Polipos

معلومات عامة:

حذر قسم خدمة مراقبة الفيروسات من شركة Doctor Web, Ltd مستخدمي الاتصال الشخصي عبر الشبكة (peer to peer) من خطر الفايروس متعدد الأشكال Polipos32Win. الذي ظهر منذ حوالي شهر مضى وانتشر بشكل فعال في ملفات مختلفة عن طريق الشبكة. بدأ انتشار Polipos32Win. في آذار الماضي. وتمت إضافته لقائمة فيروسات Doctor Web, Ltd في 20 آذار 2006 ومن ذلك الوقت لم يعد هناك خطر على مستخدمي Dr.Web Anti-virus.

آلية العمل والاثار:

وبصرف النظر عن التكنولوجيا المعقدة المستخدمة من قبل صانعي الفيروس، فإن هذا الفيروس يحمل مميزات خطرة أخرى تقوم على تحييد عمل برامج مكافحة الفيروسات وبرامج الحماية الأخرى.
الفيروس يعطب الملفات التنفيذية لنظام الويندوز عبر كتابة الكود الخاص به في مساحة غير مستخدمة من قطاعات الترميز code sections وعند ذلك ينشئ الفيروس قطاعاً جديداً ويضع شيفرته فيه مغيراً بذلك قطاع الموارد section resource وعندما يزرع الفيروس في ملف ما، يغير نقطة البدء ويغير عناوين الطلبات، باختيار عشوائي يتم مع بدء انطلاقة الفيروس.
وعندما ينطلق الفيروس يزرع شيفرته في كل العمليات الفعالة باستثناء التالي: dwwin, drwtsn dumprep, 32savedump, kernel, dll32drwatson. temp ctfmon, spoolsv, csrss, smss
وبالتالي نسخ متعددة من الفيروس ستبقى في ذاكرة الكومبيوتر وكل منها مسؤول عن نشاط محدد. على سبيل المثال البحث عن الملفات لنشر العدوى، نشر العدوى في الملفات، التفاعل مع الاتصالات الشخصية عبر الانترنت...إلخ وعدوى الملفات تصبح مفتوحة أمام الأعضاء في هذه الشبكة.
النسخ الحالية من فيروس Polipos32Win. تعترض تطبيقات الـ (API functions) CreateProcessW, CreateProcessW, CreateFileW, LoadLibraryExW, SearchPathW, CreateFileW, LoadLibraryExW, SearchPathW.
وعندما تطلب أي من هذه الوظائف يتم تعطيل عدد جديد من الملفات، وعندما يتم التحكم بالملف الضحية يحاول الفيروس خلق نسخة أصلية من الملف في المسار المؤقت باسم: ptf*.tmp وتشغيلها. يفعل هذا للتهرب من الفحص الذي يمكن أن يقوم به من يقوم بالتنصيب.
الشك من انتشار فيروسات مماثلة يسبب الكثير من القلق لمستخدمي الاتصال الشخصي عبر الشبكة. ومن الغريب أن حضور هذا الفيروس في الشبكات لم يكن سرياً عن أي شخص طيلة الشهر الماضي. وبرنامج دكتور ويب لمكافحة الفيروسات هو البرنامج الوحيد الذي اكتشفه. في بداية انتشار الوباء استقبل قسم الدعم الفني في Doctor Web, Ltd. انذارات خاطئة من المستخدمين لكن محللي الشركة أثبتوا وجود فيروس جديد... وبرنامج دكتور ويب لمكافحة الفيروسات اكتشف بنجاح تعديلات مختلفة من هذا الفيروس متعدد الاشكال، بالاعتماد على التكنولوجيا رفيعة المستوى المستخدمة من قبل الدكتور ويب.

الحماية والدفاع:

حالياً، صممت خدمة مراقبة ورصد الفيروسات في Doctor Web, Ltd إجراءاً علاجياً للملفات المصابة بفيروس Polipos32Win.. وهذا الاجراء مخصص لمستخدمي برامج مكافحة الفيروسات التي لم تستطع أن ترصد هذا الفيروس حتى الآن. ولمستخدمي برامج مكافحة الفيروسات التي لم تمنع أجهزة الكومبيوتر المصابة من نقل العدوى إلى أجهزة كومبيوتر أخرى...
تقنية الاصلاح أو العلاج هي الأخرى تقنية معقدة وفك شفرة الفيروس يمكن أن تستغرق زمناً طويلاً.
وللحماية من الاصابة بهذا الفيروس فكغيره من الفيروسات نستطيح الحماية باستخدام فايروول مناسب وقوي وكذلك نستخدم برامج الكشف عن الفيروسات للكشف عنه.