Name of Publication: Dubai Photo Media, the Dubai-based leading regional news portal (English & Arabic)
Date of Publication: 16/6/2004
Page(s) in Publication:

DPM News Agency Distribution of Press Release

Zafi.B يستطيع تعطيل برامج مكافحة الفيروسات

2004/16/6

الفيروس الجديد ينتشر بسرعة مذهلة.. وبلغات متعددة

حذرت شركة التكنولوجيات الألمانية المتطورة AGT أبرز الشركات في ألمانيا وأوروبا التي تركز على توفير حلول تأمين شبكات المعلومات والاتصالات لمنطقة الخليج والشرق الأوسط وشركة F-Secure لتأمين الشبكات ومكافحة الفيروسات الإلكترونية، مستخدمي الكمبيوتر في المنطقة من نوع جديد متغير من الفيروس الإلكتروني زافي، وهو "زافي. بي" Zafi.B الذي يتسلل عبر البريد الإلكتروني والذي تم رصده في حالة نشطة يوم الجمعة 11 يونيو الجاري.

وكانت الشركة قد رفعت درجة التأهب للرصد والمتابعة إلى المستوي 2 اعتبارا من الأحد 13 يونيو الماضي، وذلك في ضوء سرعة انتشار هذا الفيروس.

ويمكن لهذا الفيروس أن ينتشر عبر البريد الإلكتروني من خلال الملحقات المتغيرة COM- EXE- PIF.- . كما أن الفيروس يرسل الرسائل بعدة لغات مختلفة مثل الإنجليزية، الفرنسية، الروسية، الإسبانية، السويدية، الألمانية، الفنلندية، الإيطالية.. الخ.

ومثل أي فيروس عادي آخر فإن Zafi.B يجمع العناوين من حافظات عناوين المستخدمين ثم ينتشر عن طريق إرسال نفسه لتلك العناوين.

وعندما ينشط الفيروس فإنه ينسخ نفسه عدة مرات على كل أنظمة تشغيل "ويندوز" سواء في شكل DLL أوEXE. ، بعد ذلك يقوم الفيروس بعمل مسح عبر كل الملفات المخزنة في النظام ويعيد تشكيلها على هيئة الملفات الخاصة بتخزين برنامج Winamp 7.0 أو برنامج Total Commander 7.0 بالنسبة لكل ملفات الحفظ المحتوية على كلمتي المشاركة أو التحميل في اسمها. وبالإضافة إلى هذا فإن الفيروس الجديد يعطل وينهي كل التطبيقات المحمية بنظام مكافحة الفيروسات داخل ملفاتها.

وتسعي شركة AGT عبر الشراكة الاستراتيجية مع شركة F-Secure إلي توفير أحدث تكنولوجيات

Preparation of Press Rel e

Zafi.B worm can terminate antivirus programs

6/16/2004

Advanced German Technology, AGT, a leading supplier of premier security products, solutions and services, focusing on the Middle East and F-Secure Corporation, the leading provider of centrally managed security solutions for the mobile enterprise, are warning computer users in the region of a new variant of the Zafi email worm - Zafi.B - that was found in the wild on Friday, June 11th.
Due to the worm's rapid speed of spread, it was raised to Radar level 2 alert on Sunday, june 13th. The worm spreads by email in variable PIF.-, .EXE-, or COM -attachments. It also sends the messages in several different languages; e.g. in English, Italian, Spanish, Russian, Swedish, German or Finnish.

Like a typical email worm, Zafi.B also gathers addresses from the users address books and then spreads by sending itself to those addresses. When the worm activates, it copies itself to the Windows System Directory with a random .DLL and random .EXE name. After this the worm scans through all directories in the system and replicates as either 'winamp 7.0 full_install.exe' or 'Total Commander 7.0 full_install.exe' to all folders that contain 'share' or 'upload' in their name. In addition to this, it terminates all applications that have 'firewall' or 'virus' in their filename.

In a strategic partnership with F-Secure, for the Middle East, AGT focuses on providing Arab organizations with F-Secure's award-winning security solutions, including antivirus, desktop firewall with intrusion prevention and network encryption.