Whitepaper

KASPERSKY lab

TA TILLBAKA kontrollen

Be Ready for What's Next.

INNEHÅLL

Det pågår ett krig

Under tre dagar i slutet av 2009 kom cyberbrottslingar över bankuppgifter, användarnamn och lösenord hos Texas-företaget Hillary Machinery och genomförde mer än 45 enskilda transaktioner till över 40 olika mottagare. Resultatet blev en förlust på över 800 000 dollar. Även om Hillary Machinery lyckades få tillbaka en del förlorade de 250 000 dollar, och fick dessutom stå för advokat- och rättegångskostnader. En tvist pågår fortfarande mellan företaget och banken. Företagets ägare Troy Owen säger: ”Även om förlusten inte fick oss på fall så har det definitivt gjort att våra utvecklingsplaner har fått läggas på is.”

Det går inte en dag utan att tidningarna skriver om företag som råkar ut för cyberattacker. Databrottsligheten formligen exploderar. Banktrojaner stjäler inloggningsuppgifter till bankerna och offren drabbas av massiva ekonomiska förluster. Under 2010 genomförde CSO Magazine undersökningen Cyber Security Watch Survey. Chefredaktören Bill Brenner slår fast: ”Även de företag som gör stora satsningar på datasäkerhet medger att det nästan är omöjligt att hålla sig framför kriminaliteten.” Det pågår ett krig. Ett krig mot cyberbrottslingar som endast har ett mål i sikte - att stjäla andras pengar. Dagens cyberbrottslingar är ständigt på jakt efter data som lätt kan omvandlas till pengar eller inloggningsuppgifter som ger dem möjlighet att överföra medel direkt från företagens kassakistor.

SANS.ORG säger följande i sin rapport The Top Cyber Security Risks: ”Antalet attacker är nu så stort och brottslingarna så avancerade att många organisationer har problem med att avgöra vilka nya hot och sårbarheter som utgör den största risken. De vet inte hur de ska fördela sina resurser för att åtgärda de mest troliga och skadliga attackerna först. Även om IT-avdelningarna satsar på säkerhet idag missar många att skydda det primära attackmålet - användarnas enheter.

Användares stationära eller bärbara dator eller smartphone – det primära målet för dagens cyberbrottslingar. Användarnas IT-utrustning blir alltmer mobil och det traditionella ”IT-gränssnittet” är ett inadekvat begrepp för att avgöra rätt skydd för företagen och användarna. IDC konstaterar att ”användarnas utrustning nu är den primära försvarslinjen”. I den här artikeln behandlas det växande hotet från sabotageprogram, hur cyberbrottslingar riktar in sig på användarna och hur du kan skydda deras utrustning från skadliga aktiviteter.

Det växande hotet från sabotageprogram

Under de senaste 25 åren har Kaspersky Lab skyddat företagen från Internethot och vi kan idag konstatera en exponentiell tillväxt av hot från skadliga program. Siffrorna nedan är onekligen en tankeställare. Över 70 000 nya hot upptäcks varje dag - 3,4 miljoner upptäcktes under hela 2009. Över 3 500 antivirussignaturer släpps varje dag för att skydda från de senaste attackerna. En särskilt hektisk dag skapade Kaspersky 13 500 signaturer för att bekämpa den stora volymen hot som spreds den dagen. Utöver traditionellt skydd av arbetsstationer och servrar har över 1 200 signaturer skapats för att skydda smartphones mot hot från skadliga program.

Och trenden fortsatte under 2010:

• Under första kvartalet 2010 gjordes över 327 miljoner försök att infektera användardatorer över hela världen, en ökning med 26,8 % jämfört med föregående kvartal.

• Under första kvartalet 2010 upptäcktes dessutom över 119 miljoner värdservrar för skadliga program av vilka 27,57 % fanns i USA, 22,59 % i Ryssland och endast 12,84 % i Kina.

• Det totala antalet attacker som riktade in sig mot sårbarheter i webbläsare och insticksprogram, samt PDF-läsare, ökade med 21,3 % varav nära hälften riktade in sig på sårbarheter i Adobe-program.

Ett tekniskt dokument om cyberbrott som nyligen släpptes av RSA avslöjar att 88 % av företagen på Fortune 500 har haft datorer infekterade med trojaner i sina miljöer. Enligt Uri Rivner vid RSA är ”dessa trojaner fullt upptagna med att flytta flera TB företagsdata till dolda drop zones i ’dark cloud’ i den kriminella cybervärldens infrastruktur”. Hans uppfattning bekräftas av data som rapporterades av CNET News i oktober 2009 där det angavs att 63 % av de medelstora företagen upplevde att cyberhoten ökade under 2009. Enligt artikeln anser 71 % av de medelstora företagen i USA att en allvarlig attack skulle driva dem till nedläggning. Detta häpnadsväckande avslöjande tydliggör fokus för dagens cyberbrottslighet - stöld av pengar. Faktum är att enligt FBI:s Internet Crime Complaint Center har cyberbrottsligheten ökat med 22,3 % under 2009, medan rapporterade förluster på grund av dessa brott mer än fördubblades från 265 miljoner dollar till över 560 miljoner dollar under samma år. Betänk att siffrorna endast gäller de attacker som har rapporterats. Eftersom det stora antalet attacker inte rapporteras är antalet och de ekonomiska förlusterna betydligt större.

Förutom allt skadligare attackmetoder som resulterar i allt större stölder per intrång riktar sig cyberbrottslingarna inte längre enbart mot de stora företagen. Små företag, statliga och lokala myndigheter samt utbildningsinstitutioner är särskilt i fokus för cyberbrottslingarna eftersom de ofta inte har tillräckliga säkerhetsbudgetar och -skydd. Medelstora företag i USA förlorade över 100 miljoner dollar under 2009 genom bedrägliga banköverföringar. Till och med Pentagon, en organisation som gör stora investeringar på säkerhetsområdet, utsattes för cyberbrott under 2009 vilket resulterade i förlust av flera TB data, inklusive data om det nya attackflygplanet F35 Lighting II. Trots att deras mest känsliga information lagras på datorer som inte är anslutna till Internet lyckades hackare få tillgång till topphemlig information via datorer tillhörande tredjeparts underleverantörer som var inhyrda för att konstruera och bygga jaktflygplanen.

Varför är slutanvändarna målet?

De ökande hoten från dagens sabotageprogram är fokuserade på användarnas utrustning. Varför är det så? Varför är cyberbrottslingar så intresserade av slutanvändarna? Förklaringen ligger i flera faktorer:

• Decentraliserade data. Data lagras inte längre på stordatorer. Känsliga och hemliga affärsdata skapas, används och sparas på stationära eller bärbara datorer och till och med på smartphones. Att få tillgång till sådana enheter innebär åtkomst till data med ett stort ekonomiskt värde.

• Nycklarna till kungariket. Genom att placera rätt trojan i ett användarsystem får cyberbrottslingen åtkomst till data samt inloggningsuppgifter till andra system inom företaget, inklusive bank- och finanssystem. Miljontals dollar förloras varje dag genom bedrägliga överföringar från företagens bankkonton genom dessa inloggningsuppgifter som har fångats in av trojanerna.

• Total kontroll. Åtkomst på root-nivå i en dator ger också cyberbrottslingen åtkomst till alla system eller data som datorns legitima användare har tillgång till. Cyberbrottslingen kan även göra om datorn till en ”zombi”-maskin som ingår i ett större botnet, och som kan användas till att sprida sabotageprogram till andra system. Och framförallt, med åtkomst av den här typen kan hackaren övervaka e-post, chatt, Internet-trafik samt tangenttryckningar och mycket mer. Hackaren får tillgång till en rik källa av möjligheter.

Dagens datorhackare är inte av samma karaktär som gårdagens skriptglada nördar som sökte berömmelse och ära. Dagens cyberbrottslingar har ingen önskan att avslöja sig. De vill kunna stjäla data och pengar utan användarens vetskap.

Att antal faktorer gör slutanvändaren till ett lätt offer:

• Enkel åtkomst. Nätverken saknar skarpa gränser. De har blivit mer genomsläppliga för att slutanvändarna ska kunna ha ständig tillgång till allt som Internet har att erbjuda. Slutanvändarna är den nya frontlinjen och därför det nya målen för cyberbrottslingarna.

• Mobila data. Företagens representanter reser världen runt och ansluter till oskyddade nätverk på flygplatser och hotell, i flygplan och i hemmet. Dessa nätverk ligger utanför företagens skyddade miljö. Affärsdata är utsatta för ständiga hot, gränserna blir än mer uppluckrade och mottagliga för cyberbrott.

• Många attackvektorer. Slutanvändarna använder idag Internet både för arbete och personliga göromål vilket ger cyberbrottslingen flera attackvektorer. Välkända webbplatser blir leverantörer av sabotageprogram och sociala medier en lekplats för cyberbrottslingar. Cyberbrottslingarna spanar på enskilda personer och företag och engagerar sig i sociala online-medier för att hålla kontroll över vänner, familj, kunder, potentiella kunder och partners. Personlig surfning på Internet, webbplatser för dating, musik, video osv. är andra attackvektorer för cyberbrottslingarnas skadliga kod. Och låt oss för all del inte glömma det ständigt närvarande hotet från e-post.

Det yttersta målet är att smitta användarutrustningen med sabotageprogram. Än en gång citerar vi RSA:

”Efter infekteringen börjar sabotageprogrammet, ofta en trojan, att registrera all Internet-relaterad trafik, loggar tangenttryckningar, tjuvläser e-post, lösenord som har sparats i webbläsaren och en lång rad med andra data. Trojaner nöjer sig inte med bankinloggningsuppgifter och kreditkortsdata. De kan stjäla hela din sociala nätverksstatus eller din medicinska historik, privata chatt, kommunikation med myndigheter och allt arbetsrelaterat innehåll, inloggningsuppgifter till interna system, e-post som du har skickat och tagit emot, företagets bokslut eller känsliga kundrelaterade webbformulär i kundvårdssystem”.

När trojanen väl är installerad i användarsystemet sprider den sig snabbt och försåtligt, och kan på många sätt bli otroligt lönsam. Det är inte att undra på att cyberbrottslingarna medvetet riktar in sig på slutanvändarna. Utan rätt typ av skydd erbjuder företagens användarutrustningar en miljö med rika möjligheter till intrång.

Hur attackerar cyberbrottslingarna slutanvändarna?

Tror du att du är säker? Tro inte det. Att skydda nätverksgränser har visat sig vara ineffektivt när det gäller de senaste målen för cyberbrottsligheten. Enligt Uri Rivner vid RSA ”... slagfältet håller på att förändras. Anställda, snarare än nätverket, är nu i frontlinjen”. Låt oss titta på hur dagens cyberbrottslingar riktar in sig på slutanvändarna. Förr var operativsystemet - i första hand Microsoft Windows - hackarens paradis. Allt eftersom operativsystemen har blivit säkrare har klientprogram från tredjepart hos slutanvändarna blivit den främsta attackvektorn för cyberbrottslingar. Användaren hämtar program som t.ex. WinZip, Realplayer, Quicktime, Adobe PDF och insticksprogram till webbläsare (ActiveX-kontroller, videokodec osv.) och har inget större intresse av att underhålla dessa applikationer. Dessa odokumenterade program som aldrig underhålls och sällan uppdateras är fulla av sårbarheter. IT-avdelningen vet knappast vilken version av dessa program som körs i deras miljöer eller vilka uppdateringar och korrigeringar som har installerats.

Enligt statistik från Secunia PSI är endast 2 % av alla Windows-datorer fullständigt uppdaterade.

Det är på grund av dessa sårbarheter som cyberbrottslingarna får tillgång till företagens användarutrustning och kan skicka sabotageprogram till att utföra sina onda planer.

Cyberbrottslingar riktar sina sabotageprogram mot användarna via ett antal attackvektorer:

• Kommunikationsbehovet. 8 av 10 e-postmeddelanden innehåller i dagsläget skadligt eller oönskat innehåll. Enligt Gartner sexfaldigades hoten från e-post under 2009. Hoten inkluderar infekterade bilagor, nätfiskelänkar och omdirigeringar till tredjeparts servrar som laddar ned sabotageprogram.

• Goda webbplatser blir dåliga. Över 1,73 miljarder användare, 25 % av världens befolkning, besöker över 234 miljoner webbplatser varje dag. Enbart under 2009 skapades 47 miljoner nya webbplatser på Internet. Cyberbrottslingarna använder den exponentiella ökningen i Internet-surfande till att sprida sin skadliga kod till intet ont anande användare. Två tekniker, SQL-injektion och XSS (Cross-Site Scripting), står för 80 % av alla webbattacker. Cyberbrottslingarna drar nytta av Internets sårbarhet och använder dessa attackmetoder för att hacka etablerade webbplatser och plantera förbryllande JavaScript som hämtar sabotageprogram när användarna besöker sidan. Det här kallas för ”drive-by download”. Användarna infekteras med sabotageprogram genom att helt enkelt besöka oskyldiga webbplatser som har blivit infekterade av servrar från tredje part. Sabotageprogram sprids inte längre enbart genom webbplatser för spel och porr. 77 % av webbplatserna som innehåller skadlig programvara är helt oskyldiga webbplatser som har blivit komprometterade av cyberbrottslingar.

• Ständig uppkoppling. Sociala medier är på uppåtgång för både enskilda och företag.

Behovet av att hålla kontakten med partners, kunder, marknad, familj och vänner har lett till att företagen har öppnat sina skyddade gränser för en mycket osäker form av masskommunikation. Facebook, LinkedIn, Twitter och MySpace är vanliga sociala medier som företagen låter sina anställda besöka varje dag, både av privata och yrkesmässiga skäl.

Cyberbrottslingar riktar in sig på den snabbt växande användningen av sociala medier för att tjäna pengar, dvs. stjäla, och för att sprida sabotageprogram till datorer och in i företagens nätverk. Sociala medier bygger på två vanliga mänskliga egenskaper: tillit och nyfikenhet. Du känner tillit eftersom du endast bjuder in den som du känner och litar på, och därför är innehållet som sänds från dina vänner ”OK”. Nyfikenheten driver dig att klicka. Den typiska användaren klickar på snart sagt vad som helst. Problemet är att vi sällan vet vart klickandet leder eller vilka skador som kan uppstå genom att öppna en fil, en webbplats eller en app. Dessa två egenskaper i kombination gör sociala medier synnerligen farliga.

• Rädsla, osäkerhet och misstro. Scareware och ransomware håller på att bli vanliga metoder för att lura pengar från godtrogna och ovana användare. Medan de besöker en webbplats dyker det upp ett meddelande som talar om att användaren har virus och är utsatt för en risk. Meddelandet erbjuder skydd genom ett (falskt) säkerhetsprogram som kan laddas ned för ca 30 - 60 dollar. Säkerhet används alltså som lockbete. Sanningen är att du förlorar pengar och att programmet du laddar ned i själva verket är det skadliga programmet, och inte ett program som skyddar dig från skadliga program. Scareware-bedragare tjänar tre gånger så mycket som VD:n på ditt företag.

Skydda användarna från cyberattacker

Hoten från sabotageprogram har vuxit exponentiellt och det kan konstateras att IT-säkerhetsbudgeten knappast har ökat i samma omfattning. Än mer värt att notera är att utgifterna för slutanvändarskydd inte har vuxit i takt med det verkliga hotet. Traditionellt har IT-avdelningarna fokuserat på nätverksgränssnittet - brandväggar, IDS och IPS, spam- och URL-filter. Trots att dessa är absolut nödvändiga och en viktig del i en skalbaserad säkerhetsstrategi är de inte särskilt användbara när det gäller att skydda slutanvändarna från våldsamma angrepp med flera attackvektorer. URL-filter hindrar användarna från att besöka vad som betraktas som ”dåliga webbplatser”, men fungerar inte för att skydda dem från sabotageprogram som sprids genom drive-by-download på etablerade webbplatser. Brandväggar konfigureras för att ge användarna obegränsad tillgång till Internet. Ironiskt nog betyder det även att cyberbrottslingar får direkttillgång till datorerna.

Skydd av användarutrustning har länge betraktats som en produkt, med priset som den avgörande urvalsfaktorn. Det finns till och med företag som använder sig av gratis antivirus-program. Tyvärr medföljer även skadlig programvara ”på köpet”. Med IT-avdelningar som fokuserar på att skydda nätverksgränssnitten ägnas AV-skydd inte särskilt mycket uppmärksamhet. Vissa IT-chefer ser inte heller skillnaden mellan olika AV-produkter. Det finns de som tror att alla antivirusprogram är skräp och väljer ut det de anser vara minst dåligt.

Åsikterna är förståeliga med tanke på de katastrofala erfarenheter som vissa kunder har haft. Men de är långt ifrån riktiga. Faktum är att det är stor skillnad på hur olika antivirusprogram detekterar och tar bort skadliga program från datorer, vilket en lång rad med oberoende testlaboratorier har kunnat visa. Nu är det dags att ändra inställning och fokusera både på detektering och respons hos användarna.

Otaliga faktorer måste beaktas när antiviruslösningar utvärderas:

• Total detekteringsgrad: Hur effektiv är leverantören när det gäller att detektera både känd och okänd skadlig kod, där den tidigare bygger på signaturbaserad analys och den senare bygger på heuristiska eller regelbaserade analyser. Leverantören ska kunna detektera många varianter av skadlig kod: Trojaner, virus, rootkits osv. Bra resultat på viss typ av detektering, men dåligt på en annan, ger ett otillräckligt skydd.

• Heltäckande skydd: Skadliga program kan infektera en enhet på många olika sätt och alla säkerhetsföretag värda namnet borde effektivt kunna blockera alla attackvektorer mot användaren. Säkerhetsleverantören bör även kunna skydda systemet oavsett dess fysiska belägenhet och enkelt kunna anpassa skyddet när utrustningen flyttas, så att säkerheten kan intensifieras utanför företagets nätverksgränssnitt. Personliga brandväggar, ID, antispam, antivirus, antinätfiske, skydd mot sabotageprogram och mycket mer måste alla betraktas som viktiga delar i den totala skyddsstrategin.

• Prestanda: Skyddet är inte mycket värt om det hindrar användaren från att utföra sina uppgifter. ”Bloatware”, som antivirusprogram ofta kallas, använder så mycket systemresurser att den anställde inte kan använda sitt datorsystem förrän skanningen är klar. Det är oerhört viktigt att skyddet påverkar den anställdes produktivitet så litet som möjligt. Är det möjligt att få skydd och prestationer samtidigt? Absolut!

• Administration: Antivirusskyddets administrativa konsol är en mycket viktig beslutsfaktor vid valet av system. En omständlig, svårförståelig, resursintensiv administration gör det svårt att hantera säkerheten och hela säkerhetslösningen kommer att bli lidande. Administration ska vara enkel och lättarbetad, men ändå granulär och kraftfull nog för att förhindra risker i användarnas datormiljö. Det ska dessutom gå snabbt att genomföra installation och underhåll av säkerhetspunkterna på användarnivån.

• Support: Ingen har tid att sitta och vänta i 45 minuter eller mer för att få hjälp med ett problem, och det ska ingen heller behöva göra. Testa supporten innan du köper ett AV-skydd så att du vet att de svarar snabbt och är effektiva. Hur snabbt svarar de på uppringningen? Hur effektivt löser teknikern problemet? Support ska inte vara till besvär, det ska vara en tillgång.

• Pris: Den här kategorin behandlas sist av ett särskilt skäl. Alla AV-företag är i dagsläget mycket konkurrenskraftiga när det gäller priset. Men de är inte lika konkurrenskraftiga när det gäller funktionen. Priset är viktigt, med först när du har hittat ett säkerhetsprogram som ger dig rätt skydd, funktion och administration.

Skyddet av användarnas enheter är för viktigt för att bara ses som ett produktinköp. En noggrann inventering av antivirusskydd försäkrar dig om att du får bästa detektering och respons på användarnivå.

När det kommer till kritan - är du verkligen säker?

Stephan, administratör vid Jackson Public School i Mississippi, trodde att han hade rätt skydd för att förhindra att sabotageprogram infekterade hans nätverk. Stephan hade ansvar för mer än 9 200 enheter och hade vidtagit omfattande åtgärder för att se till att alla var säkra. När de på grund av prestandaproblem bytte leverantör till Kaspersky upptäckte de hur oskyddade de i själva verket hade varit. Vid installationen av Kaspersky upptäckte IT-teamet att nätverket var i högsta grad infekterat:

- 14 459 virusinstallationer hittades hos slutanvändarna
- 43 olika trojaner
- 56 olika virus
- 15 701 infekterade objekt över hela nätverket

Den skadliga programvaran hade julafton! Deras tidigare antivirusprogram hade inte klarat av att upptäcka och ta bort sabotageprogram. Det var först när de installerade ett förstklassigt antivirus-paket från Kaspersky Lab som de upptäckte hur infekterade de var. Virusnivån var helt oacceptabel med tanke på de investeringar som trots allt hade gjorts för att skydda sig mot risker. De fick offra arbetstid och kostnader i veckor innan alla hot i miljön var utrensade. Du kanske tror att du är säker, men är du säker på det? Vem har tillgång till dina data utan att du vet om det? Vem kan använda användarnas utrustning för att komma igenom gränssnittsäkerheten som du så noggrant har byggt kring ditt nätverk? Blockerar din aktuella säkerhetsleverantör verkligen skadliga program och skyddas verkligen användarnas enheter? Detta är viktiga frågor i dagens hotfulla digitala miljö och de kräver svar.

Det är dags att ta upp kampen mot cyberbrottsligheten, och frontlinjen finns hos slutanvändarna!

I del 2 av artikeln tar vi upp 10 sätt för cyberbrottslingar att komma över data och inloggningsuppgif-ter hos slutanvändarna utan att IT-avdelningarna stoppar dem. Det krävs en helt annan syn på IT för att åstadkomma ett välfungerande skydd för användarens utrustning - och användaren. Cyberbrott får inte löna sig!

Gå till www.kaspersky.com för att hämta del 2 i Det pågår ett krig.

Det är dags att ta upp kampen mot cyberbrottsligheten - och frontlinjen finns hos slutanvändarna!

Kaspersky Lab AB
Färögatan 33
164 51 Kista
Sweden

+46 8 5785 3000
corporatesales@kaspersky.se

www.kaspersky.se
www.securelist.com
www.threatpost.com

17za