# 5 vanliga hot som passerar obemärkta förbi traditionella anti-virusprogram

Kreatörer av skadlig kod har inte övergivit sina gamla knep utan de har lagt till nya metoder för att ligga steget före den traditionella antivirus-programvaran. De signaturdetekteringar och YARA-regler som tidigare gav tillräckligt bra försvar, räcker idag inte som skydd mot phishing, utpressningsprogram och kryptomining. Idag behövs lösningar som distribuerar en AI-modell med maskininlärning. Traditionella antivirusprogram är utformade så att de blockerar filbaserad skadlig programvara. Det fungerar genom att programmet skannar filer på hårddisken och sätter alla skadliga filer i karantän. Denna lösning var bra under säkerhetsprogrammens barndom, men idag utvecklas attacker på ett sätt som kringgår denna typ av skydd. Här är de fem vanligaste cybersäkerhetshoten som kan kringgå traditionella antiviruslösningar.

**1. Samma virus återkommer**

Ta en titt på alla offentliga skadedatabaser som [VirusTotal](https://www.virustotal.com/%22%20%5Cl%20%22/file/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa/detection%22%20%5Ct%20%22_blank) och du kommer se att samma gamla hot laddas upp dagligen. Mängder med vanliga skadliga program genereras igen, ibland inom några timmar, med en helt annat filhash. En del skadlig programvara ändrar dess innehåll baserat på lokala parametra för olika enheter, vilket resulterar i en ny hash varje gång de körs. Med en redan känd skadlig fil kan försvarare generera en unik ”checksum” som identifierar en kopia av filen, oavsett namn eller plats, på alla system som använder vanliga verktyg.

**2. Är hotet okänt visas det inte**

Många antivirusverktyg har slutat att enbart kontrollera enligt signaturer och använder nu även ett regelbaserat skanningssystem, vanligtvis [YARA](https://yara.readthedocs.io/%22%20%5Ct%20%22_blank)-verktyget. YARA erbjuder en förbättring jämfört med enkel filhashning eftersom den tillåter en skanner att utföra flera tester på filens innehåll. Till exempel kan en regel skapas som inte bara letar efter vissa fasta strängar i skadlig programvara utan den söker också efter regelmönster. YARA-reglerna är ett stort steg framåt och distribueras av många, men det finns två problem som gör det enkelt för skadlig programvara att undvika upptäckt. För det första kan skaparen av den skadliga koden räkna ut vilka strängar en given motor använder för att upptäcka deras skadliga program och ändra strängarna för att undvika upptäckt. För det andra, och mer problematiskt, är att den här tekniken förlitar sig på att antivirusprogrammet redan har sett den skadliga programvaran åtminstone en gång tidigare för att analysera den och utveckla en regel för dess upptäckt. Det betyder att försvararen alltid är ett steg bakom angriparen, och ibland räcker ett fönster på några dagar för att angriparna ska komma in och ut ur sina mål utan upptäckt.

**3. Skadliga Office-dokument som ser oskyldiga ut**

Vi tenderar att tänka på vanliga dokument som ofarliga samlingar av formaterade data. Men när dokument innehåller dynamiska element som JavaScript i PDF-filer eller kodutförandefunktioner som makron och DDE i MS Office-dokumenttyper kan det leda till en skada bara genom att öppna en fil som innehåller dessa funktioner eftersom de körs så snart dokumentet laddas. Adobe Reader och Microsoft Office är populära mål för den här typen av skadliga dokument både på grund av deras vanlighet och deras historik med upprepade sårbarheter. För äldre antiviruslösningar som bygger på signaturer kan det vara svårt att upptäcka sådana skadliga dokument av två skäl. Filhasher kan enkelt ändras bara genom att skapa ett dokument med liknande "normalt innehåll" och till och med skanning via YARA-regler kan besegras med enkel kodförvanskning.

**4. Skadlig kod utan tillhörande filer**

De flesta förknippar skadlig programvara med någon sorts skadlig fil som laddas ner skador eller stjäl personuppgifter. Under de senaste åren har angriparna emellertid insett att traditionella antiviruslösningar har en stor blind fläck: skadliga processer kan köras i minnet utan att lämna efter sig filer som antivirusskannare kan hitta. Attacker med skadlig kod utan fil har blivit allt vanligare under de senaste åren, där anmärkningsvärda exempel inkluderar WannaCry, Angler, Duqu och Poweli. En av anledningarna till ökningen av fillös skadlig kod har varit den utbredda användningen av PowerShell, även om JavaScript och PDF, makron och DDE också har använts i attacker utan filer. Det som gör den här typen av attacker så svåra att upptäcka för traditionella antivirusprogram är det faktum att de vanligtvis undergräver betrodda processer, till exempel PowerShell och rundll32.exe – ett viktigt Windows-körbart program som laddar dynamiska bibliotek med delad kod för andra program.

**5. Krypterad trafik som gömmer hotet säkert**

Ytterligare en blind fläck för antivirus av äldre modell är krypterad trafik vilket tack vare påtryckningar från Google och andra nu har blivit normen för de flesta webbplatser. Medan https- och SSL-certifikat är ett bra sätt att säkra kommunikation med en pålitlig webbplats, skyddar de lika "hjälpsamt" angriparnas kommunikation. Skadliga aktörer kan dölja sina aktiviteter från att bli upptäckta genom att, precis som vanliga webbplatser, säkerställa att trafiken mellan offret och angriparens kommando-och-kontroll-server (C2) är skyddad av end-to-end-kryptering. Nya siffror tyder också på att nästan hälften av alla nätfiskewebbplatser nu använder det säkra https-protocol för att dölja sina aktiviteter från både användare och för en stor del säkerhetsprogramvara.

På SentinelOne förstår vi att angripare aldrig kommer att sitta still, och att de kommer fortsätta utveckla sina tekniker. Det är därför vi har byggt en produkt som inte litar på traditionella lösningar utan tar upp kampen med angriparna genom att använda aktiv EDR som förutsäger om en process är skadlig oavsett var den kommer ifrån.

**Om SentinelOne**

SentinelOne levererar autonomt ändpunktsskydd genom en enda agent som automatiskt förhindrar, detekterar och spårar alla attacker oberoende var ifrån de kommer. S1-plattformen är konstruerad så att den är extremt enkel att använda. Dessutom sparar kunderna tid genom att tillämpa plattformens AI som automatiskt eliminerar hot i realtid både lokalt och i molnet. Det är den enda lösning som ger fullständig synlighet över nätverk direkt från slutpunkten.

För mer information besök sentinelone.com eller följ oss på[@SentinelOne](https://twitter.com/sentinelone),[LinkedIn](https://www.linkedin.com/company/2886771?trk=tyah&trkInfo=clickedVertical%3Acompany%2CclickedEntityId%3A2886771%2Cidx%3A2-3-4%2CtarId%3A1483744835083%2Ctas%3ASentine) eller[Facebook](https://www.facebook.com/sentinelone/).