



RAPPORT

SÄKERHETSRAPPORT OM MALWARE: SKYDDA VERKSAMHETEN, KUNDERNA OCH VINSTEN

INNEHÅLL

- 3 MALWARE (SABOTAGEPROGRAM) DYKER UPP PÅ WEBBPLATSER ÖVERALLT
- 3 VAD ÄR MALWARE?
- 4 HUR GÅR ETT MALWAREANGREPP TILL?
- 5 AFFÄRSMODELLEN FÖR MALWARE
- 6 SAMMANFATTNING
- 6 OM VERISIGN



SÄKERHETSRAPPORT OM MALWARE: SKYDDA VERKSAMHETEN, KUNDERNA OCH VINSTEN

MALWARE DYKER APP PÅ WEBBPLATSER ÖVERALLT

Den här rapporten hjälper dig att förstå hotet från malware, även kallat sabotageprogram, och hur det kan påverka affärerna på nätet. Vi visar vilka motiv brottslingarna har för att distribuera malware på nätet och hur de infekterar webbservrar. I rapporten belyser vi också de tekniker som systemadministratörerna kan använda för att upptäcka när och hur angriparna har smittat webbservern.

Några exempel på andra viktiga punkter att diskutera när det gäller malware:

- Hur angriparna distribuerar malware via webbläsare i stället för via traditionella metoder, t.ex. infekterade e-postbilagor.
- Vilka motiv moderna brottslingar har när de infekterar slutanvändarsystem.
- Hur malware distribueras genom infektering av äkta webbplatser.
- Vilka verktyg som har utvecklats för att infektera så många sidor som möjligt.
- Hur datorbrottslingarna har utvecklat angreppstekniker som gör att malware kan infektera tusentals webbplatser samtidigt genom att utnyttja sårbarheter på webbplatserna.
- Hur angriparna distribuerar sin kod via skadlig reklam för att infektera de populäraste och ofta väl skyddade webbplatserna.

VAD ÄR MALWARE?

Malware är en allmän term för program vars syfte är att skada eller möjliggöra brott och detta är ett allt större problem på Internet. Hackare installerar sabotageprogram genom att utnyttja säkerhetsbrister i webservern och på så sätt få tillträde till webbplatsen. Sabotageprogram inbegriper allting från reklamprogram, som visar oönskad popup-reklam, till trojanska hästar (trojaner), som kan hjälpa brottslingar att stjäla konfidentiell information, t.ex. bankkontouppgifter.

Malware distribueras allt oftare via webbläsare. Metoden har blivit vanligare på senare år, eftersom filtrering av e-post har gjort det svårare för angriparna att distribuera sina program via spam. Dessutom går det inte längre så lätt att sprida från

system till system via nätverk på grund av att brandväggar har blivit allt vanligare på arbetsplatserna och i hemmen. Via webben finns möjligheter för hackare att tränga in på ditt företags webbplats och använda den som värd för spridning av malware till dina kunder.

Sabotageprogrammets kod är inte lätt att upptäcka och den kan infektera kundernas datorer bara genom att de besöker din webbplats. Sådana program kallas för "drive-by malware" (förbifarts-program) och användarna är i stor utsträckning (eller helt och hållet) ovetande om att systemet har blivit smittat genom den här typen av angrepp – vilket gör detta till ett alldeles särskilt lömskt problem. Hackarna använder sådana program för att sprida virus, kapa datorer eller stjäla känsliga data, t.ex. kreditkortsnummer eller andra personliga uppgifter.

Hur drive-by malware fungerar drive-by malware och är små webbplatser utsatta för risk?

Malware av det här slaget hämtas automatiskt till användarens system utan dennes godkännande. Datorbrottslingar utnyttjar sårbarheter hos webbläsare och/eller insticksprogram för att överföra sabotageprogrammet genom att gömma det på en webbsida som osynligt element (t.ex. en inbäddad ram - "iframe" - eller ett svårtolkat javaskript), eller genom att bädda in den i en bild (t.ex. en Flash- eller PDF-fil) som omärkbart skickas från webbplatsen till besökarens dator. Alla typer av webbplatser löper risk att drabbas. Små webbplatser kan vara mer sårbara, eftersom de ofta inte har de resurser och den expertkunskap som krävs för att upptäcka och snabbt åtgärda angrepp.

Malware kan infektera dina kunders datorer även om de bara är inne och tittar på din webbplats. Genom att inrikta sig på webbplatser med låg trafik kan hackarna undgå upptäckt längre och därigenom vålla mer skada.



HUR GÅR ETT MALWARE ANGREPP TILL?

För att infektera en dator via en webbläsare måste en angripare göra två saker. För det första måste han hitta ett sätt att få kontakt med offret. Sedan måste han installera sabotageprogrammet i offrets dator. Båda de här momenten kan genomföras snabbt och utan att offret märker något, alltefter angriparens metod.

Ett sätt för angriparen att få offrets webbläsare att köra sabotageprogrammet är att helt enkelt be offret att besöka en infekterad webbplats. Självklart är det få som besöker en webbplats om de får veta att den är infekterad, och angriparen måste därför maskera det onda syftet med webbplatsen. Listiga angripare använder de senaste metoderna och skickar ofta meddelanden infekterade med sabotageprogram via sociala nätverk, t.ex. Facebook, eller via snabbmeddelandesystem (Instant Messaging). Även om dessa metoder har visat sig fungera förhållandevis bra, förutsätter de fortfarande att användaren lockas att besöka en viss webbplats.

Andra angripare siktar in sig på webbplatser som potentiella offer besöker på eget initiativ. För att åstadkomma detta smittar angriparen en sådan webbplats genom att där lägga in ett litet stycke HTML-kod, som länkar till den egna servern. Koden kan hämtas var som helst, inklusive en helt annan webbplats. Varje gång en användare besöker en webbplats som är smittad på detta sätt, har angriparens kod möjlighet att infektera användarens system med malware.

Vanliga typer av överföringsmetoder för malware:

- **Programuppdateringar:** Ett malware kan skapa inbjudningar på webbplatser för sociala medier och lockar användarna att se en video. Med den länken försöker man lura användarna att tro att de behöver uppdatera den programvara som behövs för att se videon. En programvara som är skadlig.
- **Bannerannonser:** Intet ont anande användare klickar på en bannerannons som då försöker installera malware på användarens dator, eller också kan användaren skickas till en webbplats där han uppmanas att hämta en PDF med ett väl dolt sabotageprogram. Han kan även uppmanas att ange betalningsuppgifter för att kunna hämta en viss PDF-fil.
- **Nedladdningsbara dokument:** Användaren lockas att öppna ett välkänt program, t.ex. Microsoft Word eller Excel, som innehåller en förinstallerad trojan.
- **”Man-in-the middle”-angrepp:** Användarna kan tro att de kommunicerar med en webbplats som de litar på. I själva verket samlar en datorbrottsling in de data som användarna skickar till webbplatsen, t.ex. inloggningsnamn och lösenord. Eller så kan brottslingen kapa (ta över) en session och hålla den öppen när användaren tror att den har stängts. Brottslingen kan sedan genomföra sina skadliga transaktioner. Om användaren var inloggad på en bank, kan brottslingen överföra pengar. Om han gjorde inköp, kan en brottsling få tillgång till och stjäla det kreditkortsnummer som användes vid transaktionen.
- **Tangentloggare:** Användaren luras – med någon av ovan nämnda metoder – att hämta en programvara som loggar (registrerar) tangenttryckningar. Loggningsprogrammet övervakar sedan vissa åtgärder, t.ex. musanvändning eller tangenttryckningar och tar skärmdumpar för att på så sätt få reda på privata bank- eller kreditkortsuppgifter.



AFFÄRSMODELLEN FÖR MALWARE

Hur gör angriparna för att tjäna pengar på sina sabotageprogram? De kan på många sätt använda infekterade datorer i vinstsyfte. Ett av de enklaste är genom annonsering. Precis som många webbplatser skaffar sig inkomster genom att visa reklam, kan sabotageprogram visa annonser som ger datorbrottslingen inkomster.

Ett annat sätt är genom utpressning. Ett stort nätverk med infekterade datorer kan vara mycket kraftfullt, och vissa angripare använder detta hot för att få webbplatsägare att betala ut pengar till dem. En grupp datorer som styrs av en angripare, ett så kallat "botnät", kan skicka en väldig massa trafik till en webbplats, vilket kan leda till att den överbelastas. Brottslingen kan sedan kontakta webbplatsens ägare och begära pengar för att upphöra med angreppet. Brottslingar använder också ofta infekterade datorer för att samla in värdefulla användardata, t.ex. personuppgifter för Internet-banker. Detta slags sabotageprogram, en så kallad "infostealer" (infotjuv) eller banktrojan, är en av de mest raffinerade och lömska formerna av sabotageprogram. Brottslingen kan sedan använda personuppgifterna för eget brottsligt bruk eller sälja dem till någon som kan använda dem i vinstsyfte.

Vad är svartlistning och varför är det viktigt att undvika det?

På grund av den avsevärda skada som kan vållas av sabotageprogram, placerar Google, Yahoo, Bing och andra sökmotorer varje webbplats som visar sig vara infekterad med ett sådant program på en blockeringslista, en "svart lista". Efter en sådan svartlistning skickar sökmotorn en varning till eventuella besökare om att webbplatsen är osäker, eller så blir den helt och hållet utesluten ur sökresultaten.

Det spelar ingen roll hur mycket du har "sökoptimerat" din webbplats - om den blir svartlistad kan effekten på affärsverksamheten bli förödande. Svartlistningen kan göras utan föregående varning, görs ofta utan din vetskap och är mycket svår att häva. Att vidta lämpliga åtgärder för att förhindra svartlistning av sökmotorer är av avgörande betydelse för det långsiktiga resultatet för varje webbplats.

VERISIGN ÄR FORTSATT LEDANDE INOM NÄTSÄKERHET

VeriSign var, i mitten av 1990-talet, först med en kommersiell SSL-lösning. Vi är den främsta leverantören av SSL-certifikat, och VeriSign är i dag världens mest kända märke för Internet-säkerhet. Det anseendet har odlats under många år och har utvecklats tillsammans med kunder och nätföretag. VeriSigns branschledande ställning och tillämpningen av den senaste tekniken har gjort våra SSL-lösningar ledande på marknaden.



Utöver den sinnesro som det ger när man väljer ett beprövat SSL-certifikat har VeriSign fortsatt att rikta in sig på sina kunders behov genom att ständigt förbättra sin SSL-teknik med stöd för nya standarder och med integration med kompletterande tekniker och lösningar. VeriSign fortsätter på den vägen genom att i sina SSL-lösningar erbjuda daglig malwaresökning av webbplatser för att på så sätt säkerställa att din webbplats, ditt värdefulla varumärke och dina kunders konfidentiella information är skyddade mot de ständigt föränderliga hoten på Internet.



SAMMANFATTNING

Försäljning och tjänster via nätet har vuxit enormt under det senaste årtiondet. Den allt större användningen av Internet har samtidigt medfört ökad brottslig aktivitet. Malware har blivit allt vanligare, och de äventyrar e-handelns tillväxt genom att skapa rädsla för att privat information ska hamna i orätta händer. Detta leder till oro, som i sin tur gör att nätföretagens resultat inte är vad de borde kunna vara. Det behövs ett effektivt sätt att bekämpa användningen av sabotageprogram om e-handeln ska kunna utnyttja alla sina möjligheter.

VeriSign tillhandahåller en övergripande, förtroendeskapande lösning för din näthandelsverksamhet genom att kombinera den främsta typen av SSL-certifikat med innovativa funktioner, detta för att säkerställa att dina offentliga webbplatser regelbundet genomsöks efter malware. I kombination med VeriSignsigillet, världens främsta förtroendemärke, hjälper VeriSign dig att lugna dina kunder när de har kontakt med dig via nätet. Om du vill vara säker på att konsumenterna ser din webbplats som en tillförlitlig e-handelsplats, är VeriSigns SSL-certifikat rätt val.

OM VERISIGN

VeriSign är den betrodda leverantören av infrastrukturtjänster på Internet för den digitala världen. Miljarder gånger varje dag förlitar sig företag och konsumenterna på vår Internetinfrastruktur för att kommunicera och sköta sina affärer på ett säkert sätt.

Besök oss på www.Verisign.eu för mer information.

