ویروس باج گیر «لاکی» Locky

ویروس » لاکی «در دسته‌بندی نرم‌افزارهای» باج افزار «یا بصورت تخصصی‌تر در دسته بندی ویروس‌های» باج گیر «قرار می‌گیرد. این دسته از ویروس‌ها به روش‌های گوناگون مانع کار عادی سیستم کامپیوتر می‌گردند و به سرعت تقاضای مبلغی پول بعنوان باج می‌نمایند. معمولاً ویروس‌های باج گیر کارایی کامپیوتر را کاملاً مختل می‌نمایند یا اطلاعات آنرا غیر قابل دسترسی می‌کنند به نحوی که هیچ کار مفیدی نتوان با آن انجام داد. در صورتی که قربانی مبلغ باج را بپردازد ویروس سیستم را به حالت عادی بر می‌گرداند و خودش را پاک می‌کند اما اگر قربانی حاضر به پرداخت مبلغ باج نباشد باید از خیر تمامی اطلاعات خود بگذرد و با پاک کردن تمامی اطلاعات هارد دیسک و نصب مجدد سیستم عامل کامپیوتر را به حالت عادی برگرداند.

نحوه نفوذ لاکی

لاکی توسط ۱-ایمیل و ۲-فایل پیوست شده به ایمیل منتقل میشود، بویژه پیوستی که از نوع فایل ورد (word) باشد. این فایل ورد شامل یک ماکرو است که به محض اجرا شدن» ویروس باج گیر «اصلی را از اینترنت دانلود می‌کند. البته خود ایمیل بدون پیوست نیز قدرت انتقال را دارد بنابراین بهتر است از بازکردن ایمیل‌های تبلیغاتی یا با آدرس ناآشنا بپرهیزید. در برخی موارد کاربران ایرانی آلوده شده به مرجع آنتی ویروس ایران اعلام نموده‌اند که ایمیلی با عنوان مُعین‌را باز نموده‌اند و بعد از آن دچار مشکل شده‌اند بطور کلی در بیشتر موارد ایمیل‌های تبلیغاتی و با آدرس‌های ناآشنا بوده‌اند. بطور دقیق‌تر به محض اجرا شدن فایل ورد، ماکرو یک فایل از نوع BAT در هارد دیسک قربانی می‌سازد که قابلیت اجرای دستورات سیستم عامل را دارد. این فایل BAT**مانند یک دانلود کننده، فایل دیگری را با فرمت VBScript از اینترنت گرفته و اجرا می‌کند.**

نحوه خرابکاری ویروس لاکی

این ویروس به محض آلوده شدن کامپیوتر شروع به دستکاری اطلاعات فایل‌های شما می‌کند. هدف اصلی این ویروس رمزگذاری اطلاعات مهم فایل‌های کامپیوتر است. از آنجایی که بیشتر فایل‌های مهم کاربران متن‌های نوشته شده بابرنامه‌های آفیس، فیلم‌ها، عکس‌ها و تصاویر شخصی می‌باشند این ویروس با *رمزکردن* اطلاعات داخل آنها مانع دسترسی عادی به آنها می‌شود. برخی از فایل‌های معروف متنی، تصویری و صوتی که توسط ویروس لاکی مورد حمله قرار می‌گیرند عبارتند از:

.doc, .docx, RTF, .pdf, .XLS, .PPT, .dotx, .docm, .DOT, .max, .xml, .txt, .CSV, .uot, .mid, .wma, .flv, .mkv, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla, .swf, .wav, .qcow2, .vdi, .vmdk, .vmx, .gpg, .aes, .ARC, .PAQ, .tar.bz2, .tbk, .bak, .tar, .tgz, .rar, .zip, .djv, .djvu, .svg, .bmp, .png, .gif, .raw, .cgm, .jpeg, .jpg, .tif, .tiff, .NEF, .psd, .cmd, .bat, .class, .jar, .java, .asp, .brd, .sch, .dch, .dip, .vbs, .asm, .pas, .cpp, .php, .ldf, .mdf, .ibd, .MYI, .MYD, .frm, .odb, .dbf, .mdb, .sql, .SQLITEDB, .SQLITE3, .asc, .lay6, .lay, .ms11 (Security copy), .sldm, .sldx, .ppsm, .ppsx, .ppam,

.docb, .mml, .sxm, .otg, .odg, .uop, .potx, .potm, .pptx, .pptm, .std, .sxd, .pot, .pps, .sti, .sxi, .otp, .odp, .wks, .xltx, .xltm, .xlsx, .xlsm, .xlsb, .slk, .xlw, .xlt, .xlm, .xlc, .dif, .stc, .sxc, .ots, .ods, .hwp, .dotm, .stw, .sxw, .ott, .odt, .DOC, .pem, .csr, .crt, .key, wallet.dat

توجه داشته باشید که ویروس لاکی فقط به فایل‌های درایو Cشما بسنده نمی‌کند بلکه تمام فایل‌های موجود در درایوهای کامپیوتر شما را حتی حافظه‌های فلش و هارددیسک‌های اکسترنال متصل به آنرا نیز رمز می‌کند.

بعد از رمزگذاری پسوند فایل‌ها به .lockyتغییر می‌یابد البته این ویروس نام فایل‌ها را نیز عوض می‌کند که باعث سخت‌تر شدن کار با فایل‌ها می‌شود .رمزنگاری مورد استفاده این ویروس ترکیبی از دو رمزنگاری بسیار پیچیده RSAو AES-128می‌باشد که هر دو واقعاً از رمزنگاری‌های قوی هستند. در حال حاضر امکان شکستن سریع این نوع رمزنگاری بدون داشتن کلید رمز میسر نیست.

بعد از اتمام رمزگذاری نوبت درخواست پرداخت باج است. این ویروس مبلغی بین ۲۰۰ تا ۴۰۰ دلار بصورت بیت‌کوین‌درخواست می‌کند تا کلید رمز و برنامه بازگرداننده اطلاعات بصورت اول آنرا در اختیارتان قرار دهد. بیت‌کوین یک نوع پول الکترونیکی است و از آنجایی که امکان ردیابی آن سخت است در بین هکرها بسیار محبوب است.

بهتر است بدانید ویروس لاکی حتی فایل‌های VSS (Volume Snapshot Service)که به عنوان فایل های shadow copiesنیز معروف هستند را به طور کامل حذف می کند Shadow copies **.روشی است که ویندوز به صورت پَنهانی و بدون اینکه در فعالیت‌های کاربر خللی ایجاد شود، از درایوهای مشخص شده snapshotتهیه می کند.**

نحوه انتشار ویروس لاکی در شبکه

باج افزار » لاکی «حمله خود را از یک کامپیوتر آلوده دارای سیستم عامل ویندوز شروع می‌کند و به تدریج به دیگر سیستم‌های قابل دسترس در شبکه گسترش می‌یابد. گرچه حمله از سیستم عامل ویندوز شروع می‌شود اما این ویروس قابلیت آلوده کردن دیگر سیستم عامل‌ها نظیر لینوکس و OS Xاپل را نیز دارد.

نتیجه گیری

بطور کلی بهترین روش در امان بودن از ویروس‌ها، پیشگیری از آنها است، بنابراین لازم است حتماً به یک آنتی‌ویروس اورجینال با دیتابیس بروز مجهز باشید و حتماً از جدیدترین نسخه آن استفاده نمایید. از بازکردن ایمیل‌های تبلیغاتی یا ایمیل‌های با آدرس ناآشنا بپرهیزید. درضمن باید خطرهای ناشی از فعال بودن ماکروها را در مجموعه برنامه‌های آفیس، نظیر ورد و اکسل خوب بشناسید، چرا که تنها با باز کردن یک فایل wordممکن است علاوه بر از بین رفتن تمام اطلاعات خود، اطلاعات دیگر کامپیوترهای متصل به شبکه را نیز از بین ببرید. متأسفانه در حال حاضر به غیر از داشتن نسخه پشتیبان از اطلاعات، هیچ راهی برای بازگرداندن اطلاعات وجود ندارد. به شما توصیه می‌کنیم حتماً از اطلاعات خود روی DVD پشتیبان بگیرید تا درصورت آلوده شدن به ویروس لاکی اولاً بتوانید فایل‌های خود را بازیابی نمایید و دوماً تیم مرجع امکان مقایسه حداقل یک فایل سالم و فایل آلوده معادل آنرا داشته باشد تا بر اساس مقایسه آنها امکان تشخیصوجود داشته باشد.