**گزارش عملکرد کدهای مخرب و بد افزار ها در ماه ژوئن ۲۰۰۹، بررسی خانواده بد افزار ها و راه های مختلف توزیع آنها و افزایش پیچیدگی جرایم اینترنتی.**

بد افزارها و کدهای مخرب مستقر در ابزارهای ذخیره سازی قابل حمل ، فایل های Auto Run ، دانلود بر روی درایو ها، رمز گذاری با استفاده از مکانیزم های پیچیده ، دلایل اصلی انتشار رو اعلام ۲۰ مورد از خطرناکترین کدهای مخرب و تقسیم بندی آنها در ۲ لیست مجزا می باشد.

چین با ۵۶% رتبه اول را در ایجاد بد افزار ها و روسیه با فاصله بسیار زیاد و با ۵% تولید بد افزار در مقام دوم قرار دارد.

**لیست بد افزار ها و کدهای مخربی که در زمان اجرای برنامه ها یا فایلها فعال می شوند** (On Access Malware List):

این نوع از بد افزار ها از خطرناک ترین برنامه های مخرب بوده و هچنین وسعت توزیع آنها نیز بسیار زیاد می باشد، که به هنگام اجرای آن در کامپیوتر کاربران و یا دانلود از اینترنت توسط ابزارهای امنیتی بلاک شده اند.

یکی از این بد افزارها که Net-Worm.Win32.Kido.ih نام دارد در ابتدای لیست ۲۰ ویروس برتر این ماه قراردارد که 58,200 کامپیوتر را آلوده کرده است . دو نوع دیگر از این بد افزار در این لیست نیز با میزان توزیع بسیار بالا ،نشان دهنده حضور بسیار فعال خانواده این برنامه مخرب در محیط سایبر می باشد. بد افزار Kido همچنین می تواند به راه های مختلفی خود را توزیع کند.

۲ برنامه مخرب بسیار مطرح دیگر در این لیست شامل دو کرم اینترنتی (Worm) از خانواده Autorun و یک آگهی افزاری (adware) که بر روی مرورگر اینترنت و برنامه های دریافت ایمیل مانند (Outlook, Live..) نوار ابزاری ایجاد می کند که از طریق این نوار ابزار به نمایش بنرهای ناخواسته می پردازند که حذف این آگهی افزارها نیز بسیار مشکل می باشد.

**بد افزارهای شناسایی شده در وب:** لیست دوم شامل برنامه های مخرب شناسایی شده در صفحات وب و بد افزار هایی که تلاش بر اجرای خود از طریق صفحات وب را می کنند می باشد. این لیست به سوالات ذیل پاسخ می دهد:

- چگونه از بد افزار ها اغلب صفحات وب را آلوده می کنند؟
- کدامیک از برنامه های مخرب بیشتر از بقیه، با و یا بدون آگهی کاربر از طریق صفحات آلوده دانلود شده اند؟

در این لیست ، برنامه دانلودری به نام Trojan Downloader Gumblar.a مقام اول را به خود اختصاص داده است، این تروجان پس از نصب شدن بر روی کامپیوتر کاربر تاثیر مستقیم بر روی ترافیک وب کاربر با تغییر نتایج جستجوی گوگل دارد و همچنین به جستجوی رمزهای عبور FTP ذخیره شده در سیستم می پردازد تا بتواند ازاین طریق آنها را نیز آلوده کند.

در حال حاضر تعداد سرور های آلوده شده مشخص نبوده ، بعلاوه، این بد افزار همچنان در حال توزیع و آلوده کردن سیستم

های حفاظت نشده می باشد.

برای اطلاعات بیشتر و مشاهده کامل این گزارش به سایت www.cyberoam.com/ir مراجعه نمائید.