

Zelfs baas van Interpol valt twee keer ten prooi aan identiteitsdiefstal op Facebook

Criminelen veroveren cyberspace

Sociale media zijn voor criminelen een gemakkelijke manier om iemands netwerk binnen te dringen. Zelfs Ronald Noble, hoofd van Interpol, is er het slachtoffer van geworden. Er werden twee valse accounts in zijn naam aangemaakt op Facebook. Gisteren vielen dan weer duizenden twitteraars ten prooi aan hackers.

DOOR KATRIEN STRAGIER

BRUSSEL ● Ook het aantal virussen gericht naar sociale media is op een jaar tijd fors toegenomen. Een tiende van alle malware is intussen gesneden op leest van sociaalnetwerksites. 'Criminele aanvallen op social media zijn schering en inslag', weet Eddy Willems, beveiligingsexpert bij G Data. 'En niet alleen bij accounts van bekende figuren.'

Hij is een van de belangrijkste figuren in de politiewereld, maar toch is ook Interpolbaas Ronald Noble recentelijk het slachtoffer geworden van identiteitsdiefstal op het internet. Criminelen plaatsten op Facebook twee profielen online onder zijn naam, terwijl de echte Ronald Noble nooit een account heeft aangemaakt. Een van de nabootsers probeerde meer te weten te komen over een recente operatie van Interpol naar voortvluchtigen die worden gezocht voor moord, pedofilie, drugs en witwaspraktijken.



FOTO AFP

■ Criminelen plaatsten op Facebook twee profielen van Interpolbaas Noble, terwijl hij nooit een account heeft aangemaakt.

een zelfverklaarde fan zich via deze tactiek uit voor de Gentse burgemeester Daniël Termont. "Sommigen maken zo'n nepprofiel voor de grap, maar dikwijls hebben ze minder goede intenties. Het zijn trouwens niet alleen bekende koppen die geviserd worden. Ook van gewone mensen worden valse accounts aangemaakt, bijvoorbeeld om benaalde gege-

cent heeft nog e-mail als doel. Er is een duidelijke verschuiving naar *social media*", besluit Willems. Gisteren werd Twitter nog getroffen door een veiligheidslek. Ingelogde gebruikers die hun muis boven een berichtje bewogen, verstuurden ongewild nieuwe berichten. Sommigen kregen ook websites voor zich waar ze niet om gevraagd hadden.

palingen ontbreken. Wel wordt er in verschillende landen aan gewerkt, zeker in de VS is het een topprioriteit."

Niet verwijderbaar

Ook technisch wordt er naar bijkomende beschermingsmaatregelen gezocht. "Google is applicaties aan het uitwerken

g Data. 'En niet alleen bij accounts van bekende figuren.'

Hij is een van de belangrijkste figuren in de politiewereld, maar toch is ook Interpolbaas Ronald Noble recentelijk het slachtoffer geworden van identiteitsdiefstal op het internet. Criminelen plaatsten op Facebook twee profielen online onder zijn naam, terwijl de echte Ronald Noble nooit een account heeft aangemaakt. Een van de nabootsers probeerde meer te weten te komen over een recente operatie van Interpol naar voortvluchtigen die worden gezocht voor moord, pedofilie, drugs en witwaspraktijken.

Veiligheidslek

Interpol kwam de identiteitsdiefstal pas onlangs op het spoor. "Cybercriminaliteit is aan het uitgroeien tot een erg concrete bedreiging. Gezien de anonimiteit in cyberspace, kan het een van de gevaarlijkste criminele bedreigingen worden die we ooit al onder ogen hebben gezien", zei Noble vorige week op een conferentie van Interpol in Hongkong. "Het is een groeiend probleem", bevestigt Eddy Willems, expert in computerbeveiliging. "Het is ook zo gemakkelijk om een profiel in iemand anders naam aan te maken. Naam en foto ingeven en klaar is kees. Daarna sturen de nabootsers friend requests uit. De ontvangers herkennen de naam en foto en gaan bijna blindelings op het vriendschapsverzoek in."

In ons land gaf enkele weken geleden



■ **Criminelen plaatsten op Facebook twee profielen van Interpolbaas Noble, terwijl hij nooit een account heeft aangemaakt.**

een zelfverklaarde fan zich via deze tactiek uit voor de Gentse burgemeester Daniël Termont. "Sommigen maken zo'n nepprofiel voor de grap, maar dikwijls hebben ze minder goede intenties. Het zijn trouwens niet alleen bekende koppen die gevisieerd worden. Ook van gewone mensen worden valse accounts aangemaakt, bijvoorbeeld om bepaalde ge-

cent heeft nog e-mail als doel. Er is een duidelijke verschuiving naar *social media*", besluit Willems. Gisteren werd Twitter nog getroffen door een veiligheidslek. Ingelogde gebruikers die hun muis boven een berichtje bewogen, verstuurden ongewild nieuwe berichten. Sommigen kregen ook websites voor zich waar ze niet om gevraagd hadden.

ROBERT NOBLE (BAAS INTERPOL): Cybercriminaliteit kan door de anonimiteit op het internet uitgroeien tot een van de gevaarlijkste bedreigingen ooit

vens los te weken van het bedrijf waarvoor je werkt", vertelt Willems. Bovendien worden bestaande accounts op sociaal-netwerksites meer en meer binnenge-drongen. "Hackers schrijven specifieke malware en virussen waarmee ze met je logingegevens aan de haal gaan. Die kwaadaardige software wordt op het internet te koop aangeboden. Gaat het om een bekend of machtig iemand, dan drijft dat de prijs op."

Het voorbije jaar is het aantal malware gericht op sociale media met 7 procent gestegen. "Dat is enorm. Amper één pro-

Juridische stappen tegen cybercrime blijken niet eenvoudig. De hackers opereren dikwijls van buiten Europa. "Maar zelfs als de Belgische autoriteiten pakweg Yahoo om informatie vragen, kan het zijn dat het weigert die te geven omdat het een buitenlands bedrijf is", merkt professor Paul De Hert (VUB) op. "De bestaande wetgeving zegt ook niets over dit nieuwe type van misdrijven. Je kunt de wetgeving rond privacy invoeren en er is ook een arrest van het Europees Hof voor de Rechten van de Mens dat tegen cyber-crime beschermt, maar specifieke strafbe-

palingen ontbreken. Wel wordt er in verschillende landen aan gewerkt, zeker in de VS is het een topprioriteit."

Niet verwijderbaar

Ook technisch wordt er naar bijkomende beschermingsmaatregelen gezocht. "Google is applicaties aan het uitwerken waarbij je naast je wachtwoord ook een code moet ingeven die je per sms ontvangt", aldus Eddy Willems. Die code zou bij elke inlogbeurt veranderen. "Maar het is een kwestie van jaren alvorens er ook bij sociale media zulke technieken zullen komen."

Bijkomende hinderpaal is dat online-profielen ook voor de staatsveiligheid een veel gebruikte bron van informatie zijn. "Politiediensten staan niet te springen om het onderzoek naar open bronnen te beperken", beaamt De Hert. "Maar er moeten grenzen komen op publiek toegankelijke data. Momenteel kun je bijna niets meer verbergen dat ooit op het internet stond, zelfs al is het tien jaar geleden. Alle websites worden namelijk gearchiveerd. Er moet dringend een regeling komen dat wie dat wil, al zijn gegevens van Facebook of andere media definitief kan verwijderen."