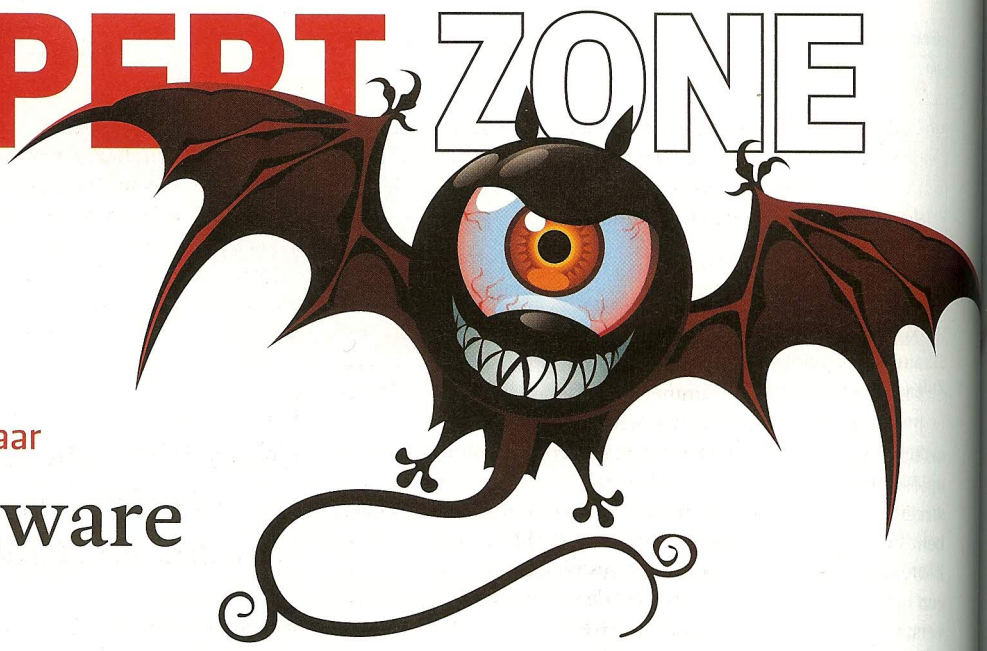
EXPERT ZONE



Smartphones in gevaar

Gaat malware mobiel?

Het zal ook cybercriminelen niet zijn ontgaan dat iedereen tegenwoordig met een smartphone rondloopt. Slaat de malware-epidemie over naar je mobiele toestel of moet je de dreiging uit een andere hoek verwachten? • R.P.

Paniek bij Android-gebruikers deze zomer. Antivirusbedrijf Kaspersky bracht naar buiten dat een valse applicatie, vemomd als gratis mediaspeler, na installatie ongemerkt SMS'jes stuurde naar dure betaalnummers, waarna de malwareschrijver de winst opstreek. Uiteindelijk bleek slechts een klein groepje Russische Android-eigenaren geïnfecteerd, maar het nieuws zorgde er wel voor dat de gratis antivirus-app DroidSecurity in korte tijd ruim vijf miljoen keer werd gedownload.

Staan we op de drempel van een nieuwe mobiele malware-epidemie? Nauwelijks. Volgens het Finse antivirusbedrijf F-Secure zijn er op dit moment welgeteld 520 mobiele virussen in omloop. Niet erg indrukwekkend vergeleken met de duizenden nieuwe Windows-malwarebesmettingen die dag in dag uit opduiken. Mobiele virussen zijn duur, mobiele besturingssystemen zijn nog niet ingeburgerd en de malwaremaffia richt zich liever op het vinden en massaal uitbuiten van nieuwe lekken in Windows(-programma's).

Lokale antivirusexpert Eddy Willems van G-Data, denkt ook dat een malwareplaag voor smartphones voorlopig nog wel even op zich laat wachten: "Er is nog geen duidelijke winnaar uit de bus gekomen in de wereld van de mobiele besturingssystemen, terwijl we op de pc een reuzenaandeel van Microsoft Windows zien. Het loont meer om malware te maken voor Windows dan voor welk mobiel platform dan ook."

Sociale netwerken

Als de dreiging voorlopig niet van de kant van je Android-telefoon, iPhone of Windows Phone 7-toestel komt, waar moet je je dan wel voor hoeden? Verrassend genoeg is je eigen sociale omgeving een veel groter gevaar. "E-mail is uit bij online criminelen, sociale netwerken zijn in," zegt hoofdonderzoeker Mikko Hyppönen van F-Secure. Hij geeft aan dat mensen veel sneller geneigd zijn om een uitnodigende link van een online contact in Facebook aan te klikken dan een bijlage in een e-mail te openen. "Spam verplaatst zich naar de sociale netwerken, want daar is het vertrouwen te vinden", aldus Hyppönen.

De grote populariteit van Facebook en Twitter hebben online criminelen duidelijk niet onberoerd gelaten. Om de andere week duikt weer een nieuwe worm of exploit op die gebruikmaakt van een veiligheidslek in de vaak reusachtige netwerken. Twitter kreeg recent te maken met een agressieve worm die 'mouse on over'-technieken gebruikte, wat inhoudt dat gebruikers alleen al besmet werden door hun muis te laten rusten op een getwitterde weblink. Een Facebook-worm maakte gebruik van een JavaScript-lek en boobytrapte de 'Vind ik leuk'-knop op een valse pagina over een schokkende zelfmoord. En TrendMicro's TrendLabs pikte afgelopen september het Mehika-botnet op, waarbij besmette zombie-pc's commando's stuurden via Twitter.

In de meeste gevallen gaat het echter om besmette links die op Facebook of Twitter worden geplaatst. Omdat url-verkorters, diensten die ellenlange weblinks kleiner maken, enorm populair zijn op dit soort sites, is het vaak erg moeilijk te zien waar je op klikt en moet je dus vertrouwen op de afzender. Technici weten dan wel binnen enkele uren de gaten te dichten die besmetting mogelijk maken, maar die korte tijd is al genoeg om duizenden mensen te besmetten.

Vertrouwen, of eerder het misbruik daarvan, is en blijft het voornaamste wapen van online criminelen. Het tijdperk van massale besmettingen via e-mailvirussen en de daaropvolgende media-aandacht is voorbij. De moderne internetcrimineel schuwt aandacht tegen elke prijs en steelt liever kleine bedragen van een groot aantal gebruikers in plaats van in één keer zijn grote slag te slaan.

Uit het recent verschenen jaarlijkse Norton Cybercrime Report blijkt dat veel slachtoffers van dit soort aanvallen zich schamen

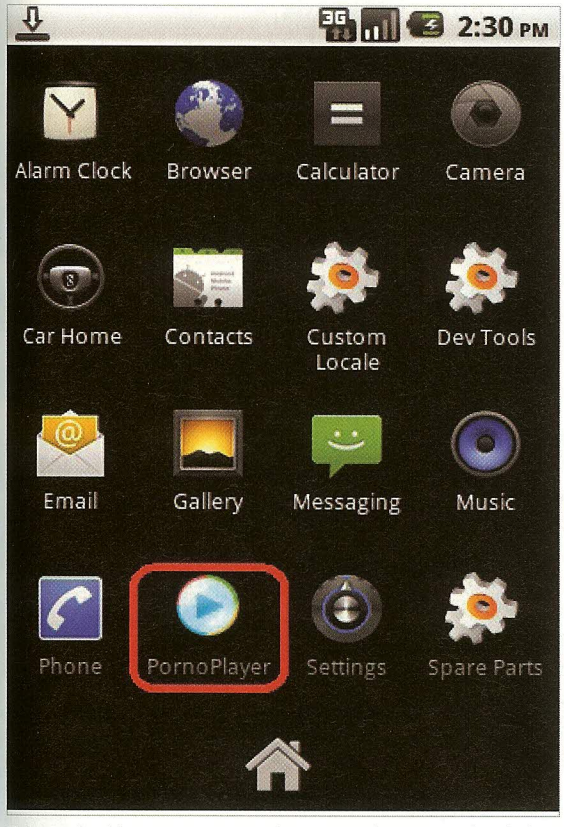
en vaak nalaten om naar de politie te stappen. Bovendien denktt vier op de vijf ondervraagden dat de daders toch niet gepakt zullen worden. Een kleine groep besluit om zelf achter de dader aan te gaan, wat een riskante onderneming kan zijn.

Gestolen data

Het stelen van je persoonlijke gegevens is allang geen uitdaging meer, munt slaan uit al die gestolen data is dat wel. Op het web zijn uitgebreide ondergrondse marktplaatsen te vinden waar duizenden kredietkaartnummers en paspoorten te koop worden aangeboden. Maar het daadwerkelijk gebruiken van die informatie is gevaarlijk en kan tot arrestatie leiden. Online bendes gaan daarom steeds creatiever te werk.

Zo organiseerde één specifieke crimineel online pokersessies, waarbij hij voor elke deelnemer afzonderlijk een nepaccount aanmaakte, elk gekoppeld aan een gestolen creditcard. Vijf 'spelers' verloren voortdurend, terwijl de zesde man in dit doorgestoken spel het witgewaste geld opstreek.

In een ander geval bood een online dief een nieuwe Playstation 3 aan via eBay. Hij vertelde de koper dat hij de spelconsole eerst zou opsturen en dat hij pas na aankomst hoefde te betalen. De crimineel kocht vervolgens met gestolen kredietkaartgegevens via Amazon een spelcomputer en liet die als cadeau afleveren. De ontvanger betaalde, maar omdat de kredietkaartmaatschappij vervolgens de transactie blokkeerde en Amazon aangifte deed, had de koper niet lang plezier van zijn aankoop. De PS3 werd in beslag genomen en het slachtoffer was zowel zijn geld als de console kwijt.



Een voorbeeld van een SMS-Trojan, gemaakt voor Android, dat na installatie stiekem dure betaalnummers belt (Bron: Securelist.com)

Beveiliging

Het risico slachtoffer te worden van dit soort praktijken weerhoudt internetgebruikers er echter niet van massaal gebruik te maken van online diensten. Bestanden worden online opgeslagen, gevoelige documenten en privémails gearchiveerd in webmailaccounts. De smartphone speelt daarbij een steeds belangrijkere rol, omdat mensen thuis en onderweg in contact willen blijven met hun (werk)omgeving. "Veel mensen realiseren zich niet hoeveel persoonlijke informatie ze op hun telefoon hebben staan en rusten het toestel niet eens uit met een wachtwoord", zegt Luc Beirens, lid van de Belgische Federal Cyber Crime Unit (FCCU). De gespecialiseerde agent zegt dat het verlies van een smartphone in sommige gevallen kan leiden tot het kapen van gevoelige accounts, waarna je grof geld moet betalen om ze terug te krijgen. "Het is immers niet altijd zo gemakkelijk te bewijzen dat een online account in jouw bezit is", aldus Beirens.

De moderne internetcrimineel steelt liever kleine bedragen van een groot aantal gebruikers in plaats van in één keer zijn grote slag te slaan.

Het verlies van een online account betekent niet alleen het verlies van online gegevens, het heeft soms ook tot gevolg dat besmettende links of spamberichten in jouw naam massaal naar persoonlijke en zakelijke contacten worden verstuurd. De imagoschade kan groot zijn, vooral omdat gebruikers niet meteen door hebben dat hun persoonlijke account voor dit soort doeleinden wordt ingezet.

De Koobface-worm in actie op Twitter. Het is erg lastig om vooraf te zien waar je op klikt, dus moet je afgaan op de afzender. (Bron: Securelist.com)