UNDVIK DIGITAL KIDNAPPNING

Betala nu ...

Kidnapparprogram är ett av de största hoten mot dagens datorer eftersom ett angrepp gör att du förlorar antingen viktiga filer eller pengar. Här visar vi hur kidnapparprogrammen fungerar, och hur du försvårar angrepp med programmet CryptoPrevent.

Journalist
Mathias Alsted Flinck

"Du har blivit medlem i det stora sällskapet CryptoWall. Läser du detta har dina filer blivit krypterade, och det enda du kan göra för att få tillbaka dem är att köpa vårt speciella program!"

Tonen i meddelandet må vara munter, men det är inget mindre än en katastrof att dina filer har blivit tagna som gisslan. Den enda räddningen är att ge efter för kraven och betala lösensumman. Tekniken som används för att kryptera filerna är nämligen så stark att det är omöjligt att låsa upp filerna utan rätt nyckel, och hela poängen är givetvis att du bara får nyckeln om du betalar. Fenomenet kallas kidnapparprogram, eller ransomware på engelska. För tillfället är detta ett av de största hoten som du kan råka ut för eftersom det bara finns två alternativ – betala lösensumman eller förlora filerna.

De värsta formerna nöjer sig inte bara med att ta dina familjefoton och viktiga dokument som gisslan. De visar en klocka som räknar nedåt, och när den kommer hela vägen till 0:00 raderas filerna. Om du ger upp inför hotet och betalar, finns det fortfarande inga garantier för att du faktiskt får tillbaka filerna. Det är inte ovanligt att drabbade användare har betalat flera tusen kronor men aldrig fått svar från de cyberkriminella, som helt enkelt har tagit pengarna och stuckit. Resultatet blir detsamma som om de inte hade betalat, nämligen att filerna går förlorade. Kan inte polisen göra något? Det är en relevant fråga, men brottslingarna är väldigt duktiga på att dölja sina spår. Det kan se ut som att angreppet kommer från Paraguay, när det i själva verket är någon i Berlin som ligger bakom. Lösensumman brukar dessutom utkrävas i valutan bitcoin, en virtuell valuta som inte går att spåra.

Lösensummorna folk betalar för att försöka få tillbaka sina filer växer till miljonbelopp. Säkerhetsexperter uppskattar att enbart CryptoLocker, som är ett av de vanligaste kidnapparprogrammen, drar in nästan en miljard kronor årligen till de som ligger bakom utpressningen.

Om du drabbas av ett kidnapparprogram önskar vi att vi kunde presentera en guide som löser alla problem och räddar dina filer. Dessvärre är det omöjligt. Allt som finns är förebyggande åtgärder. Det vi däremot kan erbjuda är goda råd och programmet CryptoPrevent, som hjälper till att blockera de farliga filerna. Bägge finns i den här artikeln, där vi även förklarar hur kidnapparprogrammen fungerar.

Foto: Shutterstock/blindfire.

... eller vi raderar dina filer

Så funkar kidnapparprogram

Hur bär sig ett kidnapparprogram, exempel vis det välkända CryptoLocker, åt för att låsa filerna? Hur kommer det in i datorn? Här får du en inblick i hur de fruktade programmen fungerar.

1 Först skapar en cyberbrottsling ett program designat för att ta filer som gisslan. Det kamoufleras som en fil som bifogas med e-post och döljs på en webbplats eller i andra program.

2 Filen som innehåller programmet skickas som en bifogad fil till miljontals e-postadresser i form av skräppost.

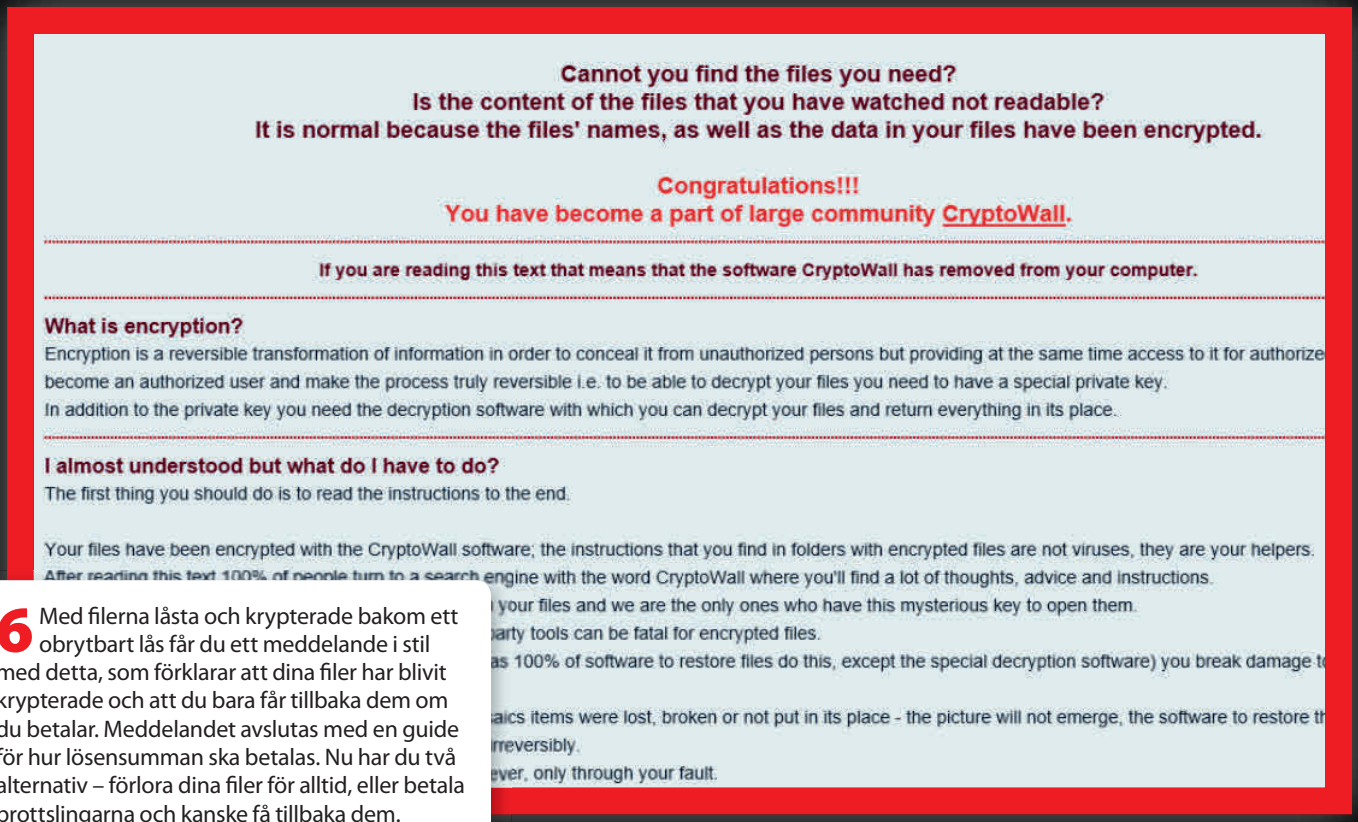
7 Om du betalar lösensumman får du eventuellt en nyckel som låser upp krypteringen och du får tillbaka dina filer. Annars förlorar du både pengar och filer.

Foto: Shutterstock/frank_peters, D-Line, Aha-Soft, MaDedee och penguiin.

3 Du öppnar meddelandet som kan se ut att komma från en betrodd myndighet. Du laddar hem den bifogade filen, och nu har kidnapparprogrammet hamnat på din dator. Nu är det bara en tidsfråga innan programmet aktiveras och börjar arbeta.

4 Kidnapparprogrammet söker igenom datorn efter klassiska filtyper som .doc, .jpg och .pdf, och krypterar dem.

5 Nu kan du bara få tillgång till dina filer med en unik kod som programmet har skapat.



Cannot you find the files you need?
Is the content of the files that you have watched not readable?
It is normal because the files' names, as well as the data in your files have been encrypted.

Congratulations!!!
You have become a part of large community CryptoWall.

If you are reading this text that means that the software CryptoWall has removed from your computer.

What is encryption?
Encryption is a reversible transformation of information in order to conceal it from unauthorized persons but providing at the same time access to it for authorize
become an authorized user and make the process truly reversible i.e. to be able to decrypt your files you need to have a special private key.
In addition to the private key you need the decryption software with which you can decrypt your files and return everything in its place.

I almost understood but what do I have to do?
The first thing you should do is to read the instructions to the end.

Your files have been encrypted with the CryptoWall software; the instructions that you find in folders with encrypted files are not viruses, they are your helpers.
After reading this text 100% of people turn to a search engine with the word CryptoWall where you'll find a lot of thoughts, advice and instructions.
your files and we are the only ones who have this mysterious key to open them.
arty tools can be fatal for encrypted files.
as 100% of software to restore files do this, except the special decryption software) you break damage t

aics items were lost, broken or not put in its place - the picture will not emerge, the software to restore th
rreversibly.
ever, only through your fault.

6 Med filerna låsta och krypterade bakom ett obrytbart lås får du ett meddelande i stil med detta, som förklarar att dina filer har blivit krypterade och att du bara får tillbaka dem om du betalar. Meddelandet avslutas med en guide för hur lösensumman ska betalas. Nu har du två alternativ – förlora dina filer för alltid, eller betala brottslingarna och kanske få tillbaka dem.

CryptoPrevent

Hämta programmet från
www.pctidningen.se/fordelszonen

Skydda datorn mot de kriminella som vill ta dina filer som gisslan.

SYSTEMKRAV
Windows 10, 8, 7, Vista eller XP

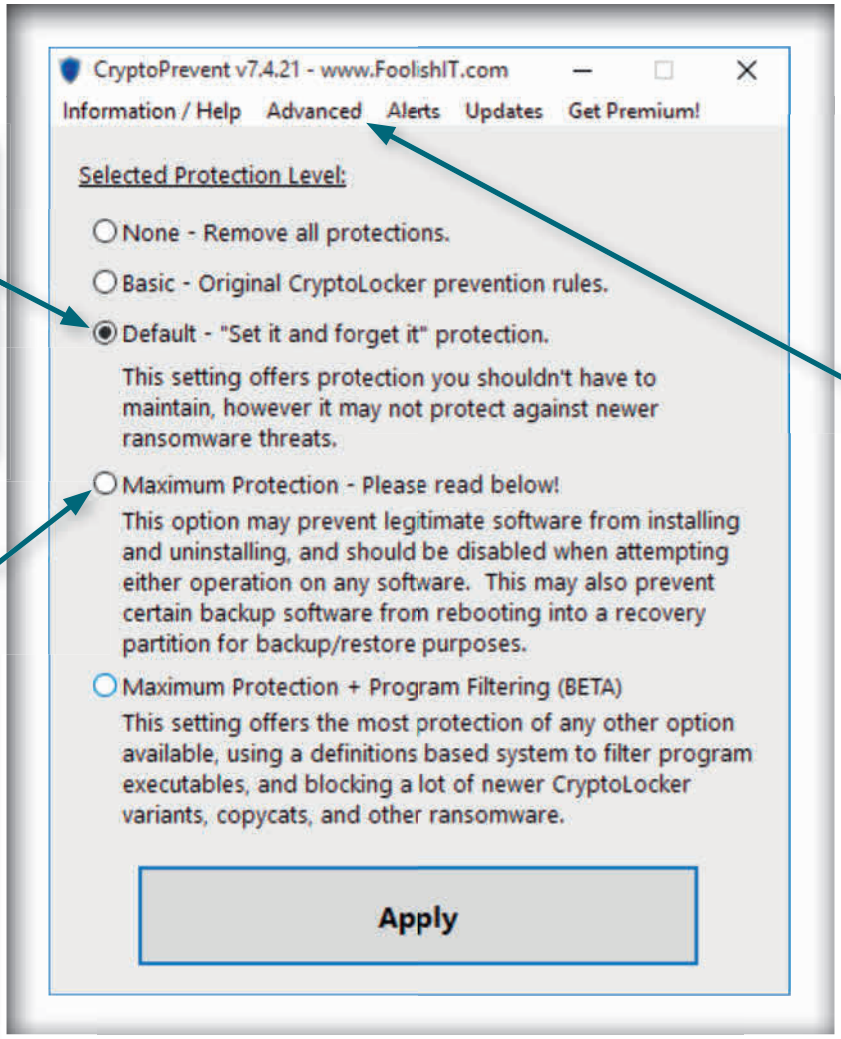
SPRÅK
Engelska

Skydda din dator mot gisslantagare

Det bästa skyddet mot kidnapparprogram är en kombination av säkerhetsprogram mot virus och sabotageprogram, kompletterat med det kraftfulla programmet CryptoPrevent. Det är utvecklat specifikt för att förhindra att kidnapparprogram krypterar dina filer. Programmet finns tillgängligt i Fördelszonen. När du har installerat det finns det olika säkerhetsnivåer att välja mellan beroende på vad du tänker göra på datorn. Här är en introduktion till CryptoPrevents viktigaste funktioner.

Default är standardinställningen som vi rekommenderar att du använder vid vanligt vardagsanvändande. Den skyddar dig, men blockerar inte erkänt bra program som till exempel backupprogram.

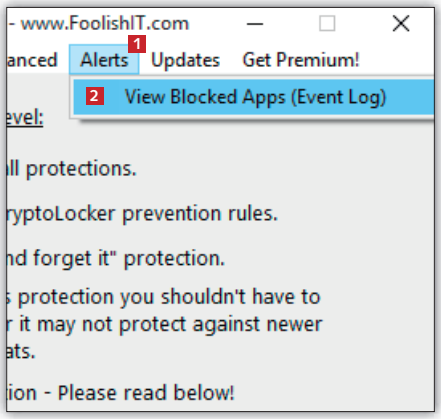
Du kan med fördel välja profilen **Maximum Protection** om du misstänker att datorn har infekterats med sabotageprogram eller om du tänker använda okända program. Skyddet är ganska brutalt och kan komma att blockera program som inte alls är skadliga.



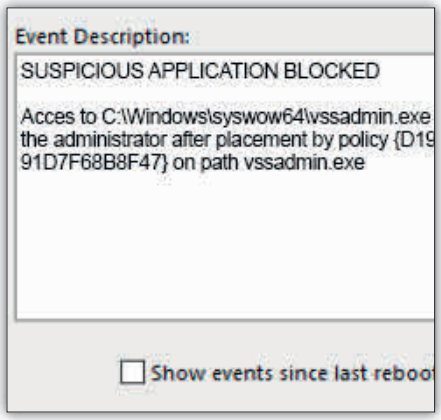
Erfarna användare kan välja att skapa regler för specifika processer under **Advanced**, och därmed skapa helt egna säkerhetsprofiler. Det är överkurs, men kan vara praktiskt om CryptoPrevent envisas med att blockera ett program som du vet är legitimt. Menyn innehåller, som namnet skvallrar om, avancerade funktioner som kräver en erfaren datoranvändare för att kunna hanteras.

Är du under attack?

CryptoPrevent körs i bakgrunden och gör inte speciellt mycket väsen av sig. Det visar inte ens några meddelanden när det blockerar misstänkta program, men du kan själv undersöka om CryptoPrevent har stoppat något.



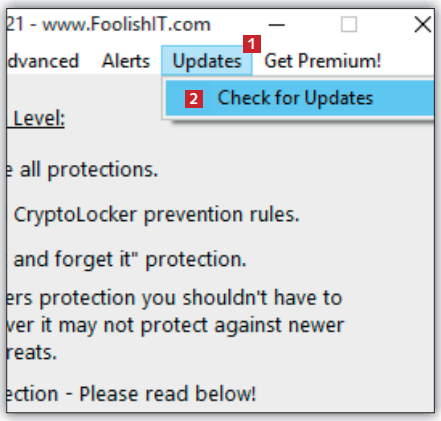
1 Starta CryptoPrevent och peka på verktygsfältet. Klicka på **Alerts** 1 följt av alternativet **View Blocked Apps (Event Log)** 2.



2 Nu visas en lista med de olika händelser som programmet har registrerat. I det här fallet har CryptoPrevent bara blockerat ett misstänkt program.

Glöm inte att uppdatera!

Glöm inte att med jämna mellanrum undersöka om det har kommit några uppdateringar, eftersom gratisversionen av CryptoPrevent inte gör det automatiskt. Genom att alltid använda den senaste versionen får du de bästa förutsättningarna för att hålla nya typer av ransomware borta. Var uppmärksam på att uppdateringar emellanåt kan medföra att programmet ändrar utseende.



1 Klicka på **Updates** 1 längst upp i verktygsfältet, följt av **Check for Updates** 2. CryptoPrevent letar efter en nyare version, och om det finns får du frågan om du vill uppdatera eller ej.

TIPS!

Betala för enkelt skydd

Du kan köpa CryptoPrevent för ungefär 150 kronor, vilket bland annat ger automatiska uppdateringar, filter som varnar för farliga filer i e-post och möjligheten att skapa egna regler för vilka program och processer CryptoPrevent ska blockera eller tillåta. Den kommersiella versionen gör det enklare att hålla datorn säker mot program som CryptoLocker.

5 råd för att undvika kidnapparprogram

■ Var alltid kritisk när du öppnar e-post. Många sabotageprogram anländer som bifogade filer i e-post som ser ut att komma från välkända avsändare som en bank, Skatteverket eller PostNord. Kontrollera alltid e-post noggrant innan du laddar hem eller rör bifogade filer.

■ Installera säkerhetsprogram på datorn. CryptoPrevent förhindrar kidnapparprogram att ta dina filer som gisslan, men inte att det kommer sabotageprogram till din dator. Med ett program som bekämpar sabotageprogram och virus minskar risken att datorn blir infekterad och sårbar för angrepp.

■ Håll ögonen öppna efter uppdateringar. Kriminella på internet försöker alltid utnyttja programs svagheter och säkerhetshål, samtidigt som programutvecklarna försöker eliminera de möjligheterna. Genom att se till att hålla allt från webbläsare till drivrutiner för skrivare uppdaterade minskar risken för intrång.

■ Akta dig för automatiska nedladdningar. Om det plötsligt börjar laddas hem filer från en webbplats utan att du har bett om det, kan det vara fara å färde. Då kan det handla om sabotageprogram eller virus. Avbryt nedladdningarna om du hinner, och gör därefter kompletta genomsökningar med dina säkerhetsprogram.

■ Gör fysiska säkerhetskopieringar av dina bilder och dokument. Det skyddar dig inte mot kidnapparprogram och virus, men det förhindrar att du för evigt förlorar ovärderliga filer om du drabbas av ett angrepp. Det medför även att du har kvar dina filer om datorn skulle gå sönder eller bli stulen.