportów globalnych firm IT ataki bezplikowe będą zjawiskiem bardzo powszechnym w kolejnych kwartałach. Używanie tego typu sposobów oszukiwania zabezpieczeń wzrosło o kilkaset procent, co zaobserwowała firma Trend Micro pod koniec grudnia 2019 roku. Zaprogramowane przez hackerów narzędzia do automatycznego wyszukiwania podatności w aplikacjach mają obecnie większe możliwości techniczne niż wcześniej. Są też trudniejsze do zaobserwowania, ponieważ do uruchomiania złośliwego kodu nie potrzebują interakcji z użytkownikiem.

Dotkliwym zjawiskiem jest niszczenie efektów pracy uniwersytetów, szpitali państwowych i prywatnych klinik, które wspólnie próbują wyizolować choroby. Trudno pojąć jak bardzo prymitywnymi pobudkami kierują się przestępcy i dlaczego zwracają się przeciwko nauce i służbie zdrowia. Działanie internetowych kryminalistów ma negatywne konsekwencje w gospodarce, co mogliśmy zaobserwować w ostatnich tygodniach. Największe serwisy informacyjne pisały o incydentach wymuszania okupów od placówek zdrowia i szkół wyższych w zamian za odszyfrowanie danych utraconych w wyniku cyberataku.

Trendy w cyber-zagrożeniach na rok 2020 podkreślają potrzebę inwestowania w rozwiązania, które pozwolą na szczegółowe raportowanie istotnych zmian w systemach i sieciach. Swój kamień dźwigają producenci i dostawcy usług IT, którzy powinny brać odpowiedzialność za rozwiązania, które dostarczają firmom i użytkownikom końcowym. Z drugiej strony przedsiębiorstwa muszą zrozumieć ryzyko i zacząć chronić się przed atakami proaktywnie, a także łagodzić skutki ewentualnych ataków. Większość organizacji nie może sobie pozwolić na utrzymanie podstawowych zabezpieczeń do ochrony sieci, nie mówiąc już o podtrzymaniu całodobowych jednostek monitorowania bezpieczeństwa infrastruktury. Firmy powinny rozważyć współpracę z doświadczonym dostawcą usług bezpieczeństwa, który pomoże im zabezpieczyć systemy IT przed współczesnymi cyberatakami.

Złośliwe dokumenty Office

Makra można łatwo połączyć z technikami socjotechnicznymi w kampaniach phishingowych. Obieg dokumentów w przedsiębiorstwach jest czymś normalnym, a domyślnie zainstalowany pakiet Office automatycznie wymusza potrzebę ochrony systemów IT przed próbą zainfekowania systemów.

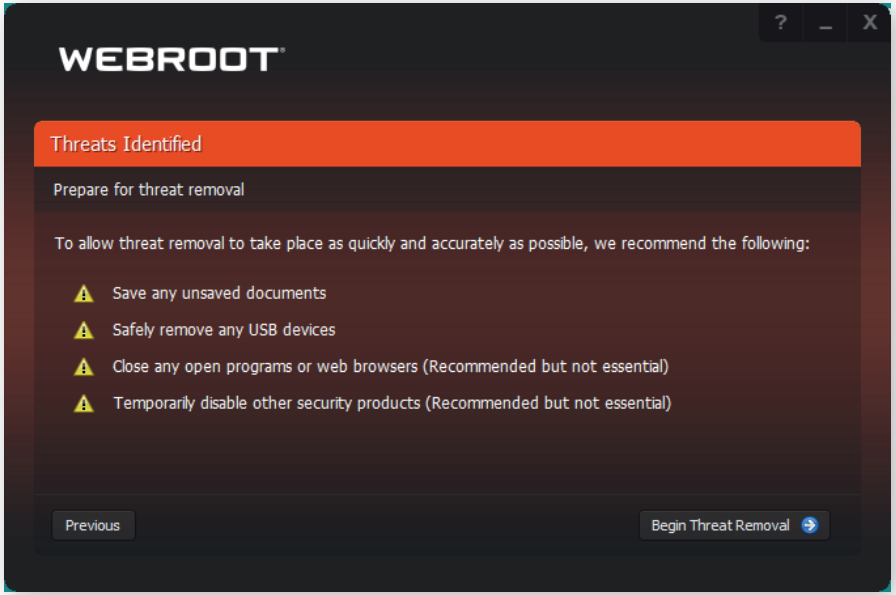
Ataki wymuszające okup

Organizacja, która utraci dostęp do danych może mieć poważny problem wizerunkowy i finansowy z powodu kar wynikających z tak zwanego RODO – rozporządzenia o ochronie danych osobowych. Ataki z udziałem próbek ransomware są ciągle popularne. Hakerzy koncentrują się głównie na średnich i dużych organizacjach, nie wykluczając państwowych instytucji. Przestępcze działania stały się groźniejsze, ponieważ wzrasta sprzedaż wykradzionych zawartości plików na forach w sieci Tor.

Techniki bezplikowego infekowania systemów IT

We współczesnych systemach operacyjnych są już wbudowane narzędzia, z których korzystają przestępcy, dlatego nie muszą oni instalować złośliwych programów. Skrypt w PowerShell jest łatwy do zaciemnienia, przez co może być trudniejszy do wykrycia za pomocą starszych narzędzi bezpieczeństwa. Administratorzy powszechnie używają PowerShell do automatyzowania pewnych czynności. W środowisku korporacyjnym działanie procesów systemowych, takich jak PowerShell lub Windows Management Instrumentation, nie jest niczym niezwykłym.

Hakerzy w ukierunkowanych kampaniach mają duże pole do popisu, ponieważ skrupulatnie przygotowują się do ataku. Zwykle „cykl życia ataku cybernetycznego” (ang. kill chain) przebiega następująco: najpierw rozpoznaje się cel, następnie dostosowuje narzędzia pod systemy IT ofiary. Ostatnim etapem jest atak i przerwanie łańcucha. Ukierunkowane ataki ATP (Advanced Threat Persistence) są trudniejsze do wykrycia i zatrzymania. Nieszablonowe techniki omijania zabezpieczeń, jeżeli zostaną użyte w kontrolowanym środowisku, mogą dużo powiedzieć o skuteczności ochrony danego produktu. Przestępcom najbardziej zależy na pieniądzach, dlatego większość kampanii kierowanych jest do masowego odbiorcy. Systemy IT, które są chronione rekomendowanymi rozwiązaniami, znajdują się w uprzywilejowanej pozycji do atakującego.



WEBROOT®
Smarter Cybersecurity™

Nazwa produktu:
WEBROOT Endpoint Protection
Data testu: kwiecień 2020

WEBROOT Endpoint Protection w sposób nowatorski wykorzystuje potencjał chmury obliczeniowej Webroot Intelligence Network. Podejrzane aplikacje są monitorowane na czas ich działania i w razie potrzeby są blokowane. Rozwiązanie doskonale poradziło sobie ze wszystkimi próbkami złośliwych dokumentów Office. Niestety podczas testowania próbek ransomware kontrolowane procesy ciągle miały dostęp do Internetu, dlatego szkodliwe oprogramowanie mogło komunikować się z serwerem C&C. Ten problem można naprawić zwiększając domyślny poziom ustawień ochrony heurystycznej w polityce bezpieczeństwa agenta antywirusowego.

Szczegóły techniczne

POZIOM 1	P1	Poziom przeglądarki, czyli wirus został zatrzymany przed albo tuż po pobraniu na dysk.
POZIOM 2	P2	Poziom systemu, czyli wirus został pobrany, ale nie dopuszczono do uruchomienia.
POZIOM 3	P3	Poziom analizy, czyli wirus został uruchomiony i zablokowany przez testowany produkt.
NIEPOWODZENIE	N	Niepowodzenie, czyli wirus nie został zablokowany i zainfekował system.

LP.	MAKROWIRUSY	NAZWA PLIKU	WEBROOT Endpoint Protection
1	c141a187c5b2c7a8d91a923a0f79a8ba4c1484e7295f922c5fac3d7c0d6792b9	1.doc	P3
2	276e5e230766222ed208b1d4d1bd994acc2e763ca71c6d28f41a17988375d099	2.doc	P3
3	23a4d7782a91e2a297f8b082500a6036048940afbee12a951dc02da2a0004ec2	3.doc	P3
4	6bed7ef049d8d9728a09a94488ac8670c9c20c0e6c294f80fd2153c37a2bead7	4.doc	P3
5	dc0699e81874193e461b6a2ca9bf7164c2fe4d214381d1b5b875203541efcab7	5.doc	P3

Aby dowiedzieć się więcej o szczegółach technicznych, prosimy o kontakt.

Szczegóły techniczne

POZIOM 1	P1	Poziom przeglądarki, czyli wirus został zatrzymany przed albo tuż po pobraniu na dysk.
POZIOM 2	P2	Poziom systemu, czyli wirus został pobrany, ale nie dopuszczono do uruchomienia.
POZIOM 3	P3	Poziom analizy, czyli wirus został uruchomiony i zablokowany przez testowany produkt.
NIEPOWODZENIE	N	Niepowodzenie, czyli wirus nie został zablokowany i zainfekował system.

LP.	RANSOMWARE	NAZWA PLIKU	WEBROOT Endpoint Protection
1	3320f11728458d01eef62e10e48897ec1c2277c1fe1aa2d471a16b4dccfc1207	1.exe	P1
2	3299f07bc0711b3587fe8a1c6bf3ee6bcbc14cb775f64b28a61d72ebcb8968d3	2.exe	P1
3	86456ebf6b807e8253faf1262e7a2b673131c80174f6133b253b2e5f0da442a9	3.exe	P1
4	9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1	4.exe	P1
5	4e6c191325b37da546e72f4a7334d820995d744bf7bb1a03605adb3ad30ce9ca	5.exe	P1

Aby dowiedzieć się więcej o szczegółach technicznych, prosimy o kontakt.

Szczegóły techniczne

	ATAKI BEZPLIKOWE	NAZWA PLIKU	WEBROOT Endpoint Protection
POWERSHELL ATTACK	c1525592fdf22f2ea068b5e2428d5e36fd9629ef8f5dd648ee792b4cb936fe53	1.bat	Atak nie został zablokowany na żadnym z etapów*
HTA ATTACK	e43ac1a50122d5f8584d21d768ea171d1f5f78075bbb73ae178506b6f8d071cb	2.hta	Atak nie został zablokowany na żadnym z etapów*

*Producent bardzo szybko zareagował na nasze zgłoszenie.
W dniu publikacji tego raportu oprogramowanie już chroni przed takimi atakami.

Aby dowiedzieć się więcej o szczegółach technicznych, prosimy kierować swoje zapytania na adres: kontakt@avlab.pl

Nazwa produktu: WEBROOT Endpoint Protection
Data testu: kwiecień 2020

WEBROOT Smarter Cybersecurity™

Przyznane rekomendacje w kategoriach

AV LAB AWARD BEST+++

Ochrona przed złośliwymi dokumentami Office

Zablokowanych zagrożeń in the wild **65/65**

AV LAB ONLY TESTED

Ochrona przed zaszyfrowaniem danych

Zablokowanych zagrożeń in the wild **18/24**

AV LAB ONLY TESTED

Ochrona przed atakami bezplikowymi

Zablokowanych scenariuszy ataków **0/2***

*Producent bardzo szybko zareagował na nasze zgłoszenie. W dniu publikacji tego raportu oprogramowanie już chroni przed takimi atakami.

THE INDEPENDENT ANTIVIRUS TESTS

AVLab jako niezależna organizacja stojąca na straży bezpieczeństwa w Internecie zajmuje się dostarczaniem informacji z branży poprzez artykuły, relacje ze szkoleń i konferencji. Naszą cechą rozpoznawczą profesjonalne recenzje i testy bezpieczeństwa, które przeprowadzamy w warunkach zbliżonych do rzeczywistości. W testach wykorzystujemy szkodliwe oprogramowanie narzędzia i techniki obchodzenia zabezpieczeń, które są używane w prawdziwych atakach.

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