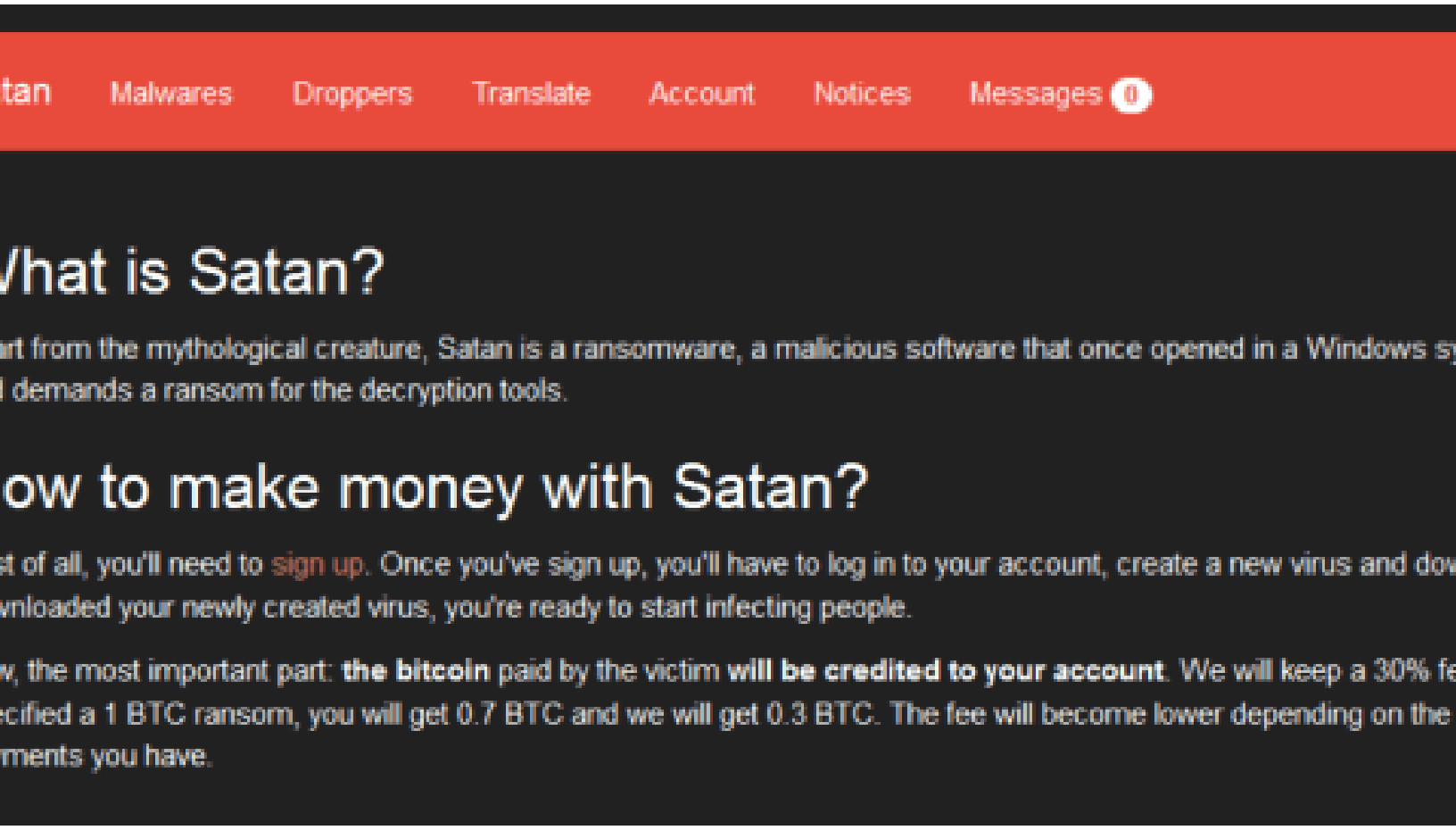
SOPHOS



Paketlösningen "Satan" tar 30 procent av de intäkter som gisslanprogrammet genererar.

2018-03-20 09:41 CET

Färdiga paket med gisslanprogram bäddar för fortsatta attacker

Under de senaste åren har vi sett en enorm ökning av gisslanprogram (ransomware). En bidragande orsak är att det i dag är enkelt att distribuera och skapa den här typen av program. Utvecklingen eldas också på av att Ransomware as a Service (RaaS) nu finns som färdiga paketlösningar för människor med begränsade tekniska förkunskaper.

E-post är fortfarande det vanligaste sättet att distribuera gisslanprogram. Där ser vi också att skaparna använder olika tider på året för att få högsta möjliga genomslagskraft. Under julen såg vi exempelvis en stor ökning av gisslanprogram som distribueras via falska e-postmeddelanden som ser ut att

komma från Postnord.

Ett liknande exempel dyker upp i samband med att deklarationerna ska lämnas in. Då ökar antalet e-postmeddelanden som ser ut att komma från Skatteverket för att lura användare att klicka på länkar eller öppna bifogade filer.

Färdigpaketerade RaaS-tjänster i molnet

– Utvecklingen påskyndas dessutom av att nästan vem som helst kan köpa sig en färdig paketlösning, ett RaaS-kit. Det är en färdigpaketerad molntjänst på samma sätt som exempelvis SaaS (Software as a Service) och IaaS (Infrastructure as a Service). Tjänstepaketeringen gör det förhållandevis enkelt för personer med väldigt lite teknisk förkunskap att planera och genomföra attacker, kommenterar Per Söderqvist, säkerhetsexpert på Sophos.

I en del fall säljs RaaS-paketen mot att en procentandel av de pengar som gisslanprogrammet inbringar går till säljaren. I andra fall kan det handla om att tjänsten säljs mot en engångsavgift som kan omfatta mer eller mindre support och olika garantier. De mer ambitiösa RaaS-aktörerna erbjuder ofta stöd för flera språk, chattfunktion och support dygnet runt.

Flera forskare och säkerhetsföretag arbetar i dag med att identifiera och kartlägga marknaden för RaaS. Samtidigt säljs majoriteten av RaaS-paketen på det så kallade ”dark web” och att mäta hur många som faktiskt köper och använder tjänsterna är svårt att avgöra. Marknaden kan av uppenbara skäl inte analyseras med enkäter och kundundersökningar. De som utvecklar dessa verktyg är i allmänhet också väldigt duktiga på att dölja sina spår.

SophosLabs arbetar med att analysera skadlig kod och har på senare tid sett en tydlig en ökning av den här typen av gisslanprogram. Dorka Palotay, säkerhetsanalytiker vid SophosLabs, har identifierat några av de mer framträdande RaaS-kiten:

Philadelphia

Detta är ett av de mer sofistikerade RaaS-paket som finns att tillgå. Philadelphia har utvecklats av Rainmaker Labs och ger möjlighet att skräddarsy gisslanprogram. För en relativt liten summa (389 dollar) får användaren även full tillgång till en obegränsad licens som bland annat inkluderar fria uppdateringar och tillgång till support.

I april 2017 greps en tonåring i Österrike för att ha använt detta RaaS-paket. Det hade då använts för att infektera ett lokalt företag där bland annat servrar och databaser hade krypterats. Företaget krävdes på 400 dollar för att få dessa dekrypterade men vägrade betala och lyckades till sist återställa all data från backuper.

Stampado
Detta är föregångaren till Philadelphia och började säljas sommaren 2016. Stampado har också utvecklats av Rainmaker Labs men är inte alls lika avancerad som efterföljaren Philadelphia. Priset är också betydligt lägre, endast 39 dollar. Trots att Philadelphia finns tillgängligt säljs Stampado fortfarande.

Satan
Denna tjänst har ett annat upplägg där de ger bort en licens gratis. I stället tar de en marginal på de pengar som genereras genom deras tjänst. De påstår att deras ransomware inte kommer att upptäckas av antivirusprogram och kunden kan själv sätta ett pris. Satan tar sedan 30 procent av de intäkter som deras gisslanprogram genererar.

De erbjuder dessutom en rabatt beroende på hur mycket pengar som dras in genom deras tjänst.

Viktigt att vara vaken och ha rätt resurser
Attackerna lär fortsätta så det viktigaste är att fortsätta vara vaksam och ha rätt resurser och hjälpmedel på plats för att snabbt kunna åtgärda problem när de uppstår.

Sedan är de allmänna råden alltid aktuella, dvs gör regelbundna backuper som du förvarar krypterade på en annan plats, aktivera inte makron i e-postbilagor och se till att vara snabb med att använda nya uppdateringar och patchar. Då gör vi det svårare för skurkarna att ställa till skada.

---

av säkerhetsexperter som arbetar med att säkra klienter (bärbara datorer, servrar och mobila enheter) och nätverk med hjälp av moln- och AI-baserade lösningar. Sophos lösningar skyddar mot ständigt nya hot i form av bland annat gisslanprogram, skadlig kod, så kallade exploits, riktade attacker och nätfiske.

I molnplattformen Sophos Central finns en hel portfölj av produkter och tjänster, inklusive det avancerade klientskyddet Intercept X och brandväggen XG. Det ger en automatiserad, synkroniserad säkerhet och en helhetslösning som är tillgänglig via API:er. Sophos säljer sina produkter och tjänster via en global kanal med över 47 000 partner och Managed Service Providers (MSP). Företaget riktar sig också direkt till konsumenter med Sophos Home. Sophos har sitt huvudkontor i Oxford, England och är noterat på Londonbörsen under namnet ”SOPH”. Mer information finns på www.sophos.com

Kontaktpersoner

Per Söderqvist
Presskontakt
Team Leader Sales Engineer
Nordics and Baltics
Per.Soderqvist@Sophos.com
+46 (0) 76 175 00 64