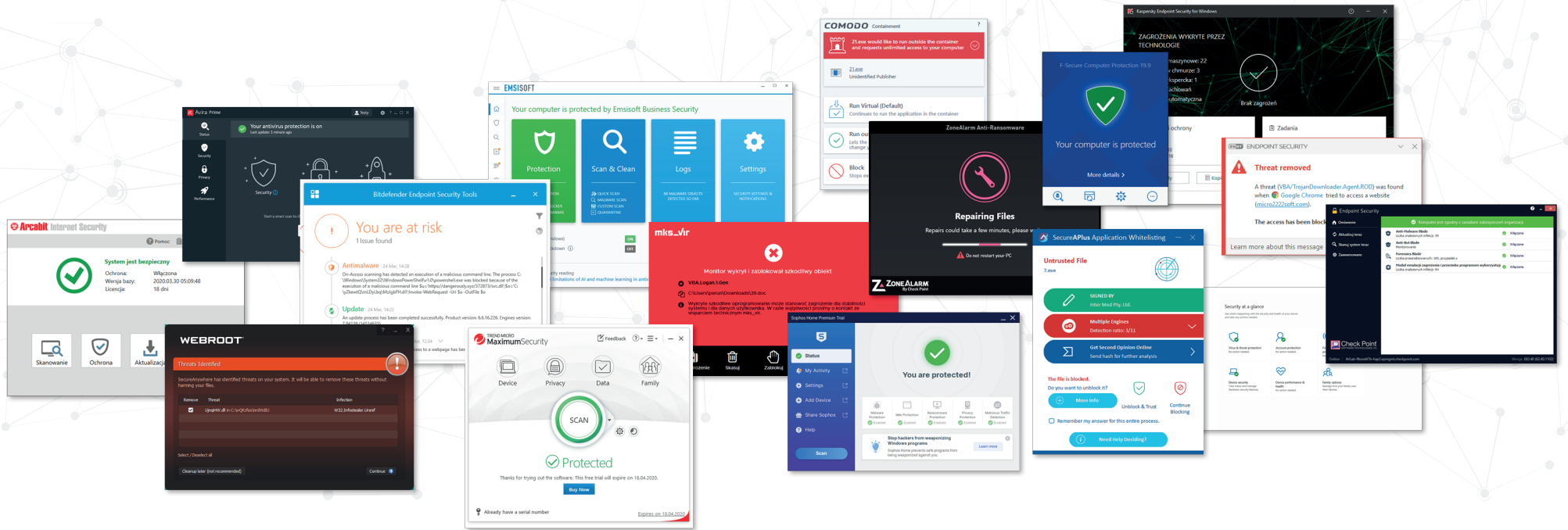




THE INDEPENDENT ANTIVIRUS TESTS



Data testu: kwiecień 2020

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 uruchomienia 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 powinni 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. Przemocne 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 pieniądzu, dlatego większość kampanii kierowanych jest do masowego odbiorcy. Systemy IT, które są chronione rekomendowanymi rozwiązaniami, znajdują się w uprzywilejowanej pozycji do atakującego.

# Makrowirusy - szczegóły techniczne

LP.	MAKROWIRUSY	NAZWA PLIKU
1	c141a187c5b2c7a8d91a923a0f79a8ba4c1484e7295f922c5fac3d7cod6792b9	1.doc
2	276e5e230766222ed208b1d4d1bd994acc2e763ca71c6d28f41a17988375d099	2.doc
3	23a4d7782a91e2a297f8b082500a6036048940afbee12a951dc02da2a0004ec2	3.doc
4	6bed7ef049d8d9728a09a94488ac8670c9c20c0e6c294f80fd2153c37a2bead7	4.doc
5	dc0699e81874193e461b6a2cagbf7164c2fe4d214381d1b5b875203541efcab7	5.doc
6	174e0317f0e0f1d0b7aa5f9fdg9bf476b8ag10d067effeadfa2eagebfcd03a46	6.doc
7	db29ff54d37ebd7694c5190fc3ddbocfffd896c7ed43b3f4abb8ab28658ff955	7.doc
8	bg8a210cb0682233e9b26bf11137456f9c93b2ed49bd15a903a88171fe754f87	8.doc
9	620b091c4d2e1da67922cba308d9d88c2e7d9de10bda08384f597f3cb1e2e3cd	9.doc
10	8e76efb8ca44047f31a9933cb281a119905ec7e390b774ac2493d5c29bbdcbe5	10.doc
	...	
65	6a864e0fc61af9a2a824654ebd6165c9ced5e9ccb2a4e6d0bd8bec7d2a83766e	65.xls



## POZIOM 1

Poziom przeglądarki, czyli wirus został zatrzymany przed albo tuż po pobraniu na dysk.



## POZIOM 2

Poziom systemu, czyli wirus został pobrany, ale nie dopuszczono do uruchomienia.



## POZIOM 3

Poziom analizy, czyli wirus został uruchomiony i zablokowany przez testowany produkt.



## NIEPOWODZENIE

Niepowodzenie, czyli wirus nie został zablokowany i zainfekował system.

# Makrowirusy

Liczba porządkowa testowanej próbki złośliwego oprogramowania

NAZWA PROGRAMU	1	2	3	4	5	6	7	8	9	10	...	65	ZABLOKOWANYCH ZAGROZEŃ	PRZYZNANY CERTYFIKAT
ARCABIT Internet Security	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P3	65/65	
AVIRA Antivirus Pro	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P3	65/65	
AVIRA Prime	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P3	65/65	
BITDEFENDER GravityZone Elite	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P1	65/65	
CHECK POINT Endpoint Security	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P3	65/65	
COMODO Advanced Endpoint Protection	P3	P3	P3	P3	P2	P3	P3	P2	P2	P2		P3	65/65	
COMODO Internet Security	P3	P3	P3	P3	P2	P3	P3	P2	P2	P2		P3	65/65	
EMSISOFT Anti-Malware	P3	P3	P3	P3	P3	P3	P3	P3	P3	P3		P3	65/65	
EMSISOFT Business Security	P3	P3	P3	P3	P3	P3	P3	P3	P3	P3		P3	65/65	
ESET Endpoint Protection Advanced Cloud	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P1	65/65	

Liczba porządkowa testowanej próbki złośliwego oprogramowania

NAZWA PROGRAMU	1	2	3	4	5	6	7	8	9	10	...	65	ZABLOKOWANYCH ZAGROZEŃ	PRZYZNANY CERTYFIKAT
F-SECURE Protection Service for Business	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P3	65/65	
G DATA Endpoint Protection Business	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P1	65/65	
KASPERSKY Endpoint Security Cloud	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P3	65/65	
MKS_VIR Internet Security	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P3	65/65	
SECUREPLUS Pro	P3	P3	P3	P3	P3	P3	P3	P3	P3	P3		P3	65/65	
SOPHOS Home Premium	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P3	65/65	
TREND MICRO Maximum Security	P2	P3	P1	P1	P1	P1	P1	P1	P1	P1		P3	62/65	
WEBROOT SecureAnywhere Antivirus	P3	P3	P3	P3	P3	P3	P3	P3	P3	P3		P3	65/65	
WEBROOT Endpoint Protection	P3	P3	P3	P3	P3	P3	P3	P3	P3	P3		P3	65/65	
WINDOWS Defender Antivirus	P3	P3	P3	P3	P3	P3	P3	P3	P3	P3		P3	60/65	
ZONEALARM Extreme Security	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P1	65/65	

# Ransomware - szczegóły techniczne

LP.	RANSOMWARE	NAZWA PLIKU
1	3320f11728458d01eef62e10e48897ec1c2277c1fe1aa2d471a16b4dccfc1207	1.exe
2	3299f07bc0711b3587fe8a1c6bf3ee6bcbbc14cb775f64b28a61d72ebcb8968d3	2.exe
3	86456ebf6b807e8253faf1262e7a2b673131c80174f6133b253b2e5f0da442a9	3.exe
4	9a4e4211f7e690ee4a520c491ef7766dcf1cc9859afa991e15538e92b435f3a1	4.exe
5	4e6c191325b37da546e72f4a7334d820995d744bf7bb1a03605adb3ad30ce9ca	5.exe
6	b933cb32689517aac6e459d33e9d8c7c8f31f0710008bfa09d9e91c2526826ef	6.exe
7	d4492a9eb36f87a9b3156b59052ebaf10e264d5d1ce4c015a6b0d205614e58e3	7.exe
8	3759f8774aee2d6185b02489612382797b110ed7b5fc39edda9665c3152cbddc	8.exe
9	9ca0776e3c226e4ebb4c8c08ea750e6dbc22e447dea68e1e8795b5d5691472c0	9.exe
10	8639825230d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160	10.exe
	...	
24	29e5da1f13de425e105f065be573793c41e5bf693cf874cdaac69bd85c499dfd	24.exe



## POZIOM 1

Poziom przeglądarki, czyli wirus został zatrzymany przed albo tuż po pobraniu na dysk.



## POZIOM 2

Poziom systemu, czyli wirus został pobrany, ale nie dopuszczono do uruchomienia.



## POZIOM 3

Poziom analizy, czyli wirus został uruchomiony i zablokowany przez testowany produkt.



## NIEPOWODZENIE

Niepowodzenie, czyli wirus nie został zablokowany i zainfekował system.

# Ransomware

Liczba porządkowa testowanej próbki złośliwego oprogramowania

NAZWA PROGRAMU	1	2	3	4	5	6	7	8	9	10	...	24	ZABLOKOWANYCH ZAGROZEŃ	PRZYZNANY CERTYFIKAT
ARCABIT Internet Security	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P1	24/24	
AVIRA Antivirus Pro	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P1	24/24	
AVIRA Prime	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P1	24/24	
BITDEFENDER GravityZone Elite	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P1	24/24	
CHECK POINT Endpoint Security	P2	P1	P1	P1	P1	P1	P1	P1	P1	P1		P1	24/24	
COMODO Advanced Endpoint Protection	P1	P1	P1	P1	P3	P1	P3	P1	P3	P3		P3	24/24	
COMODO Internet Security	P1	P1	P1	P1	P3	P1	P3	P1	P3	P3		P3	24/24	
EMSISOFT Anti-Malware	P3	P3	P3	P3	P3	P3	P3	P3	P3	P3		P3	24/24	
EMSISOFT Business Security	P3	P3	P3	P3	P3	P3	P3	P3	P3	P3		P3	24/24	
ESET Endpoint Protection Advanced Cloud	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P1	24/24	

Liczba porządkowa testowanej próbki złośliwego oprogramowania

NAZWA PROGRAMU	1	2	3	4	5	6	7	8	9	10	...	24	ZABLOKOWANYCH ZAGROZEŃ	PRZYZNANY CERTYFIKAT
F-SECURE Protection Service for Business	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P1	24/24	
G DATA Endpoint Protection Business	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P1	24/24	
KASPERSKY Endpoint Security Cloud	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P1	24/24	
MKS_VIR Internet Security	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P1	24/24	
SECUREPLUS Pro	P3	P3	P3	P3	P3	P3	P3	P3	P3	P3		P3	24/24	
SOPHOS Home Premium	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P1	24/24	
TREND MICRO Maximum Security	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P1	24/24	
WEBROOT SecureAnywhere Antivirus	P1	P1	P1	P1	P1	P1	N	P1	N	P3		P1	18/24	
WEBROOT Endpoint Protection	P1	P1	P1	P1	P1	P1	N	P1	N	P1		P1	18/24	
WINDOWS Defender Antivirus	P3	P2	N	N	P1	P1	N	P1	P3	P1		P3	20/24	
ZONEALARM Extreme Security	P1	P1	P1	P1	P1	P1	P1	P1	P1	P1		P1	24/24	

# Ataki bezplikowe - szczegóły techniczne

LP.	ATAKI BEZPLIKOWE	NAZWA PLIKU
1	c1525592fdf22f2ea068b5e2428d5e36fd9629ef8f5dd648ee792b4cb936fe53	1.bat
2	e43ac1a50122d5f8584d21d768ea171d1f5f78075bbb73ae178506b6f8d071cb	2.hta

**P1**

POZIOM 1

Poziom przeglądarki, czyli wirus został zatrzymany przed albo tuż po pobraniu na dysk.

**P2**

POZIOM 2

Poziom systemu, czyli wirus został pobrany, ale nie dopuszczono do uruchomienia.

**P3**

POZIOM 3











Poziom analizy, czyli wirus został uruchomiony i zablokowany przez testowany produkt.












**N**

NIEPOWODZENIE

Niepowodzenie, czyli wirus nie został zablokowany i zainfekował system.

# Ataki bezplikowe

NAZWA PROGRAMU	POWERSHELL ATTACK	MSHTA ATTACK	ZABLOKOWANYCH ATAKÓW	PRZYZNANY CERTYFIKAT
ARCABIT Internet Security	Złośliwe polecenie zostało uruchomione, ale zapora sieciowa Arcabit zablokowała atak	Atak został zablokowany w przeglądarce	2/2	
AVIRA Antivirus Pro	Zagrożenie zostało zablokowane podczas dostępu do pliku	Atak nie został zablokowany na żadnym z etapów*	1/2	
AVIRA Prime	Zagrożenie zostało zablokowane podczas dostępu do pliku	Atak nie został zablokowany na żadnym z etapów*	1/2	
BITDEFENDER GravityZone Elite	Zagrożenie zostało zablokowane podczas dostępu do pliku	Atak został zablokowany w przeglądarce	2/2	
CHECK POINT Endpoint Security	Zagrożenie zostało zablokowane podczas dostępu do pliku	Zagrożenie zostało uruchomione, ale spowodowało to wszczęcie alarmu Check Point	2/2	
COMODO Advanced Endpoint Protection	Zagrożenie zostało zablokowane podczas dostępu do pliku	Zagrożenie zostało zablokowane podczas dostępu do pliku	2/2	
COMODO Internet Security	Zagrożenie zostało zablokowane podczas dostępu do pliku	Atak nie został zablokowany na żadnym z etapów*	1/2	
EMSISOFT Anti-Malware	Zagrożenie zostało zablokowane podczas dostępu do pliku	Zagrożenie zostało zablokowane podczas dostępu do pliku	2/2	
EMSISOFT Business Security	Zagrożenie zostało zablokowane podczas dostępu do pliku	Zagrożenie zostało zablokowane podczas dostępu do pliku	2/2	
ESET Endpoint Protection Advanced Cloud	Zagrożenie zostało zablokowane podczas dostępu do pliku	Zagrożenie zostało zablokowane podczas dostępu do pliku	2/2	

NAZWA PROGRAMU	POWERSHELL ATTACK	MSHTA ATTACK	ZABLOKOWANYCH ATAKÓW	PRZYZNANY CERTYFIKAT
F-SECURE Protection Service for Business	Zagrożenie zostało zablokowane podczas dostępu do pliku	Zagrożenie zostało zablokowane przez moduł DeepGuard	2/2	
G DATA Endpoint Protection Business	Zagrożenie zostało zablokowane podczas dostępu do pliku	Zagrożenie zostało zablokowane podczas dostępu do pliku	2/2	
KASPERSKY Endpoint Security Cloud	Zagrożenie zostało zablokowane podczas dostępu do pliku	Atak został zablokowany w przeglądarce	2/2	
MKS_VIR Internet Security	Zagrożenie zostało uruchomione, ale firewall mks_vir zablokował połączenie z serwerem hakera	Atak został zablokowany w przeglądarce	2/2	
SECUREPLUS Pro	Zagrożenie zostało uruchomione, ale spowodowało to wszczęcie alarmu SecureAPlus	Zagrożenie zostało uruchomione, ale spowodowało to wszczęcie alarmu SecureAPlus	2/2	
SOPHOS Home Premium	Atak nie został zablokowany na żadnym z etapów	Atak został zablokowany w przeglądarce	1/2	
TREND MICRO Maximum Security	Zagrożenie zostało zablokowane podczas dostępu do pliku	Zagrożenie zostało uruchomione, ale spowodowało to wszczęcie alarmu Trend Micro	2/2	
WEBROOT SecureAnywhere Antivirus	Atak nie został zablokowany na żadnym z etapów	Atak nie został zablokowany *	0/2	
WEBROOT Endpoint Protection	Atak nie został zablokowany na żadnym z etapów	Atak nie został zablokowany *	0/2	
WINDOWS Defender Antivirus	Zagrożenie zostało uruchomione, ale zaporę sieciową zablokowała połączenie z serwerem hakera	Zagrożenie zostało uruchomione, ale spowodowało to wszczęcie alarmu antywirusa	2/2	
ZONEALARM Extreme Security	Zagrożenie zostało zablokowane podczas dostępu do pliku	Zagrożenie zostało uruchomione, ale spowodowało to wszczęcie alarmu ZoneAlarm	2/2	



AVIRA Antivirus Pro	Producent bardzo szybko zareagował na nasze zgłoszenie. W dniu publikacji tego raportu oprogramowanie już chroni przed tego rodzaju atakami.
AVIRA Prime	Producent bardzo szybko zareagował na nasze zgłoszenie. W dniu publikacji tego raportu oprogramowanie już chroni przed tego rodzaju atakami.
COMODO Internet Security	Zagrożenie użyte w ataku zostało uruchomione w odizolowanym obszarze – piaskownicy Comodo. Zła wiadomość jest taka, że możliwe było przeglądanie zawartości dysku ofiary i kradzież plików.
WEBROOT SecureAnywhere Antivirus	Producent bardzo szybko zareagował na nasze zgłoszenie. W dniu publikacji tego raportu oprogramowanie już chroni przed takimi atakami.
WEBROOT Endpoint Protection	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](mailto:kontakt@avlab.pl)





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](mailto:kontakt@avlab.pl)