سرقت اطلاعات حساب کاربران و انجام تقلب‌های بانکی توسط بدافزار جدید Kronos

معرفی بدافزار

Kronos بدافزار بانکی جدیدی است که اخیراً در انجمن‌های گفت‌وگوی زیر زمینی برای فروش عرضه شده و آمار آلودگی قابل توجهی نیز از خود نشان داده است. این بدافزار از مکانیزم‌هایی برای سرقت اطلاعات حساب کاربران و انجام تقلب‌های بانکی استفاده می‌کند که شباهت زیادی با بدافزارهای مشابه مانند Zeus و Citadel دارد.

شیوه‌ی برنامه‌نویسی این بدافزار و نیز ویژگی‌های افزوده شده به آن سبب شده است که بسیاری از کارشناسان این بدافزار را ساخته تیم توسعه‌دهنده‌ی اولیه Zeus بدانند. به عبارت دیگر این بدافزار در واقع اولین وارث رسمی از بدافزار بانکی مشهور Zeus به شمار می‌رود.

شناسایی سیستم آلوده از طریق لاگ‌های شبکه

تمامی سیستم‌هایی که نام دامنه bitcoind.su را Resolve کرده باشند، آلوده هستند.

بررسی وجود آلودگی

وجود کلید زیر در رجیستری سیستم نشان آلودگی خواهد بود:

HKEY _ CURRENT _ USER\Software\ Microsoft\Windows\CurrentVersion\Run\"userinit"="
%UserProfie%\Application Data\sdra64.exe"

همچنین وجود فایلی با نام sdra64.exe در مسیر %userprofile%\Application Data می‌تواند نشانی از آلودگی سیستم باشد.

نحوه پاک‌سازی سیستم

کلید زیر بایستی از رجیستری ویندوز حذف گردد:

Microsoft\Windows\CurrentVersion\Run\"userinit"=" HKEY _ CURRENT _ USER\Software\ sdra64.exe" %UserProfie%\Application Data\

همچنین در صورتی که فایلی با نام sdra64.exe در مسیر %userprofile%\Application Data وجود داشته باشد، بایستی از روی سیستم حذف گردد.

بررسی پاک بودن سیستم

نبود کلید زیر در رجیستری ویندوز:

Microsoft\Windows\CurrentVersion\Run\"userinit"=" HKEY _ CURRENT _ USER\Software\ sdra64.exe" %UserProfie%\Application Data\

همچنین نبود فایلی با نام sdra4.exe در مسیر %user profile%\Application Data و نبود ارتباط با نام دامنه bitcoind.su

توصیه‌های امنیتی برای پیشگیری

۱. خودداری از باز نمودن هرزنامه‌ها و ایمیل‌های مشکوک
۲. خودداری از بازدید از وب‌سایت‌های ناشناس
۳. استفاده از افزونه‌های بلاک کردن تبلیغات بر روی مرورگر مانند افزوده AdBlock
۴. خودداری از کلیک بر روی لینک‌های ناشناس
۵. خودداری از اتصال Flash Drive های ناشناس به سیستم
۶. خودداری از بازدید از سایت‌های FTP ناشناس و نامطمئن
۷. به روز رسانی Adobe Flash، مرورگر، افزونه‌های مرورگر، سیستم عامل و ...