Verksamheten för samhällets informations- och cybersäkerhet
CERT-SE
08-678 57 99
cert@cert.se

Problemområde Ransomware[1]

De senaste åren har CERT-SE observerat en stor ökning i antalet fall av Ransomware som har drabbat svenska organisationer. Samtidigt med ökningen har en större komplexitet bland Ransomware-varianter observerats och med dessa även sättet som används för att lura användare att exekvera den skadliga koden.

Ransomware (används omväxlande med RW i nedan) är en variant av skadlig kod som har funnits i många år men på senaste tid blivit ett lönsamt sätt för kriminella att utpressa organisationer och individer. RW använder krypteringmetoder för att ändra på innehållet i vissa filtyper på ett sätt som gör att den drabbade inte kan läsa eller använda filerna. Utöver detta stänger många RW-varianter av vissa funktioner som har med säkerhet och återställning av filändringar att göra. Detta för att kunna tvinga användaren att betala en lösensumma.

Det vanligaste varianterna av Ransomware (CryptoLocker, CTB-locker, TorrentLocker, CryptoWall och BandaChor/Ebola) kräver inte lösensumma omedelbart, utan söker och krypterar alla filer de hittar med en viss filändelse (t.ex .docx). Många varianter söker inte bara igenom lokala filer, utan även filer som finns på gemensamma lagringsytor. Först när detta har uppnåtts får användaren ett meddelande om att dess filer blivit krypterade.

I och med att denna form av skadlig kod inte syftar till att förstöra datorn lämnar den filer som är kritiska för operativsystemet oförändrade. Filer som applikationer är beroende av kan dock bli utsatta för kryptering, vilket gör att mer komplexa system kan blir kraftigt påverkade eller förstörda. I dagsläget är det framförallt Windows-baserade datorer och servrar som drabbas av Ransomware, men även OS X och Linux-varianter har upptäckts. Dessa är dock

[1] **Bakgrund.** Detta dokument beskriver kortfattat en it-relaterad händelse som kan påverka samhällets informations- och cybersäkerhet. Rapporten har tagits fram av CERT-SE vars uppgift är att stödja samhället i arbetet med att hantera och förebygga it-incidenter.

Förutsättningar. Rapporten har till syfte att sprida information en kort tid efter en inträffad händelse. Den är därför baserad på den information som fanns tillgänglig vid tidpunkten för rapportens upprättande. Rapporten baseras på information från öppna källor vars riktighet inte har verifierats. Rapporten ska därför inte ses som komplett. Läsaren bör ta del av denna rapport utifrån dessa reservationer.

betydligt färre än de Windows-baserade varianterna då Windows operativsystem har störst marknadsandelar och därav större spridning.

Då en stor del av de som drabbas inte betalar någon lösensumma är det istället viktigt för utvecklarna av den skadliga koden att kunna inrikta sig mot så många användare som möjligt. Under det senaste året har angriparna bakom ett antal större kampanjer börjat förfina sina bedrägerimetoder samtidigt som de fortsätter att utveckla den skadliga koden. Den vanligaste metoden att infektera en dator är fortfarande via e-post som innehåller länkar till skadlig kod. Dessa mejl kan nu även vara på korrekt svenska och i stor utsträckning likna ordinarie och korrekta mejl. Detta till trots går det fortfarande att urskilja bluffmejl om användaren ser noggrant på mejlets metainformation och länkens destination.

Två tekniska utvecklingar har försvårat begränsningar av Ransomware under senare tid

Dels har utvecklarna av skadlig kod blivit mer tekniskt kompetenta vad gäller kryptering och även lärt sig av de misstag som upptäckts av säkerhetsföretag när dessa delgivit drabbade råd i syfte att hjälpa användare att återfå sina filer. Skäl till detta är bland annat att sårbarheter och råd om hur dessa undviks, behöver publiceras offentligt för att drabbade ska kunna ta del av dem. Följaktligen får även utvecklarna av den skadliga koden hjälp att förstå hur de upptäckts och således tips om vad de behöver göra för att justera sin egen Ransomware-produkt. En ökande risk är att RW-utvecklare med tiden kommer att uppnå en så pass kompetent implementering av kryptoalgoritmer att det inte kommer att gå att hitta användbara sårbarheter i dess kod för att återskapa rätt krypteringnyckel. Här kan det noteras att vissa RW-varianter kan ha uppnått detta redan nu.

Den andra utvecklingen är en ökad användning av anonymitetsnätverket Tor bland RW-varianter och för kommunikation mellan RW på en infekterad dator och en RW-kontrollserver. Innan denna utveckling har säkerhetsföretag lyckats få tag i kontrollservrar för vissa RW genom att spåra kommunikationen mellan den drabbade datorn och kontrollservern. Då dessa beslagtagits kunde man distribuera eller publicera de krypteringsnycklar som kontrollservern innehöll till de som drabbats, och vilka då kunde få tillbaka sin data utan att betala. Då Tor-nätverkets trafik i praktiken inte går att spåra är det numer sällan som säkerhetsföretag lyckas med samma sak.

MSB:s nuvarande bedömning

Trots pågående utveckling finns det fortfarande sätt att skydda sig mot Ransomware. Ett effektivt skydd för organisationer har varit att utbilda sina användare om hur bluffmejl kan se ut och hur man identifierar dem med sin mejlklient. Blir man drabbad kan man försöka koppla bort datorn från nätverket för att förhindra att den skadliga koden kan ladda ner en krypteringnyckel. Detta fungerar dock endast för vissa RW-varianter. Detta har gjort att vissa säkerhetslösningar nu även undersöker beteendet hos

programvara som liknar den skadliga kodens kryptooperationer och försöker förhindra dessa.

Ytterligare rekommendationer är att ta hänsyn till ordinarie förebyggande säkerhetsåtgärder som gäller för flesta typer av skadlig kod, till exempel att installera säkerhetsuppdateringar, ta backup och testa återläsningsfunktionen, använda antivirusskydd, undvika att vara inloggad med lokala administratörsrättigheter och använda så kallad vitlistning som kontrollerar vilka program som får köras.

Länkar till mer information

http://blog.fox-it.com/2015/09/07/the-state-of-ransomware-in-2015/

http://www.trendmicro.com/vinfo/us/security/definition/Ransomware

http://media.kaspersky.com/pdf/guard-against-crypto-ransomware-kaspersky-guide.pdf

http://blog.sensecy.com/2015/03/12/bandarchor-and-ebola-virus-ransomware-are-they-the-same-one/

Länkar till webbsidor som kan avkryptera vissa varianter av Ransomware

https://noransom.kaspersky.com/

http://www.bleepingcomputer.com/virus-removal/

http://malwaretips.com/blogs/category/ransomware/