HETE SPAM EN MALWARE

Actuele trends onder cybercriminelen

Een nieuwe CBM, een nieuwe blik op actuele onderwerpen in IT security. En wat is er actueler dan de actualiteiten? Deze maand bieden wij een kijkje in de actuele trends van cybercrime, uitgesplitst in twee categorieën: spam en malware.

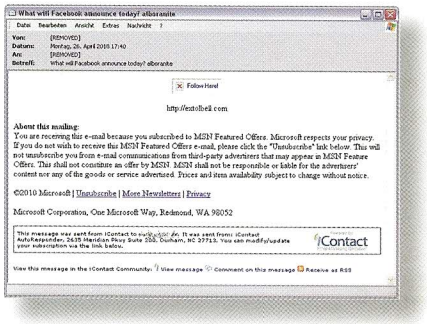
De internationale media werden de afgelopen periode gedomineerd door één onderwerp, dat ondanks de omvangrijke aandacht slechts door een enkeling goed kan worden uitgesproken: de Eyjafjallajoekull. De IJslandse vulkaan werd online besproken en niet alleen door goedwillende surfers. Het bleek één van de nieuwste tactieken van spammers om aandacht voor hun berichten te krijgen. Ongeveer 3 miljoen spamberichten over vulkaanas circuleerden over het net. En met vulkaanspam werd een nieuwe trend gezet: nieuwsspam.

Er werden in april en mei verschillende onderwerpen geïdentificeerd, die door aan louche online apotheken gerelateerde spamverstuurders werden ingezet om spamfilters te omzeilen en de aandacht van ontvangers te trekken. De spammails leken afkomstig te zijn van Russische e-mailadressen en deden zich voor als nieuwsbrieven van MSN.

Screenshot: Spambericht met actueel onderwerp

Analyse van G Data's SecurityLab wees uit dat er vier bedrijven achter de registratie van de betreffende domeinen zaten:

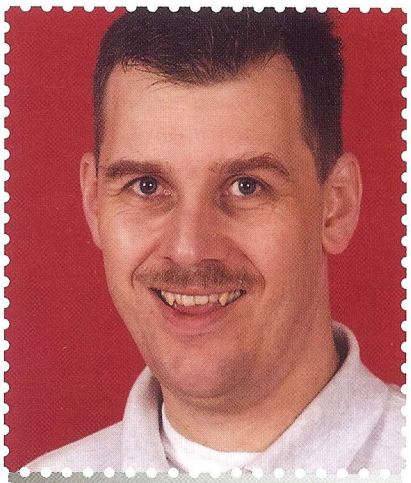
- China Springplank Inc (China)
- BIZCN.COM, INC (China)
- PEKING INNOVATIEVE LINKAGE Technology Ltd (China)
- 35 Technology Co, Ltd (China)



Deze bedrijven registreerden de volgende domeinen:

- oftenpush.com
- usuallife.com
- extolbell.com
- peopleeasy.com
- flairfew.com
- sugarspoke.com
- themreply.com
- seemlychief.com
- givingvery.com
- allownine.com
- quartwin.com
- maxistood.com

De meer dan 900 geanalyseerde onderwerpen hadden 825 unieke laatste woorden, alle beginnend met "a" (voorbeelden cursief aangegeven in de lijst hieronder). Het gebruik van lexicale woorden aan het einde van een normaal onderwerpregel is een maatregel van scammers om te proberen spamfilters te omzeilen.



Righard J. Zwienenberg is in 1988 begonnen met virusbestrijding toen hij tegen zijn eerste virus problemen aanliep op de Technische Universiteit Delft. Zwienenberg bestudeert sindsdien het gedrag van virussen en maakt hier oplossingen voor. In 1998 stapte Zwienenberg over naar het Norman Development team. In 2005 werd Zwienenberg Chief Research Officer bij Norman. Momenteel houdt hij zich bezig met gedragsanalyse van malware en In-The-Cloud problemen.

Eigentijdse malware

Malware lijkt voorlopig nog niet uit de mode te raken bij criminelen. De verspreiding van schadelijke codes is in april wederom gestegen. Analyse van G Data's SecurityLab toont aan dat cybercriminelen beveiligingslekken in PDF-programma's echt 'hot' vinden: in april was "JS:Pdfka-OE" de absolute nummer één in de malware top 10. De hoogste

nieuwe binnenkomer van de maand was "Win32:Rodecap" [Trj], een trojaans paard dat speciaal ontworpen is om e-mail-diensten als Yahoo, Hotmail en Google Mail aan te vallen.
Het misbruiken van zwakheden in programma's is een succesvolle manier om computers met malware te infecteren. Hoe meer een bepaalde applicatie gebruikt wordt, des te interessanter wordt het voor malware-schrijvers om de beveiligingslekken ervan uit te baten.
Een ander gevaar dat vaak onderschat wordt, is de Autorun-functie. Er bestaat een heel arsenaal aan malware dat deze functie misbruikt. Een voorbeeld is Worm.Autorun.VHG. Deze veelvoorkomende malware gebruikt Autorun om zichzelf te verspreiden via USB-sticks of externe harde schijven. Wie de Autorun-functie niet echt nodig heeft, kan de functie het beste uitschakelen.
PDF-documenten gelden normaal gesproken als onschadelijke bestanden, dus op bijna alle computers wordt wel een PDF-reader geïnstalleerd. Echter, de JavaScript-functie maakt van een PDF een potentieel gevaarlijk formaat: een Acrobat JavaScript, dat in een PDF verwerkt zit, wordt misbruikt en ingezet om aanvallen voor te bereiden. Ook kan de JavaScript zelf fouten bevatten, die door aanvallers worden benut om gevaarlijke code naar binnen te loodsen. Indien mogelijk, is het beter om de JavaScript-functie van de PDF-reader uit te schakelen. Een andere belangrijke maatregel is het goed up-to-date houden van de reader met nieuwe updates, om zo lekken te dichten en beschermd te zijn tegen nieuwe malware aanvallen.

Actuele trends zonder cyber-criminelen

Maar zelfs als we de (actieve) cybercriminelen weglaten, dan nog blijven er genoeg aktuele trends over waar we ons zorgen over moeten maken. Het gebruik van draadloze netwerken voor toegang tot internet wordt steeds populaireder. Tegenwoordig kan je overal het internet op met behulp van een draadloos netwerk.Waar het al gemeengoed was bij hotels, ontspruiten de WiFi hotspots zich overal, bij restaurants, benzine-stations, etc. En waar een mogelijkheid is tot het verzamelen van (niet versleutelde) informatie, daar vind je dan ook cybercriminelen. Maar recentelijk was er een onthullig over het grootschalig verzamelen van niet versleutelde gegevens, niet door cybercriminelen, maar door Google.
Op 27 April 2010 beschrijft Google op haar European Public Policy Blog wat voor informatie de Google Street View auto's allemaal verzamelen terwijl ze rond rijden om de straten te fotograferen: "... We verzamelen de vokgende gegevens – foto's, lokale WiFi netwerk gegevens en 3-D foto's van gebouwen. (...) Google verzamelt en bewaart geen informatie welke wordt verstuurd van een computer naar een andere via een WiFi netwerk."
De Duitse instantie die waakt over de privacy van gegevens heeft op 5 Mei 2010 een audit gevraagd over de data die de Google Street View auto's verzamelen. Binnen Google leidde dit tot een nadere beschouwing over wat werd

Hier volgen enkele voorbeelden van de actualiteiten van de afgelopen weken die in spamberichten voorkwamen:

- 200,000 flood Shanghai Expo preview acoustics
- Air travel updates amid volcanic ash addibility
- Alain Robert: Living on the edge adamances
- Apple posts record quarter accordingly
- AT&T unveils Buzz.com aerobatics
- Cairo reporter on the city's best actifier
- China pays tribute to quake victims acarpous
- China under growing currency pressure alamos
- Chrysler in $143M profit aitch
- Conservatives unveil manifesto acnodes
- Country profile: Georgia aglets

verzameld en het bleek dat Google weldegelijk informatie verzonden over het draadloze netwerk werd verzameld en bewaard. Dit wordt ook bevestigd in een blog van Alan Eustace, Google's Senior VP, Engineering & Research, waarin hij aangeeft wat de redenen waren om deze gegevens te verzamelen en te bewaren: "... Enkele oude programma routines waren per ongeluk niet verwijderd uit de software die gebruikt wordt in de Street View auto's".
De gegevens zijn niet gebruikt en Google zou zo snel mogelijk deze gegevens verwijderen uit haar databases.
Als gevolg van deze verklaring heeft de Ierse instantie die waakt over de privacy van gegevens Google op 16 Mei gevraagd om alle gegevens die verzonden zijn over draadloze netwerken die binnen Ierland zijn verzameld te verwijderen. Google heeft hiermee ingestemd en de gegevens zijn verwijderd onder toezicht van een onafhankelijke waarnemer, iSec Partnerc Inc. Verder heeft Google als gebaar naar andere nationale privacy instanties, een bericht uitgestuurd hoe Google de gegevens zo spoedig mogelijk zal verwijderen. In de beveiligingsoindustrie alsmeded in de media wordt echter hevig gespeculeerd hoe lang Google al bezig is geweest met het verzamelen en bewaren van gegevens, en hoe groot de de hoeveelheid gegevens is. Hier is het laatste woord nog niet over gesproken. Toch kunnen we uit dit verhaal een goede les leren. Alle informatie die Google verzamelde en bewaarde, werd verstuurd over niet beveiligde draadloze access points. Het blijkt dus maar weer eens dat het belangrijk blijft om te herhalen:
Je weet nooit wie de informatie monitoort, met opzet door cybercriminelen of per ongeluk zoals met de Google Street View auto's. Het ongemak voor het gebruiken van beveilgde access points is te verwaarlozen ten opzichte van het risico dat vertrouwlijke informatie in de verkeerde handen komt.

Malware in April 2010

	Name	Percentage	Trend*
1	JS:Pdfka-OE [Expl]	11,4 %	↔
2	Win32:Rodecap [Trj]	1,7 %	new
3	Worm.Autorun.VHG	1,7 %	↘
4	WMA:Wimad [Drp]	1,3 %	↘
5	Saturday 14th-669	1,2 %	↘
6	HTML:Iframe-inf	1,0 %	↘
7	Trojan.PWS.Kates.Z	1,0 %	new
8	Trojan.Boaxxe.X	0,8 %	new
9	Win32.Sality.OG	0,6 %	↑
10	Win32:Crypt-GBX [Trj]	0,6 %	new

* The trend shows change in position in comparison to the previous month.
↑ > 2 ↗ + 1 oder 2 ↔ ± 0 ↘ - 1 oder 2 ↓ - > 2

Beveilig uw draadloze access point

Zowel thuisgebruikers als organisaties doen er goed aan om hun access points te beveiligen, het liefts met de sterkste beveiliging die mogelijk is op het access point (WPA2) Alhoewel het verleidelijk is om een open access point te instaleren zodat bezoekers, vrienden en/of kennissen gemakkelijk gebruik kunnen maken van het internet, verhoogd dit het risico van de zogenaamde "Data Leakage", het lekken van (vertrouwelijke) informatie. Bovendien zal de eigenaar van het niet beveiligde access point ook benaderd worden indien dit access point wordt misbruikt voor allerlei andere doeleinden (spam, verspreiden kinderporno, ed).
Als we toch een positief punt moeten pakken uit dit hele gebeuren met Google, dan is het wel de media aandacht. Het toont in ieder geval aan dat iedereen nogal is gesteld op zijn privacy en dat iedereen maar weer eens met de neus op de feiten is gedrukt dat het lekken van gegevens zelf voorkomt zonder dat er opzet in het spel is.

Groeten,
Eddy Willems en Righard Zwienenberg

De Belgische **Eddy Willems** is al twee decennia actief op het gebied van IT security. In die tijd heeft hij gewerkt voor invloedrijke instituten, zoals EICAR (waarvan hij medeoprichter is), verschillende CERT-instellingen en de organisatie achter de Wildlist, als ook bij commerciële ondernemingen. Bij GData vormt Willems als Security Evangelist de link tussen de technische complexiteit van IT security en de gebruiker. Hij is verantwoordelijk voor een heldere communicatie van het G Data SecurityLab naar de security community, pers, distributeurs, resellers en eindgebruikers.