AV-LAB

THE INDEPENDENT ANTIVIRUS TESTS

test ochrony przed zagrożeniami ransomware

programy dla użytkowników domowych oraz małych i średnich przedsiębiorstw

październik 2016

Data testu: październik 2016

Konspekt

Celem badania przeprowadzonego przez AVLab w październiku 2016 roku było sprawdzenie rzeczywistej ochrony, jaką zapewniają aplikacje bezpieczeństwa użytkownikom indywidualnym oraz małym i średnim firmom przed szkodnikami z rodziny krypto-ransomware. Wyniki przedstawione w tym dokumencie odzwierciedlają faktyczną efektywność programów antywirusowych, które z wykorzystaniem wszystkich dostępnych składników ochrony i skorelowanych dynamicznych metod heurystycznych oraz behawioralnych, dostarczają urządzeniom końcowym kompleksową ochronę w czasie rzeczywistym, w tym detekcję nieznanych zagrożeń krypto-ransomware.

Chociaż niektóre z testowanych pakietów bezpieczeństwa umożliwiają wydzielenie specjalnego folderu, w którym zawarte tam pliki są w sposób ciągły monitorowane przed ich modyfikacją przez program antywirusowy, to celem tego testu było sprawdzenie, czy antywirusy radzą sobie ze współczesnymi nieznanymi zagrożeniami z rodziny krypto-ransomware. Ten szczep złośliwego oprogramowania jest niezwykle destrukcyjny w skutkach — często wyrządza straty finansowe oraz wpływa na produktywność firmy powodując zastój w prowadzeniu biznesu.

RANSOMWARE ORAZ KRYPTO-RANSOMWARE

Ransomware należy do tej rodziny szkodliwego oprogramowania, które uniemożliwiają lub ograniczają użytkownikom dostęp do systemu operacyjnego.

Współcześnie, zagrożenia ransomware przybrały inną nomenklaturę: krypto-ransomware. Wirusy te odpowiadają za szyfrowanie określonych typów plików, po czym wyświetlają komunikat z żądaniem okupu w zamian za odszyfrowanie danych.

Wśród najnowszych wariantów ransomware, możemy wyróżnić jeszcze jeden typ: disk-encryption. Te złośliwe aplikacje lub skrypty mające destrukcyjne działanie w stosunku do użytkownika komputera, szyfrują główny rekord ładujący Master Boot Record nadpisując go własnym, co powoduje restart systemu. W wyniku działania malware, wyświetlany jest fałszywy komunikat skanowania dysku w poszukiwaniu błędów (CHKDSK). W tym czasie, krypto-ransomware szyfruje plik Master File Table (MFT), w którym są zawarte wpisy do każdego pliku na danej partycji. Stąd też system operacyjny nie wie, gdzie zapisane są pliki, co uniemożliwia poprawne uruchomienie się komputera.

Użytkownicy mogą zainfekować swój system na różne sposoby. Krypto-ransomware najczęściej rozprzestrzenia się poprzez wiadomości e-mail, skrywając się pod postacią faktury, postępowania komorniczego lub informacji o niedostarczonej przesyłce pocztowej.

W ostatnich miesiącach, eksperci z FortiGuard Labs zauważyli, że jedna z najbardziej popularnych obecnie w Polsce odmian ransomware — Locky — jest pobierana za pośrednictwem trojana Nemucod. Z kolei analitycy malware, którzy pracują dla F-Secure Labs, zidentyfikowali cyberprzestępczą kampanię, w której do instalowania krypto-ransomware Cerber wykorzystywano luki w oprogramowaniu Adobe Flash za pośrednictwem narzędzia typu Exploit Kit Magnitude.

W kategorii dla użytkowników indywidualnych, najwyższe wyróżnienie otrzymały programy:

Arcabit Internet Security
Comodo Cloud Antivirus
Emsisoft Internet Security 11
Emsisoft Internet Security 12
Foltyn SecurityShield
F-Secure SAFE
G DATA Internet Security
Kaspersky Internet Security 2017
Qihoo 360 Total Security
SecureAPlus Premium
Trend Micro Internet Security 2017
Voodoo Shield Pro
Zemana Anti-Malware Premium
ZoneAlarm Internet Security Suite

W kategorii dla małych i średnich przedsiębiorstw, najwyższe wyróżnienie otrzymały programy:

Arcabit Endpoint Security
Comodo ONE Enterprise
Emsisoft Anti-Malware for endpoints
F-Secure Protection Service for Business
G DATA Client Security Business
Kaspersky Endpoint Security 10 for Windows
Seqrite Endpoint Security Enterprise Suite
Sophos Endpoint Protection

Metodologia

Aby zastosować się do zasady równości testów, zdecydowaliśmy się przetestować na ustawieniach domyślnych i w identycznym środowisku testowym wszystkie znane programy antywirusowe dla użytkowników indywidualnych oraz dla firm z sektora małych i średnich przedsiębiorstw, a także dwie niezależne aplikacje: Foltyn SecurityShield i Voodoo Shield Pro, które w kontekście do „tradycyjnych" antywirusów różnią się od nich operatywnością. Dzięki zachowaniu tej zasady, każda aplikacja została sprawdzona w takich samych warunkach i przy wykorzystaniu tego samego zestawu zagrożeń.

Do testu wykorzystano 28 plików szkodliwego oprogramowania typu krypto-ransomware. A były to m.in.: Cerber, CryptXXX, DetoxCrypto, Hitler Ransomware, HolyCrypt, Locky, Numecod, Petya, Jigsaw, Vipasana, Stampado i wiele innych. Materiał badawczy w łącznej ilości 28 próbek skompletowano we współpracy z niezależnymi badaczami.

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.

Jedyną sprawiedliwą metodą testów porównawczych jest badanie wszystkich aplikacji w takich samych warunkach i na takich samych zasadach — a więc na ustawieniach domyślnych. Na rynku istnieją już antywirusy, które posiadają specjalne mechanizmy monitorujące pliki lub foldery przed ich zaszyfrowaniem, jednak nie wszyscy producenci zdecydowali się na włączenie tych składników w domyślnym trybie. Rodzi to nasze podejrzenia, że mechanizmy te mogłyby zbyt mocno wpływać na ogólną wydajność pakietu zabezpieczającego, obniżając jego wyniki w testach wydajnościowych.

Dlatego, aby sprawdzić skuteczność ochrony najpopularniejszych programów antywirusowych dla firm i dla domu, przygotowaliśmy obraz systemu Windows 10 Professional x64 z najnowszymi aktualizacjami na dzień przed rozpoczęciem testu. Dzięki temu, wszystkie produkty zostały przebadane w identycznym środowisku testowym i w czasie testu mogły korzystać z Internetu.

Algorytm działania

1. Dla każdego testowanego programu odtwarzano obraz systemu przed każdym uruchomieniem zainfekowanego pliku, dzięki czemu wiernie odwzorowano środowisko pracy dla każdej aplikacji.
2. Jeśli było to wymagane, udzielano zezwolenia na uruchomienie malware z uprawnieniami administratora.
3. Testowane programy miały za zadanie nie dopuścić do zaszyfrowania przygotowanego zestawu plików, które umieszczono na pulpicie.

DLACZEGO KRYPTO-RANSOMWARE SPRAWIA PROBLEMY UŻYTKOWNIKOM INDYWIDUALNYM?

Bitdefender opublikował raport z ankiety przeprowadzonej w listopadzie 2015 roku wśród 3009 internautów z USA, Francji, Niemiec, Danii, Wielkiej Brytanii oraz Rumunii, w którym zostały poruszone kwestie wirusów z rodziny ransomware i krypto-ransomware (szkodników, które szyfrują pliki i żądają okupu za odzyskanie danych). Kluczowe wnioski z ankiety to:

- 50 procent ankietowanych osób nie wie, czym są zagrożenia z rodziny ransomware.
- Nawet połowa respondentów jest gotowa zapłacić do 500 dolarów za możliwość odszyfrowania plików.
- Najważniejsze dla użytkowników są osobiste dokumenty, które widnieją na pierwszej pozycji na liście „najcenniejszych" danych dla zwykłych obywateli danego kraju.
- Użytkownicy z Wielkiej Brytanii i Rumunii są skłonni płacić najwięcej za odzyskanie plików.
- W 2015 roku użytkownicy ze Stanów Zjednoczone byli głównymi ofiarami krypto-ransomware.

Testowane programy

Oprogramowanie dla użytkowników indywidualnych:

Produkt	Wersja
Ad-Aware Free Antivirus+	11.12.945.9202
Arcabit Internet Security	2016.00.248
Avast Free Antivirus 2016	12.3.2280
Avast Internet Security 2016	12.3.2280
AVG AntiVirus Free Edition	16.121.7858
AVG Internet Security	16.121.7858
Avira Free Antivirus	15.0.22.54
Avira Internet Security Suite	15.0.22.54
Bitdefender Antivirus Free Edition	1.0.3.9
Bitdefender Internet Security 2017	21.0.18.898
Comodo Cloud Antivirus	1.6.400657.347
Comodo Internet Security 8	8.4.0.5165
Comodo Internet Security Pro 10 (BETA)	10.0.0.5144
Dr Web Katana	1.01.07290
Dr. Web Space Security	11.03.09220
Emsisoft Internet Security 11	11.10
Emsisoft Internet Security 12	12.0
ESET Smart Security 9	9.0.385.1
ESET Smart Security 10 (BETA)	10.0.171.0
Foltyn SecurityShield	1.0.0
FortiClient Free	5.4.1.0840
F-Secure SAFE	16.3
G DATA Internet Security	25.2.0.3
Kaspersky Internet Security 2017	17.0.0.611
Malwarebytes Anti-Malware Premium	2.2.1.1043
Malwarebytes Anti-Ransomware (BETA)	0.9.17.661
McAfee LiveSafe	15.1.156
Norton Security	22.8.0.50
Panda Free Antivirus	17.00.01.0000
Panda Internet Security	17.00.01.0000
Qihoo 360 Total Security	8.8.0.1080
SecureAPlus Premium	4.3.3
Sophos HOME	10.5.4
Trend Micro Internet Security 2017	11.0.158
TrustPort Internet Security	2016.16.02.5698
Voodoo Shield Pro	3.45 (beta)
Webroot SecureAnywhere Complete	9.0.13.50
Zemana Antimalware Premium	2.50.133
ZoneAlarm Internet Security Suite	15.0.123.17051
Windows Defender	4.10.14393.0

DLACZEGO CYBERPRZESTĘPCY INTERESUJĄ SIĘ FIRMAMI ORAZ INSTYTUCJAMI PUBLICZNYMI?

Firmy utożsamiane są z pieniądzem.

Cyberprzestępcy zdają sobie sprawę, że jakiś procent ofiar i tak zapłaci okup.

Zaszyfrowane dane są zbyt cenne, aby mogły zostać spisane na straty.

Firmowe urządzenia są często niewystarczająco zabezpieczone.

Najsłabszym ogniwem w łańcuchu bezpieczeństwa jest człowiek (czyt. pracownik).

Pracownik łatwo pada ofiarą socjotechniki.

Niektóre warianty krypto-ransomware szyfrują pliki nie tylko na dyskach lokalnych, ale także w chmurze i w sieci lokalnej.

Większość firm nie zgłosi ataku w obawie przed zetknięciem się z organami ścigania i utratą reputacji.

Małe firmy są nieprzygotowane na zaawansowane ataki.

Małe firmy nie panują nad użytkownikami: nie uwzględniają trendu „BYOD" oraz „SHADOW IT".

Publiczne i rządowe instytucje zarządzają dużymi bazami danych, które zawierają cenne informacje nadające się na sprzedaż.

Poziom ochrony publicznych instytucji jest niższy niż sektora prywatnego.

Pracownicy sektora publicznego są w niewystarczającym stopniu przeszkoleni.

Instytucje publiczne często korzystają z przestarzałego oprogramowania.

Sektor publiczny od dawna cierpi na deficyt ekspertów od bezpieczeństwa teleinformatycznego.

Rozwiązania dla małych i średnich przedsiębiorstw:

Produkt	*Wersja*
Arcabit Endpoint Security	2016.00.248
AVAST for Business Endpoint Security	12.3.2515
AVAST for Business Basic Antivirus	12.3.2515
AVG AntiVirus Business Edition	2016.111.7797
Avira Antivirus for Endpoint	15.0.22.54
Bitdefender GravityZone	6.2.10.883
Comodo ONE Enterprise	8.3.0.5191
Emsisoft Anti-Malware for Endpoints	11.10
ESET Endpoint Security	6.4.2014.2
F-Secure Protection Service for Business	12.0.1
G DATA Client Security Business	14.0.0.641
Kaspersky Endpoint Security 10 for Windows	10.2.5.3201
Kaspersky Anti-Ransomware Tool for Business	1.1.24.0
Panda Adaptive Defense	7.62.0
Seqrite Endpoint Security Enterprise Suite	17.00
Sophos Endpoint Protection	11.5.1
Trend Micro Worry-Free Business Security	19.0.2166

AV-LAB
THE INDEPENDENT ANTIVIRUS TESTS

Produkt — *Wyniki rozwiązań przeznaczonych dla użytkowników indywidualnych oraz mikro firm.*

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Ad-Aware Free	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	0/0	1	1	0/0	1	1	1	0/0	1
Arcabit Internet Security	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	0/1	1	1	0/1	1	1	1	0/1	1
Avast Free Antivirus	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	0/0	1	1	1	1	1
Avast Internet Security	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	0/0	1	1	1	1	1
AVG AntiVirus Free	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	1	1	1	1	1	1	1	0/0	1
AVG Internet Security	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	1	1	1	1	1	1	1	0/0	1
Avira Free Antivirus	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	1	1	0/0	0/0	1	1	0/0	1	1	0/0	0/0	1
Avira Internet Security	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	0/1	1	1	0/1	1	1	1	1	1
Bitdefender Free	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	1	0/0	1	1	1	0/1	1
Bitdefender IS 2017	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	0/1	1	1	0/0	1	1	1	0/1	1
Comodo Cloud Antivirus	0/1	1	0/1	0/1	1	1	0/1	0/1	1	1	1	1	0/1	1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	1	0/1	1	0/1	1
Comodo IS 8	1	1	0/1	0/1	1	1	0/1	0/1	1	1	1	1	0/1	1	1	0/1	0/1	0/1	0/1	0/1	0/0	0/0	0/1	1	0/1	1	0/1	1
*Comodo IS Pro 10 (BETA)**	1	1	0/0	0/0	1	1	0/0	0/0	1	1	1	1	0/0	1	1	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	1	0/0	1	0/0	1
Dr. Web Katana	0/1	0/1	0/1	0/1	0/1	0/0	0/0	0/1	0/1	0/1	0/1	0/1	0/0	0/1	0/1	0/1	0/1	0/1	0/1	0/0	0/0	0/0	0/1	0/1	0/1	0/1	0/0	0/1
Dr. Web Space Security	1	1	1	1	1	1	0/1	1	1	1	1	1	0/0	1	1	1	1	1	1	1	0/1	1	1	1	1	1	1	1
Emsisoft IS 11	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	0/1	1	1	0/1	1	1	1	0/1	1
Emsisoft IS 12	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	0/1	1	1	0/1	1	1	1	0/1	1
ESET Smart Security 9	1	1	1	1	1	1	1	1	1	1	1	1	0/0	1	1	1	1	1	0/0	1	1	1	1	1	1	1	0/0	1
ESET SS 10 (BETA)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	1	1	1	1	1	1	1	1	1
Foltyn SecurityShield	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1
FortiClient Free	1	1	1	0/1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	0/0	0/1	1	1	0/0	1	0/0	1	1	1
F-Secure SAFE	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	0/1	1	1	0/1	1	1	1	1	1
G DATA Internet Security	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	0/1	1	1	0/1	1	1	1	0/1	1
Kaspersky IS 2017	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	1	1	0/1	1	0/1	1	1	1
MBAM Premium	1	1	1	1	1	1	0/0	0/1	1	1	1	1	1	1	1	0/0	1	0/1	0/0	0/1	0/1	0/1	1	1	0/0	0/0	1	1
MBAM Anti-R. (BETA)	0/0	0/1	0/1	0/1	0/0	0/0	0/0	0/0	0/0	0/0	0/1	0/1	0/0	0/0	0/0	0/0	0/1	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/1	0/0	0/0
McAfee LiveSafe	1	1	1	1	1	1	0/1	0/1	1	1	1	1	1	1	1	0/0	1	0/1	0/0	0/0	0/1	0/1	0/0	1	0/1	0/0	1	1
Norton Security	1	1	1	1	1	1	0/1	1	1	1	1	1	1	1	1	1	1	0/1	0/0	0/1	0/1	1	0/0	1	0/0	1	1	1
Panda Free Antivirus	1	1	1	1	1	1	0/1	0/1	1	1	1	1	1	1	0/1	0/0	1	1	0/0	0/0	0/0	0/0	0/0	1	1	0/1	1	1
Panda Internet Security	1	1	1	1	1	1	0/1	0/1	1	1	1	1	1	1	0/1	0/0	1	1	0/0	0/1	0/1	0/1	0/0	1	1	1	1	1
Qihoo 360 Total Security	1	1	0/1	1	1	1	1	0/1	1	1	1	1	1	1	1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	1	0/1	0/1	1	1

SecureAPlus Premium	0/1	1	0/1	0/1	1	1	0/1	0/1	1	1	1	1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	1	0/1	0/1	0/1	0/1
Sophos HOME	1	1	1	1	1	1	0/1	1	1	1	1	1	1	1	1	0/0	1	0/1	0/0	1	0/1	1	0/0	1	0/1	0/1	1	1
Trend Micro IS 2017	1	1	1	1	1	1	1	1	1	1	1	0/1	1	1	1	0/1	1	0/1	0/1	1	1	1	0/1	1	0/1	0/1	1	1
TrustPort IS	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	1	1	1	0/0	1	1	1	1	1
*Voodoo Shield Pro**	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1
Webroot SA Complete	0/1	1	1	1	1	1	0/1	0/1	1	1	1	1	0/0	1	0/1	0/0	1	0/1	0/0	1	0/1	0/1	0/0	0/1	0/1	0/1	0/0	0/1
Zemana AM Premium	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	0/1	0/1	1	1	1	1	1
ZoneAlarm Internet Security Suite	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	1	1	1	0/1	1	0/1	1	1	1
Windows Defender	1	1	1	1	1	1	0/0	0/0	0/0	1	1	0/0	0/0	0/0	1	1	0/0	0/0	0/0	1	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0

0/0: pliki zostały zaszyfrowane, ochrona była nieskuteczna
0/1: plik został uruchomiony i wyraźnie zablokowany z wykorzystaniem ochrony proaktywnej
1: plik został uruchomiony i zablokowany skanowaniem dostępowym

* Voodoo Shield Pro przetestowano w dwóch trybach: tryb AutoPilot ON i ApplicationWhitelist (SMART, ALWAYS ON). W obu przypadkach uzyskano identyczne wyniki.

* Oprogramowanie Comodo Internet Security Pro 10 w wersji BETA nie respektowało ustawień modułu automatycznej piaskownicy (Auto-Sandbox), która stanowi trzon ochrony w walce z nieznanymi złośliwym oprogramowaniem. W czasie testów, wersja stabilna nie była jeszcze dostępna, dlatego prosimy nie stawiać znaku równości pomiędzy wynikami wersji BETA a wersją stabilną Comodo Internet Security Pro 10.

Produkt	Wyniki rozwiązań przeznaczonych dla małych i średnich firm.																											
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Arcabit Endpoint Security	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	0/1	1	1	0/1	1	1	1	0/1	1
AVAST for Business Endpoint Security	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	1	1	1	1	1
AVAST for Business Basic Antivirus	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	1	1	1	1	1
AVG AntiVirus Business Edition	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	1	1	1	1	1	1	1	1	1
Avira Antivirus for Endpoint	1	1	1	1	1	1	0/1	0/1	1	1	1	1	1	1	1	0/1	1	1	0/0	0/1	0/1	0/1	0/0	1	1	0/1	0/1	1
Bitdefender GravityZone	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	1	1	1	0/0	1	1	1	1	1
Comodo ONE Enterprise	1	1	0/1	0/1	1	1	0/1	0/1	1	1	1	1	0/1	1	1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	1	0/1	1	0/1	1
Emsisoft Anti-Malware for endpoints	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	1	1	1	1
ESET Endpoint Security	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/0	1	1	1	0/0	1	1	1	1	1
F-Secure Protection Service for Business	1	1	1	1	1	1	0/1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	0/1	1	1	1	1	1
G DATA Client Security Business	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Kaspersky Endpoint Security 10 for Windows	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	1	1	1	1
Kaspersky Anti-Ransomware Tool for Business	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/0	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1
Panda Adaptive Defense	1	1	1	1	1	1	0/1	0/1	1	1	1	1	1	1	0/1	1	1	1	1	1	0/1	0/1	0/0	1	1	1	1	1
Seqrite Endpoint Security Enterprise Suite	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0/1	1	1	1	1	1
Sophos Endpoint Protection	0/1	1	1	1	1	1	0/1	0/1	1	1	1	1	1	1	0/1	1	1	1	1	1	0/1	0/1	1	1	1	1	1	1
Trend Micro Worry-Free Business Security	1	0/0	0/0	0/1	1	1	1	1	0/0	1	1	0/0	1	1	1	0/0	0/0	0/0	1	1	0/0	1	0/0	1	1	0/1	0/1	1

0/0: pliki zostały zaszyfrowane, ochrona była nieskuteczna
0/1: plik został uruchomiony i wyraźnie zablokowany z wykorzystaniem ochrony proaktywnej
1: plik został uruchomiony i zablokowany skanowaniem dostępowym

SAFESTORAGE W ARCABIT INTERNET SECURITY

Wielokrotnie testowane przez AVLab antywirusy Arcabit, jak większość aplikacji bezpieczeństwa, wykorzystuje monitor plików, poczty i przeglądarek. Jednak w odróżnieniu od innych konkurencyjnych i podobnych pakietów ochronnych, zaimplementowany przez producenta unikalny mechanizm SafeStorge szczególnie zwrócił naszą uwagę.

Niezwykle istotnym zastosowaniem mechanizmu SafeStorage jest ochrona danych przed często katastrofalnymi z punktu widzenia użytkownika efektami działań zagrożeń typu krypto-ransomware.

SafeStorage w momencie próby zaszyfrowania pliku tworzy jego kopię, pozwalając użytkownikowi lub administratorowi (SafeStorage uwzględnia też udostępnione zasoby sieciowe) w mniej niż minutę przywrócić zaszyfrowane dowolne pliki do stanu z przed infekcji. Ich kopie są przechowywane w wewnętrznej bazie pakietu Arcabit w formie spakowanej i zaszyfrowanej, która podlega ochronie w ramach wewnętrznych mechanizmów pakietu Arcabit — aplikacje zewnętrzne nie mają do nich dostępu.

W dodatku, SafeStorage posiada własny mechanizm porządkujący bazę i usuwający z niej pliki w momencie, w którym program zdecyduje, że potencjalnie zagrożenie dla ich zawartości ustąpiło. Pozwala to na oszczędne gospodarowanie miejscem na dysku (mechanizmy porządkujące SafeStorage są uruchamiane w momencie bezczynności użytkownika, żeby ograniczyć wpływ na wydajność systemu).

Pakiet bezpieczeństwa Arcabit przy instalacji pyta użytkownika, na którym dysku chce przechowywać bazę SafeStorage (oczywiście wtedy, gdy użytkownik posiada w systemie więcej dysków lub partycji). Można dzięki temu efektywnie kontrolować zużycie zasobów np. wtedy, gdy pierwszy dysk jest niezbyt pojemnym dyskiem SSD, natomiast drugi dysk to pojemny HDD, który np. w założeniach użytkownika służy właśnie do przechowywania danych.

SafeStorage pracuje synchronicznie względem zdarzeń w systemie plików tworząc kopie dokumentów, zdjęć i innych ważnych plików użytkownika w sytuacjach, które potencjalnie mogą stanowić zagrożenie dla ich zawartości. Synchroniczność pracy SafeStorage gwarantuje, że kopia pliku trafi do wewnętrznej bazy pakietu Arcabit w stanie nienaruszonym. Jednak kluczowe dla działania SafeStorage mechanizmy pracują w ramach sterownika w trybie jądra, co daje antywirusom marki Arcabit niepodważalną przewagę nad zagrożeniami szyfrującymi i innymi aplikacjami, które mogą (nawet tylko potencjalnie) uszkodzić zawartość plików użytkownika.

W kontekście bardzo skutecznej metody przywracania plików po ataku krypto-ransomware (i to bez posiadania kopii zapasowej plików na zewnętrznym nośniku), polecamy Arcabit Internet Security.


kwarantanna


SafeStorage


kopie zapasowe


menadżer procesów


audyt systemu


Arcabit Rescue Disk


czyszczenie systemu

Z CZEGO WYNIKAJĄ PROBLEMY UŻYTKOWNIKÓW?

Edukacja w zakresie bezpieczeństwa jest niewystarczająca, co odbija się na świadomości w kontekście manipulacji ze strony socjotechnicznych ataków.

Użytkownicy indywidualni tylko incydentalnie dbają o kopie zapasową swoich danych. To zupełnie inaczej niż małe i średnie przedsiębiorstwa.

Użytkownicy w niewystarczającym stopniu przykładają się do ochrony swoich plików i systemów.

Użytkownicy nie aktualizują na bieżąco zainstalowanego oprogramowania. Stwarza to potencjalne pole do popisu atakom z użyciem exploitów.

Użytkownicy są błędnie utwierdzeni w przekonaniu, że skoro nie klikają w nieodpowiednie linki oraz nie wchodzą na podejrzane strony, to nie mają się czego obawiać.

Użytkownicy nie są świadomi, że transparentne ataki drive-by oraz te exploit'ujące podatności w przeglądarce i zainstalowanym oprogramowaniu, nie wyświetlą żadnego alertu w systemie — no i w dodatku nie wymagają żadnej interakcji.

Zabezpieczone komputery oprogramowaniem antywirusowym same w sobie nie odpowiadają za bezpieczeństwo. Decyzyjność w tej kwestii nadal pozostaje w rękach użytkowników.

Interpretacja wyników

Na początku wspomnieliśmy, że zadaniem tego testu było wskazanie możliwie najlepszego rozwiązania do ochrony przed krypto-ransomware w czasie rzeczywistym. Aby zachować równe zasady testów, zdecydowaliśmy się na wykorzystanie domyślnych ustawień, pomimo, że niektóre z testowanych pakietów bezpieczeństwa posiadają tzw. „ochronę przed ransomware", jednakże z decyzji producenta, te konkretne funkcjonalności zostały domyślnie wyłączone.

Co więcej, długo zastanawialiśmy się, czy wprowadzić dodatkową kategorię oceny: „przywracanie plików po ataku krypto-ransomware". Po dokładniejszej analizie okazało się, że byłoby to niesprawiedliwe względem wszystkich testowanych programów —z jednego powodu: program Arcabit Internet Security uzyskałby miażdżącą przewagę, co nie oddawałoby prawdziwego obrazu dostępnych mechanizmów w innych pakietach na ustawieniach domyślnych. Stąd też nasza dedykowana rekomendacja dla mechanizmu SafeStorage. Dzięki SafeStorage, użytkownik bez żadnej dodatkowej konfiguracji może wykorzystać pełne możliwości pakiety ochronnego Arcabit Internet Security.

Nie braliśmy także pod uwagę dostępnych dedykowanych narzędzi do odszyfrowywania plików, ponieważ ich skuteczność zależy od zbyt wielu czynników. Narzędzia tego typu pozwalają przywrócić pliki tylko wtedy, jeśli uda się wykorzystać nieprawidłową implementację funkcji szyfrujących lub za pomocą klucza prywatnego pozyskanego w wyniku wspólnej kooperacji policji i ekspertów IT. Taki test byłby bardzo trudny do przeprowadzenia i zająłby bardzo dużo czasu — niewspółmiernie do potrzeb i do szybko zmieniającego się obrazu zagrożenia krypto-ransomware.

Przyznane wyróżnienia

BEST+++

100% skuteczności

BEST++

dozwolona 1 infekcja

GOOD+

dozwolone 2 infekcje

AVERAGE

dozwolone 3 infekcje

ONLY TESTED

powyżej 4 infekcji

Dla oprogramowania przeznaczonego do ochrony komputerów użytkowników indywidualnych i mikro firm:

Arcabit Internet Security
Comodo Cloud Antivirus
Emsisoft Internet Security 11
Emsisoft Internet Security 12
Foltyn SecurityShield
F-Secure SAFE
G DATA Internet Security
Kaspersky Internet Security 2017
Qihoo 360 Total Security
SecureAPlus Premium
Trend Micro Internet Security 2017
Voodoo Shield Pro
Zemana Antimalware Premium
ZoneAlarm Internet Security Suite

Avast Internet Security 2016
Avira Internet Security Suite
Bitdefender Antivirus Free Edition
Bitdefender Internet Security 2017
Dr. Web Space Security
ESET Smart Security 10 (BETA)
TrustPort Internet Security

Avast Free Antivirus 2016
AVG AntiVirus Free Edition
AVG Internet Security
Comodo Internet Security 8

Ad-Aware Free Antivirus
ESET Smart Security 9
FortiClient Free
Norton Security
Panda Internet Security
Sophos HOME

Malwarebytes Anti-Malware Premium
McAfee LiveSafe
Webroot SecureAnywhere Comlpete
Avira Free Antivirus
Dr Web Katana
Panda Free Antivirus
Comodo Internet Security Pro 10 (BETA)
Windows Defender
Malwarebytes Anti-Ransomware (BETA)

Dla oprogramowania przeznaczonego do ochrony stacji roboczych małych i średnich przedsiębiorstw:

AWARD BEST+++	AWARD BEST++	AWARD GOOD+	AVERAGE	ONLY TESTED
Arcabit Endpoint Security *Comodo ONE Enterprise* *Emsisoft Anti-Malware for endpoints* *F-Secure Protection Service for Business* *G DATA Client Security Business* *Kaspersky Endpoint Security 10 for Windows* *Seqrite Endpoint Security Enterprise Suite* *Sophos Endpoint Protection*	*Avast for Business Endpoint Security* *AVAST for Business Basic Antivirus* *AVG AntiVirus Business Edition* *Bitdefender GravityZone* *Kaspersky Anti-Ransomware Tool for Business* *Panda Adaptive Defense*	*Avira Antivirus for Endpoint* *ESET Endpoint Security*	---	*Trend Micro Worry-Free Business Security*

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