TEKST: EDDY WILLEMS

Malware en cybercrime woekeren...

Eddy Willems is Security Evangelist en Analist bij Kaspersky Lab. Hij is bijna 2 decennia actief in de anti-malwarewereld en is ook bekend als Directeur Informatie en Pers van EICAR (European Institute for Computer Anti-Virus Research).

Het was koud. Snel trok ik deur achter mij dicht. 'De luchthaven' deelde ik de taxibestuurder mee en weg waren we. We praatten wat over koetjes en kalfjes tot mijn taxichauffeur een raar verhaal begon op te disselen over zijn ex-vrouw die hem zou bespioneren. Hij vertelde me dat zijn ex zowat alles wist over hem, van sms'jes tot namen van mensen die alleen hij kende. Ik vroeg hem naar zijn gsm. Hij liet mij zijn nieuwe iPhone zien. Reden genoeg om dit hebbeding eens aan een snelanalyse te onderwerpen. Raad es? Er was op zijn toestel commerciële spyware geïnstalleerd zonder dat hij het zelf wist. Zijn ex-vrouw kon makkelijk sms'jes en e-mails bekijken en zag perfect de gps-locatie van de man.

Dit verhaal toont o.a. aan hoe sommige individuen nogal los omspringen met ethiek en hoe onveilig je belangrijkste buddy - je gsm - eigenlijk is. En als we het dan toch over ethiek hebben. Onlangs liet een Nederlands magazine op verzoek een bot maken door een zogenaamde 'beveiligingsexpert' die een 'brute-force attack' lanceerde naar de e-mailbox van een bekende Nederlander via het sociale netwerk 'Hyves'. Blijkbaar kent niemand vandaag nog grenzen...

We zijn het er met een aantal specialisten over eens dat geen grenzen kunnen stellen mogelijk één van de psychologische aspecten is die meespelen bij de cybercrime. Cybercrime gedreven door makkelijk geldgewin, de werkelijke drijfveer, viert hoogtij. Verleden jaar zei ik nog dat je ongeveer 20 seconden veilig bent op het internet. Nu moet ik mijn uitspraak herzien, het is nog maar één seconde. Cijfers uit ons lab geven weer dat we van meer dan 2 miljoen malware, virussen en trojans naar iets minder dan 20 miljoen zijn geklommen in ongeveer 1 jaar tijd. Een voorspelling die we begin verleden jaar gedaan hebben en die nu ook bewaarheid is. Ik durf mij vandaag gewoonweg niet meer te wagen aan dat soort berekeningen maar het is een feit dat malware met bakken binnenstroomt. Vandaar dat vele vendors genoodzaakt zijn om het over een andere boeg te gooien. Het buzzword 'in-the-cloud' preventie duikt dan ook her en der op. Persoonlijk noem ik dit 'logische evolutie' en is het normaal dat er inderdaad bredere middelen worden ingezet om deze malware en cybercrime-stroom een halt toe re roepen. Cybercrime organiseert zich steeds beter en wordt steeds professioneler en dat levert dan ook deze groei op. De economische crisis draagt hier zelfs een steentje aan bij en werkt cybercrime nog in de hand. Trouwens hoe meer data er online wordt vastgelegd hoe gevaarlijker het risico. Natuurlijk kan informatisering helpen bij het efficiënt en effectief omgaan met informatie, maar door meer en meer data te koppelen lopen we wel een steeds groter risico dat deze gegevens in verkeerde handen vallen.

Is er dan geen verbetering merkbaar? Wel laat ons veeleer zeggen dat de infectievectoren verschuiven. Een prachtig voorbeeld is de vermindering van malwareverspreiding via mail. De malware-aanvallen verplaatsen zich meer naar Web 2.0 sites of omgevingen. Een prachtig voorbeeld zijn de wormen of stukjes botnets die soms verscholen kunnen zitten in de grote sociale netwerksites zoals Facebook. En zit niet half België op Facebook dezer dagen? Sommigen kunnen amper met de computer werken maar hangen wel een hele dag rond op Facebook. En je vertrouwt toch iedereen en alles op dergelijke sites, niet?

Op technologisch vlak denk ik dat we de volgende maanden meer interessante en vernieuwende securitytechnieken zullen zien. Na de 'in-the-cloud' technologiëen moeten we eens kijken of we security ook niet eens anders kunnen bekijken. Een voorgerecht van encryptie en firewall-opportuniteiten, een hoofdgerecht waarbij vernieuwende virtualisatie hand in hand gaat met proactieve en heuristische technieken en waarbij whitelisting om de hoek komt kijken opgediend met een IPS-sausje erbovenop, daarna duidelijk afgewerkt met een dessert van DLP en Vulnerability Checking en Remediation. Alhoewel ik een hele grote wijnliefhebber ben, laat ik dit magische, dorstlessende geschenk voorlopig eventjes aan jullie eigen verbeelding over zodat iedereen ook zijn eigen geliefkoosde wijn(vendorspecialiteit) kan inschenken.

Op malwarevlak gaat het dus van kwaad naar erger de volgende maanden: meer ingewikkelde en grotere botnets, meer Web 2.0 gebaseerde malware dus ook meer sociale netwerksites die problemen zullen hebben, meer Mac-gerelateerde malwareproblemen, de mogelijke doorbraak van de gsm-malware, meer zero-day attacks allemaal gelinkt aan het verschijnsel cybercriminaliteit. Persoonlijk pleit ik verder voor een internationale samenwerking van de vendors met de politiediensten en overheidsorganisaties. De eerste stappen richting internationale samenwerking zijn inmiddels gezet. Zo wil de Europese Unie online gaan patrouilleren. Een mooie gedachte maar niet zo evident om uit te voeren zeker omdat het een zeer lastig internationaal scenario zou kunnen gaan worden.

"Ik duwde de deur van de taxi met een schokkende beweging dicht. De spyware had ik van zijn toestel gehaald. Hopelijk had ik met mijn goede bedoelingen niet te erg ingegrepen in zijn dagelijks leven of dat van zijn ex. En nu op naar het vliegtuig dat mij terugbracht naar mijn gezin, mijn werk en.. de malware."¶