سه شنبه 02 اسفند 1390 - 08:15

زورگیري به سبک دیجیتال

در قرن 21 به سر می‌بریم و دنیا روزبه‌روز پیشرفت می‌کند. همگام با این پیشرفت‌ها مزاحمت‌ها و زورگیری‌های قدیمی نیز منسوخ شده و روش‌های مدرن جایشان را می‌گیرد.

جام جم آنلاین: در قرن 21 به سر می‌بریم و دنیا روزبه‌روز پیشرفت می‌کند. همگام با این پیشرفت‌ها مزاحمت‌ها و زورگیری‌های قدیمی نیز منسوخ شده و روش‌های مدرن جایشان را می‌گیرد.
امروزه شاید بتوانیم طی روز و در اماکنی که پلیس حضور دارد به‌طور کامل از شر اراذل و اوباش خیابانی در امان باشیم اما با گسترش فناوری و نبوغ بسیار زیاد برخی از این اراذل و اوباش در محیط‌هایی همچون اینترنت، نمی‌توان از دست آنها در امان بود! همگی شما با ویروس‌ها و پیامدهای مخرب آنها آشنا هستید! اما تعداد کمی از کاربران با بدافزارهایی تحت عنوان ransomware آشنایی دارند و به آنها آلوده شده‌اند!

این بدافزارها که می‌توانیم آنها را اراذل و اوباش دیجیتال یا باجگیرهایی به سبک امروزی معرفی کنیم، پس از آلوده کردن رایانه شما اطلاعاتتان را قفل کرده و برای برداشتن این قفل از شما پول زور طلب می‌کنند! در چنین شرایطی که ان‌شاءالله نصیب هیچ کاربری نشود، همانند بسیاری از فیلم‌های پلیسی، راه‌حل‌های ممکن برای پسگیری اطلاعات از چنگال این گروگانگیرهای پنهان و ناشناس، پرداخت پول درخواستی یا کمک گرفتن از پلیس برای شناسایی و آزادکردن گروگان‌هاست!

روش اول (پرداخت پول) مختص کسانی است که پولشان زیادی کرده اما روش دوم (بازپس‌گیری اطلاعات بدون پرداخت هزینه) مختص کاربرانی است که یک قدم جلوتر از این زورگیرها حرکت می‌کنند و البته از خوانندگان پر و پا قرص کلیک هستند!

شاه‌کلید اینجاست

نرم‌افزار WindowsUnlocker ابزار جدیدی است که توسط کمپانی مشهور Kaspersky طراحی شده است. این نرم‌افزار عملکردی همانند دیسک نجات کسپراسکای دارد و تفاوتش در این است که دیسک نجات برای پاکسازی رایانه در مواقع آلودگی به ویروس‌ها کاربرد دارد و WindowsUnlocker در مواقع گروگان گرفته شدن اطلاعات شما توسط ransomware ها مورد استفاده قرار می‌گیرد.

وقتی رایانه شما به ransomware آلوده شود و نتوانید حتی به محیط سیستم‌عامل دسترسی داشته باشید، با استفاده از این برنامه می‌توانید براحتی رایانه را در محیط داس بوت سپس نرم‌افزار را اجرا کنید. مشاهده می‌کنید که نرم‌افزار WindowsUnlocker در چند ثانیه بخش‌های کلیدی سیستم‌عامل از جمله رجیستری را مورد بررسی قرار داده و همه اطلاعات مربوط به باجگیرها را از روی رایانه شما حذف می‌کند. در نهایت با راه‌اندازی مجدد رایانه‌تان مشاهده خواهید کرد تمام اطلاعات شما از دست گروگانگیرها آزاد شده و براحتی می‌توانید از آنها استفاده کنید.

چگونه؟

چنانچه رایانه‌تان به این نوع بدافزار آلوده شده است یا به هر دلیل دیگری قصد دارید به‌طور کامل با روش استفاده از این نرم‌افزار آشنا شوید ، می‌توانید مراحل زیر را دنبال کنید:

1ـ ابتدا نسخه‌ای از این نرم‌افزار را که به صورت یک فایل ایمیج قابل رایت روی دیسک‌های فشرده یا حافظه‌های فلش است از لینک زیر دانلود کنید:

http://utils.kaspersky.com/Distr/WindowsUnlocker/KWU_1.0.3.upd.iso

2ـ چنانچه قصد دارید توسط دیسک فشرده از نرم‌افزار مربوطه استفاده کنید ، آن را روی سی‌دی یا دی‌وی‌دی مورد نظرتان رایت کنید.
در غیر این‌صورت چنانچه بخواهید آن را به حافظه فلشتان منتقل کنید ، می‌توانید با کمک ابزار
Kaspersky USB Rescue Disk Maker، آن را به حافظه فلش منتقل و فلش را نیز آماده بوت توسط این ابزار کنید.

http://rescuedisk.kaspersky-labs.com/rescuedisk/updatable/rescue2usb.exe
3ـ رایانه را توسط دیسک یا حافظه فلش ایجاد شده در مرحله 2 بوت کنید.

4ـ زبان موردنظر را از فهرست به‌نمایش درآمده انتخاب کرده و کلید اینتر را فشار دهید.

5 ـ برای استفاده راحت‌تر از برنامه، با کلیک روی گزینه Kaspersky Rescue Disk Graphic Mode کلید اینتر را فشار دهید تا برنامه در حالت گرافیک فراخوانی شود.

6 ـ درحالت گرافیک روی منوی Start کلیک کنید و گزینه KasperskyWindowsUnlocker را انتخاب کنید.

7ـ مشاهده می‌کنید که یک صفحه سفید باز شده و به بررسی بخش‌های مختلف سیستم‌عامل می‌پردازد. در نهایت نیز گزارشی از عملیات انجام شده در اختیار شما قرار می‌گیرد و با یک‌بار راه‌اندازی مجدد رایانه، تمامی بدافزارهای مورد نظر از روی رایانه حذف شده و براحتی می‌توانید از اطلاعات خود استفاده کنید.