ITRC
مرکز تحقیقات مخابرات ایران

دانشگاه شیراز

مرکز تخصصی آپا درزمینه اختلالات امنیتی مرتبط با بد افزارها

cert@shirazu.ac.ir

بدافزار TROJ_QUICKTM.A

تنظیم کننده:

سمانه غنی- سعیده نکوخیز

ویرایش: ۱

شماره سند: V-89/5-4

www.ircert.cc

ITRC

مرکز تحقیقات مخابرات ایران

دانشگاه شیراز

کد آسیب پذیری: V-89/5-4

نام محصول آسیب پذیر: بدافزار TROJ_QUICKTM.A

نوع سیستم عامل: Windows 98, ME, NT, 2000, XP, Server 2003

کشف توسط:شرکت Trendmicro

تاریخ و زمان کشف: 30 July 2010 و زمان 5:20:44 PM

سطح خطر: زیـا د

شرح:

این بدافزار با استفاده از روش های مهندسی اجتماعی، ممکن است کاربران را با انجام اقدامات خاص به طور مستقیم یا غیر مستقیم فریب دهد و باعث ایجاد روال مخرب گردد. این بدافزار می تواند با استفاده از فایل ویدیویی خاص، منجر به دریافت سایر فایل های مخرب گردد.

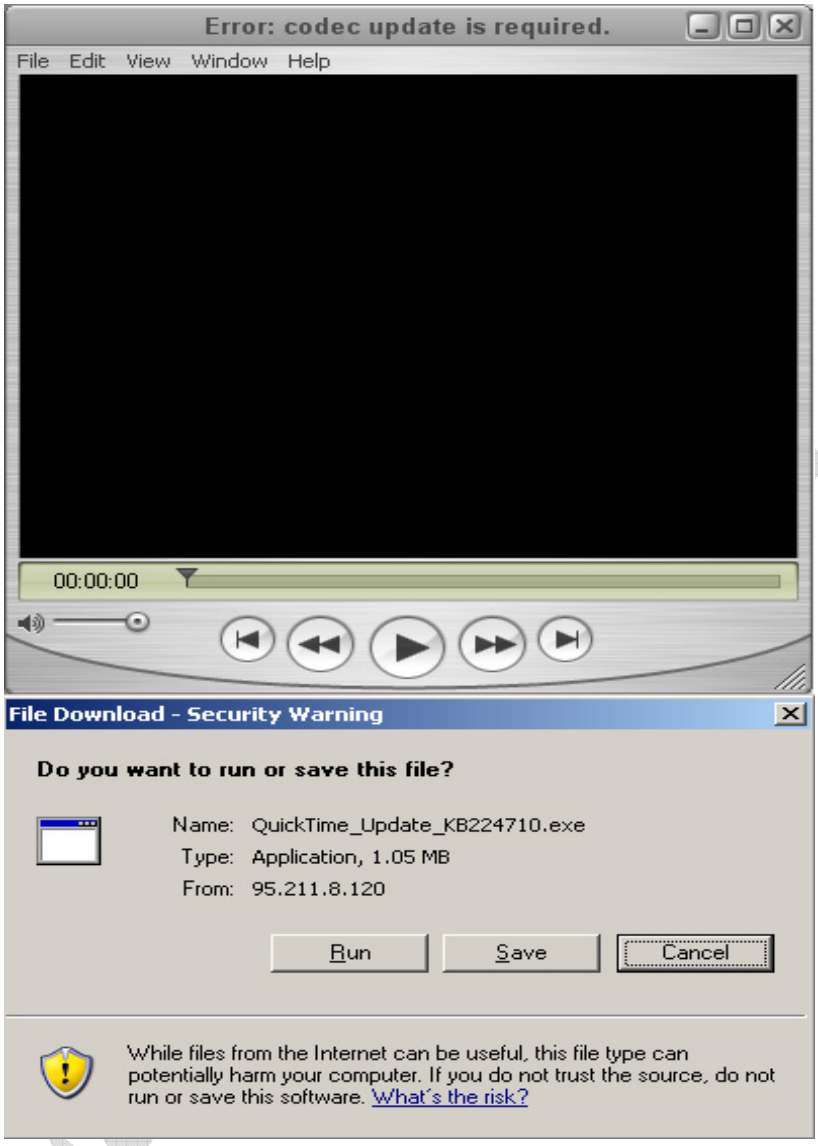
این تروجان ممکن است به طور ناخواسته توسط کاربر هنگام بازدید از سایت های مخرب دریافت گردد.

نمونه شناخته شده ای از بازدید های ناخواسته کاربر مطابق اقدامات زیر می باشد:

۱) هدایت کاربر به سایت http://{BLOCKED}y.{BLOCKED}staller.com/0.c

سپس در این قسمت کاربر منتظر می ماند تا فایل هایی را که شرکت ترند مایکرو به عنوان TROJ_DLOAD.QWK شناسایی کرده است دریافت و اجرا نماید.

۲) هنگام پخش فایل های ویدیویی یک پیغام خطا مبنی بر دریافت نسخه بروز رسانی شده Quicktime player به کاربر نمایش داده می شود.



نحوه رفع مشکل:

کاربران Windows ME و Windows XP می بایست قبل از انجام هر عمل اسکن اطمینان حاصل کنند که برنامه System Restore در کامپیوتر شان غیرفعال است و اجازه اسکن تمام قسمت های کامپیوتر را به آنها می دهد.

مرحله اول: حذف فایل های مخرب مرتبط با بدافزار TROJ_QUICKTM.A:

- TROJ_TRACUR.SMDI
- TROJ_DLOAD.QWK

مرحله دوم: کامپیوتر خود را با برنامه های ضد بدافزار شرکت ترندمایکرو اسکن نمایید و فایل های مخرب شناسایی شده به عنوان بدافزارTROJ_QUICKTM.A را از سیستم کامپیوتر خود حذف نمایید.

مرکز آپای دانشگاه شیراز

منابع:

http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ%5FQUICKTM%2EA&VSect=P

http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ%5FQUICKTM%2EA&VSect=Sn

http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ%5FQUICKTM%2EA&VSect=T

مرکز آپای دانشگاه شیراز