FBI / CIA worm virus: Sober Y

December 2005

Henk Jongedijk, maandag 23 oktober 2006 - 00:00:00

De worm komt binnen als een mailtje dat afkomstig lijkt van de FBI. Het virusmailtje heeft bijvoorbeeld als afzender department@fbi.gov, mail@cia.gov, post@fbi.gov of admin@fbi.gov. Onderwerpen van het bericht zijn bijvoorbeeld: "Your IP was logged" of "You_visit_illegal_websites". De grootte van het mailbericht is rond de 75.6kB. Uiteraard komen deze mailtjes niet van de FBI of van de CIA: de bijlage bevat het Sober.Y virus. De mailtjes zijn meestal in het Engels (de FBI en CIA varianten), maar kunnen ook in het Duits opgesteld zijn. In dat geval zou het gaan om een waarschuwing van de Duitse Bundeskriminalamt (BKA).

Het bericht is telkens anders en variabel, maar de volgende tekst wordt vaak gesignaleerd: ?We have logged your ip-address on more than 30 illegal Websites. Important: Please answer your questions! The list of questions are attached?. Wie echter de bijlage opent, wordt het slachtoffer van de worm.

Als het virus actief wordt, gaat het op de harde schijf op zoek naar e-mailadressen waarnaar het zichzelf kan doorsturen. Ook antivirusbedrijven waarschuwen massaal voor deze worm die diverse namen heeft gekregen als Sober.Z, Sober.Y, Sober.W en Sober.X. Bij de Common Malware Enumeration, een onlangs opgericht industrieplatform dat virusvarianten een nummer geeft, is het virus bekend als nummer 681.

Volgens antivirussoftwaremaker F-Secure is deze Sober-variant de grootste virusuitbraak van dit jaar. Ook andere antivirusbedrijven signaleren grote hoeveelheden virusmailtjes. F-Secure heeft het over 'enkele miljoenen in de afgelopen uren'. Het Nederlandse Cleanport zegt dat deze Sober-worm in twaalf uur tijd is gegroeid tot 40 procent van het totale e-mailverkeer. Het simpelweg updaten van je antivirussoftware heeft volgens het Sans Institute niet zo veel zin. "Antivirussoftwarebedrijven bieden geen betrouwbare oplossing tegen de huidige bedreigingen. Virussen als Sober veranderen namelijk om de paar uur en blijven zo de antivirusupdates een stap voor."

Sober.Y is actief zodra Windows start en is terug te vinden in de Windows map, waar een nieuwe map 'WinSecurity' wordt aangemaakt. De worm probeert processen van een aantal veiligheidsproducten te stoppen: wanneer dat succesvol is, laat de worm een bericht-venster zien. Ook kan Sober.Y bestanden downloaden en uitvoeren en z'n activiteiten synchroniseren middels tijdservers. Gebruikers die de e-mail hebben ontvangen kunnen een klacht indienen bij Internet Crime Complaint Center (http://www.ic3.gov/).

De beste remedie is en blijft: open de bijlagen van onbekenden nooit!

Bronnen:

http://www.webwereld.nl/articles/38472
http://cme.mitre.org/data/list.html#681
http://isc.sans.org/diary.php?storyid=880
http://www.fbi.gov/pressrel/pressrel05/emailscheme112105.htm
http://www.f-secure.com/v-descs/sober_y.shtml
http://www.planet.nl/planet/show/id=74253/contentid=657057/sc=33d3ce
http://www.zibb.nl/ict/nieuwsbericht/asp/artnr/1070171/versie/1/
http://www.sophos.com/pressoffice/news/articles/2005/11/toptennov05.html
http://www.sophos.com/virusinfo/analyses/w32soberz.html
http://www.kaspersky.com/virusscanner
http://housecall.trendmicro.com/
http://www.pine.nl/virusstats.php
http://infosecurity.array.nl/site/jsp/nieuws.jsp?art_iID=2995

http://www.virusalert.nl/?show=virus&id=1249&name=W32.Sober.x@mm