

هشدار بسیار جدی و مهم در مورد بدافزارهای مخرب، غارتگر و باجگیر

هشدار بسیار جدی و مهم در مورد بدافزارهای مخرب، غارتگر و باجگیر

به دنبال انتشار اخباری در خبرگزاری‌ها در مورد انتشار باج‌افزارهایی که با آلوده کردن شبکه عملیات جاری سازمان‌ها را مختل کرده‌اند، مطالب زیر از سوی واحد پشتیبانی فنی در راستای پیشگیری از آلودگی با این بدافزارهای تنظیم شده است:

زمینه‌های آلوده شدن به بدافزارها

زمانی که شما سهواً خطاهای زیر را انجام دهید، امکان درگیر شدن سیستم، سرور و شبکه به باج‌افزار و بدافزارها فراهم می‌شود:

- باز کردن ایمیل دارای پیوست یا ضمیمه مشکوک و مخرب.
- کلیک روی لینک‌های مخرب که در ایمیل، شبکه‌های اجتماعی یا سایت‌ها قرار دارند.
- بازدید از سایت‌های مخرب که اغلب دارای ماهیت مستهجن هستند.
- دانلود فایل‌های مشکوک کرک‌ها، نرم‌افزارهای اجرایی و آلوده از وب سایت‌ها
- باز کردن ماکروهای فاسد در اسناد برنامه مثل واژه پردازها (Word) و صفحه گسترها (Excel)

- اتصال به دستگاه‌های جانبی USB مثل Memory ، هارد اکسترنال، MP3 player ، که محتویات آنها مطمئن نیستند یا به سیستم‌های عمومی متصل شدند.

پیشگیری و جلوگیری از ورود بدافزار یا باج‌افزار

- علی‌رغم اینکه وجود آنتی‌ویروس و بروز بودن آنها بسیار مهم است، خواهشمند است موارد زیر را در نظر داشته باشید:
- هیچگاه به ایمیل‌های با محتوای نامعلوم و یا ایمیل‌هایی که در junk و spam قرار می‌گیرند، پاسخ ندهید.
- تنها از وب‌سایت‌های امن یا وب‌سایت‌هایی که می‌شناسید استفاده نمایید.
- به طور منظم از کلیه اطلاعات مهم و بانک‌های اطلاعاتی خود نسخه پشتیبان تهیه و خارج از سیستم و سرورها نگهداری کنید.
- به طور منظم از روند تهیه نسخ پشتیبان بانک‌های اطلاعاتی نظارت و اطمینان حاصل نمایید.
- در صورتیکه منابع سرورهای شما در شبکه مانند درصد استفاده CPU به طور غیرطبیعی در بالاترین حد خود فعالیت می‌نمایند ممکن است بدافزار یا باج‌افزارها در ابتدای آلوده نمودن کلیه اطلاعات باشند. از وضعیت منابع سرورها با استفاده از سیستم‌های پایش و یا نرم‌افزار پایشگر قبل از بروز رخدادها مطلع شوید.