Active Protection™

Zaščitite podatke pred izgubo zaradi izsiljevalskih programov

Neprekinjena razpoložljivost podatkov v okolju s spreminjajočimi se grožnjami

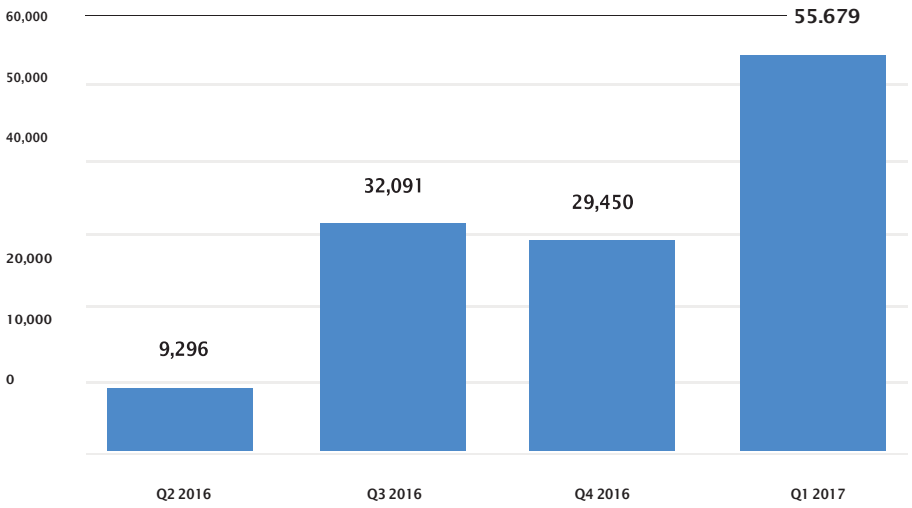
Ostermanova raziskava je pokazala, da izsiljevalski programi napadejo 47 odstotkov podjetij in stavimo lahko, da se je ta številka maja 2017 še povečala po globalnih napadih "WannaCry". Žal to pomeni šele začetek napadov izsiljevalskih programov in malokdo se zaveda posledic, ki jih imajo tovrstni zlonamerni programi.

Kaj je izsiljevalski program?

Izsiljevalski programi so vrsta zlonamernih programov, ki blokirajo dostop do nekaterih ali vseh podatkov, shranjenih na napravi. Da uporabnik napravo ali podatke lahko odklene, se od njega zahteva odkupnina, po navadi v splošno uporabljeni e-valuti.

Izraz izsiljevalski program pokriva dve vrsti zlonamernih programov: tako imenovani *Windows® blockers* (orodja za blokiranje Windowsov), ki blokirajo operacijski sistem ali brskalnik s pojavnim oknom in izsiljevalski programi, ki šifrirajo podatke. Med izsiljevalske programe prištevamo tudi nekatere prenašalce Trojancev in sicer tiste, ki ob okužbi naprave prenesejo izsiljevalski program za šifriranje podatkov.

Napadi izsiljevalskih programov se množijo z alarmantno hitrostjo, kar je razvidno iz spodnjih tabel. Industrijski strokovnjaki med njimi tudi FBI, žal napovedujejo, da bo število napadov izsiljevalskih programov še naprej eksponentno naraščalo.



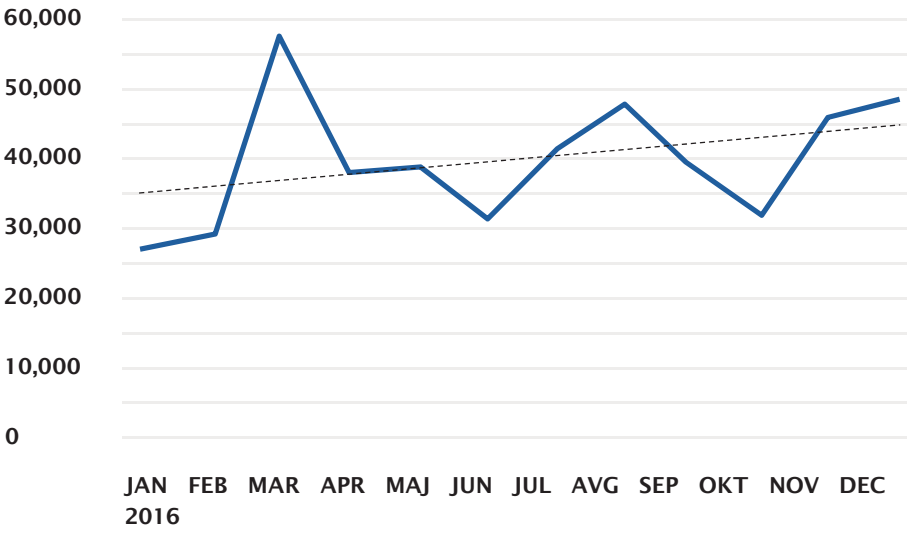
Število novo ustvarjenih modifikacij kripto-virusov, Q2 2016 – Q1 2017
Kaspersky Lab report, May 2017

GLAVNE PREDNOSTI

Acronis Active Protection je nova generacija zaščite podatkov, plod 14-letnih Acronisovih izkušenj z varovanjem podatkov več kot pol milijona organizacij.

- Je zaščita varnostne kopije pred izsiljevalskimi programi v realnem času. Tudi v primeru napada ne izgubite podatkov.
- Varuje vaše podatke, datoteke varnostne kopije in varnostno kopiranje samo, tudi če je različica izsiljevalskega programa nova oz. še ni bila identificirana.
- Uporaba je enostavna: prijazna uporabniku, popolnoma pregledna in zagotavlja avtomatsko zaščito.

Acronis Active Protection zagotavlja višjo raven zaščite podatkov pred izsiljevalskimi programi v sedanjosti in prihodnosti.



Mesečno odkriti izsiljevalski programi na globalni ravni

Symantec Corporation's Report, April 2017

ACRONIS ACTIVE PROTECTION: UČINKOVIT ODGOVOR NA GROŽNJE IZSILJEVALSKIH PROGRAMOV

Acronis Active Protection (aktivna zaščita Acronis) je napredna tehnologija za operacijske sisteme Windows. Acronis načrtuje razširitev, tako da bi bili na podoben način pokriti tudi Android® ter drugi mobilni in namizni operacijski sistemi.

Acronisovi proizvodi in tehnologija Acronis Active Protection, katere postopek patentiranja je v teku, predstavljajo temelj trdnega načrta neprekinjenega poslovanja.

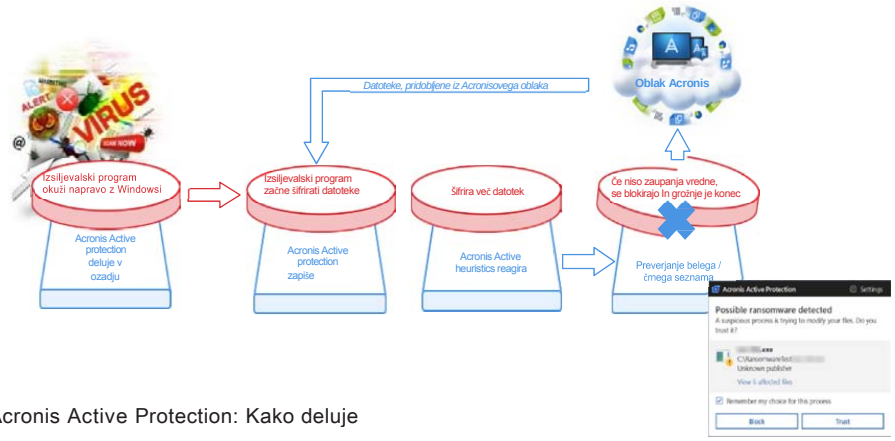
Napad izsiljevalskega programa želite vedno čim prej zaustaviti, po možnosti že kar za pisalno mizo, še preden lahko okuži mrežo in druge uporabnike. Ravno zato potrebujete rešitev, ki prepozna in zaustavi grožnjo še pred udarcem.

Acronis zagotavlja eksaktne rešitve za učinkovito obrambo pred napadi izsiljevalskih programov, saj vsi njegovi proizvodi vključujejo Acronis Active Protection. Organizacije vseh dimenzij in potrošniki se lahko ubranijo izsiljevalskih programov z Acronisovimi proizvodi v povezavi z rešitvijo za zaščito pred zlonamernimi program po vaši želji.

Hevristični pristop k odkrivanju

Jedro aktivne zaščite – Acronis Active Protection – predstavlja hevristika, sodoben pristop, naprednejši od odkrivanja posameznih podpisov. En podpis lahko odkrije samo en vzorec. S hevrističnim pristopom pa lahko zaznamo na stotine datotek, ki pripadajo isti družini, in sicer s primerjanjem verige dogodkov v datotečnem sistemu, izvedenih na podatkih, s podatkovno zbirko zlonamernih vedenjskih vzorcev.

Acronisovo vedenjsko hevristiko dopolnjujejo beli in črni seznami. Medtem ko hevristika lahko zazna nove grožnje, le-ti delujejo na osnovi izkušenj / rezultatov vedenja in preverjati je treba



Acronis Active Protection: Kako deluje

ali gre za napačno pozitivno prepoznavo. Zato Acronis Active Protection na osnovi belega in črnega seznama preverja tudi sumljive procese. Ko uporabnik blokira potencialen napad izsiljevalskega programa, gre to na črni seznam, tako da se zlonamerni program ob naslednjem vnovičnem zagonu ne zažene in uporabniku ni treba vedno znova blokirati izsiljevalskega programa.

Enostranski napadalci skušajo ogroziti varnostne kopije, tako da napadejo posrednika programa za varnostno kopiranje. Z Acronisom se seveda to ne bo zgodilo, saj Acronis Active Protection predstavlja samozaščito za Acronisov posredniški program. Noben proces v sistemu, razen Acronisovega programa, ne more spremeniti datotek varnostne kopije. Poleg tega Acronis Active Protection vključuje učinkovit samoobrambni mehanizem, ki prepreči vsak značilen napad, tako da spletni kriminalci ne morejo onemogočiti izvajanja Acronisovega programa ali spremeniti vsebine datotek varnostne kopije.

Acronis Active Protection nadzira tudi glavni zagonski zapis (MBR) vseh naprav uporabnika, ki imajo na trdem disku sistem Windows, in ne dovoli nobene spremembe legitimnih pripomočkov, ki niso na belem seznamu.

Ali Acronis Active Protection deluje za vse datoteke?

Deluje. Poglejmo si tri načine, kako varuje prav vse datoteke.

1. Izsiljevalski program napade katero koli datoteko

Ko je datoteka napadena, si uporabnik običajno pomaga tako, da kompromitirane podatke obnovi iz varnostne kopije datotek. S tehnologijo Acronis Active Protection v dejanskem času pa se šifrirane datoteke po potrditvi uporabnika avtomatsko obnovijo na zadnjo različico. Ta funkcija je zelo pomembna še zlasti pri načrtovanem varnostnem kopiranju. Če imate varnostno kopiranje načrtovano ob polnoči, napravo pa izsiljevalski program napade ob enajstih zvečer, lahko izgubite več kot deset ur dela. Kadar so procesi pod stalnim nadzorom, ob napadu izsiljevalskega programa ni izgubljen noben podatek.

2. Izsiljevalski program napade lokalno datoteko varnostne kopije

V tem primeru Acronis Active Protection aktivno nadzira lokalne pogone in preprečuje, da bi bile datoteke varnostne kopije zlonamerno spremenjene.

3. Zlonamerno spremenjene varnostne kopije v oblaku

Datoteke, shranjene v prostoru za shranjevanje v Acronisovem oblaku so izjemno varne pred neposrednimi spremembami z zlonamerno kodo. Acronis Active Protection uporablja trdno, celovito šifriranje in omejuje dostop do spreminjanja datotek na podpisano in pooblaščeno programsko opremo Acronisovega posrednika.

Napadi izsiljevalskih programov in kako jih obravnavamo

V spodnji tabeli so naštete nekatere napadalske tehnike izsiljevalskih programov in metode, ki jih Acronis Active Protection uporablja kot obrambo.

Zakaj je Acronis Active Protection boljši od kombinacije protivirusnega programa in klasične programske opreme za varnostno kopiranje?

Dva ločena proizvoda ne moreta jamčiti, da so vaši podatki varni pred izsiljevalskimi programi, saj nista integrirana. Pri klasičnem pristopu so vaši podatki izgubljeni, če vaša programska oprema za zaščito pred zlonamernimi programi ne zazna napada na podatke. Acronis Active Protection, podprt z varnostnimi kopijami lokalnega prostora za shranjevanje in varno shrambo v Acronisovem oblaku, obnovi izvirne podatke iz lokalnih predpomnilnikov, lokalnih varnostnih kopij in varnostnih kopij v oblaku.

Vrsta vedenja	Razlaga	Acronis Active Protection se odzove
Prepis na mestu	Izsiljevalski program odpre in na mestu spremeni podatkovne datoteke.	Pogon posreduje obvestila o dostopu do datotek storitve s hevrističnimi podatki in prekrije zapis (copy-on-write) sumljivih aktivnosti. Storitev zazna primer, začasno prekine izsiljevalski program in pogon povrne datoteko iz predpomnilnika v prejšnje stanje.
Preimenovanje	Izsiljevalski program odpre, preimenuje in spremeni podatkovne datoteke.	Isti vzorec kot zgoraj.
Nova datoteka	Izsiljevalski program ustvari novo datoteko, kopira izvirno vsebino, novo datoteko spremeni in izbriše izvirno datoteko.	Isti vzorec kot zgoraj.
Prepis preko glavnega zagonskega zapisa	Izsiljevalski program napade fizični pogon, naredi prepis preko MBR, sistem se ponovno zažene, HDD/MFT se pri vnovičnem zagonu šifrira (chkdsk spremenjen/prikrit).	Pogon spremlja operacije WRITE/SCSI v MBR preko RAW FS in obvešča storitev. Storitev preveri proces in sprejme odločitev.
Prepis na mestu / preimenovanje / nova datoteka se vstavijo v poznane, dobre procese	Izsiljevalski program naredi vstavek v dobro poznan, dober proces in izvede zlonamerna dejanja, kot so opisana zgoraj.	Pogon posreduje storitvi obvestila o poskusu vstavljanja, storitev da pogonu navodilo, da opazuje proces, ne da bi prekril zapis (copy-on-write). Če se zaznajo sumljivi vzorci, dobi uporabnik navodilo, da datoteke obnovi iz oblaka.

Velikokrat program za zaščito pred zlonamerno programsko opremo ne zazna zlonamernega programa, ki zahteva odkupnino, saj spletni kriminalci ciljajo na sam program za zaščito ter poiščejo šibke točke v tehnologiji odkrivanja ali v arhitekturi programa.

Klasični pristopi so zato šibki, saj je dovolj, da spletni kriminalci šifrirajo program za zaščito programske opreme in se s tem izognejo, da jih zazna.

Prav zato vsi prodajalci programov za zaščito pred zlonamernimi programi priporočajo, da se sistemi varnostno kopirajo. Obenem vse rešitve varnostnega kopiranja v oblaku ščitijo pred vektorjem preprostega napada – poškodbo podatkov na lokalni napravi. Nobeden pa ne varuje pred ciljnim napadom na varnostne kopije.

Acronis Active Protection varuje pred grožnjami prihodnosti

Spletni kriminalci napadajo varnostne kopije, saj je njihov trenutni posel ogrožen. Projekti, kot so No More Ransom ,osveščajo uporabnike, naj upoštevajo dva preprosta, vendar zelo pomembna koraka – svoje sisteme in podatke naj varnostno kopirajo in nikakor ne plačajo odškodnine!

Posledično zdaj spletni kriminalci napadajo datoteke varnostne kopije. Vzporedno z vse bolj množično uporabo varnostnih kopij v oblaku tudi spletni kriminalci postajajo vse bolj kreativni. Da bi ogrozili varnostno kopijo v oblaku, morajo pridobiti poverilnice za dostop do oblaka – običajni programi za zaščito pred izsiljevalskimi programi pa teh poverilnic nimajo.

Zato bodo spletni kriminalci napadali posrednika na napravi, ki deluje kot prehod za prenos podatkov v oblak. V tehničnem smislu obstaja več načinov, da se v lokalni posrednik vstavi zlonamerna koda in ogrozi podatke v varnostni kopiji v oblaku. Na srečo pa imamo rešitev, ki lahko to ustavi – Acronisova serija proizvodov z aktivno zaščito oz. Active Protection.

Neodvisni laboratoriji so soglasni

Neodvisni laboratorij AV-Test je preizkusil štiri nove programe in prišel do zaključka: “Test nedvoumno dokazuje, da bi morala koristna zaščita pred zlonamernimi programi vključevati uvedbo programa za varnostno kopiranje.
Tehnologija Acronis Active Protection je bila edina na testu, ki je bila zmožna ustaviti napade izsiljevalskih programov.”.”

V neodvisnem laboratoriju MRG Effitas so prišli do enakega zaključka. V zvezi s testi, ki so se nanašali na Acronis, so izjavili : “Odkrili nismo nobene šibke točke.”

Na povezavi Acronis Blog boste našli več informacij o testih neodvisnih izvajalcev.

Acronis Active Protection: Zaustavimo napade prihodnosti

Izsiljevalski program išče nove datoteke varnostne kopije, da jih šifrira.

Izsiljevalski program je izboljšan, da lahko napade posrednika varnostne kopije, dobi dostop do oblaka in ogrozi datoteke varnostne kopije.

Acronis Active Protection ustavi napad.

Uporabnik ne plača I01150171; uporabi varnostno kopijo, kot priporočajo prodajalci AV.

Aktivira se samoobrambna funkcija AAP 1111.

Za dodatne informacije
obiščite www.acronis.com

Avtorska pravica © 2002-2017 Acronis International
Vse pravice pridržane. Acronis in logotip Acronis predstavljata blagovno znamko Acronis International GmbH
v ZDA in/ali drugih državah. Vse druge blagovne znamke ali registrirane blagovne znamke so last njihovih imetnikov.
Pridržujemo si pravico do tehničnih sprememb in odstopanja od ilustracij; napake so izključene. 2017-06

Prevod: Prevajanje Alenka Kikelj, s.p.

Za vse dodatne informacije se obrnite na Cores, d.o.o., Kranj, Ulica Mirka Vadnova 6, 4000 Kranj, telefon 04-280-9400 in e-pošta prodaja@cores.si .

CORES®
INFORMACIJSKI SISTEMI