چکیده گزارش بدافزار Duqu

مقدمه:

در چهارم اکتبر ۲۰۱۱ شرکت امنیتی سمانتک گزارشی مبنی بر انتشار بدافزاری به نام w۳۲.Duqu را که دارای اهداف جمع آوری اطلاعات از سازمان های دارای سیستم های کنترل صنعتی را بر عهده دارد را منتشر نمود بر اساس این گزارش Duqu عملکردی مشابه با بدافزار Stuxnet و حتی قوی تر از آن ، ولی اهداف متفاوت دارد این بدافزار تروجانیست که هدف آن دسترسی از راه دور به اطلاعات سیستم ها می باشد. مهاجمین در این بدافزار به دنبال اطلاعاتی همچون مستندات و گزارشات طراحی سازمان های هدف بوده تا بتوانند در حملات بعدی از آنها استفاده نمایند و بدافزار اطلاعات را به دو کشور هندوستان و بلژیک ارسال می نماید.

یافته های کلیدی بر اساس گزارشات و اطلاعات جمع آوری شده شامل موارد ذیل می باشد:

۱- بر خلاف احتمالات قبلی مطرح شده بعید به نظر می رسد این بدافزار توسط تیم های مستقل هکرها توسعه یافته باشد.

۲- بر اساس گزارش Kaspersky مشاهده بیشترین میزان آلودگی در ایران و سودان است

۳- وجود توابع و ماژول های مشترک میان بدافزار Duqu و Stuxnet

۴- تولید بدافزار توسط گروه تولید کننده Stuxnet و یا افرادی که به کد Stuxnet دسترسی کامل داشته اند

۵- مشاهده زمان کامپایل Duqu پس از اعلام و دستیابی به آخرین نمونه Stuxnet

۶- عدم وجود هیچ کدی مبنی بر هدف حمله به سیستم های صنعتی در Duqu

۷- اشتراک سازی روش انتشار Duqu بر اساس فایل های به اشتراک گذاشته شده در شبکه های سازمان ها و دسترسی به بخش های محافظت شده شبکه سازمانی

۸- محدودیت در سازمان های هدف بدافزار Duqu

۹- از بین رفتن بدافزار بعد از ۳۶ یا ۳۰ روز آلوده ساختن سیستم قربانی به صورت خودکار.

۱۰- تأیید وجود نسخه های متفاوت بدافزار بنابر انتخاب اهداف و قربانی های مختلف در کشورها

۱۱- شناسایی حداقل چهارده نسخه از بدافزار Duqu

۱۲-بدافزار Duqu دارای چهارچوب چند منظوره بوده که منجر به فعالیت بدافزار از طریق ماژول های متفاوت در سراسر دنیا می گردد.

۱۳- استفاده از روال های تشخیص آلودگی فعلی بر اساس شناسایی فایل درایور بوده و امکان شناسایی فایل PNF اصلی بدافزار را ندارد زیرا DLL اصلی بدافزار که امکان ایجاد مجدد Duqu را میسر می سازد پنهان می باشد.

۱۴- مهاجمین قابلیت اعمال تغییرات دلخواه خود بر کد بدافزار و ایجاد نسخه های جدید را پیش از اجرای افشای نحوه عملکرد نسخه قدیمی تر را دارد برخی از درایورهای این بدافزار در تاریخ ۱۷ اکتبر ایجاد شده اند.

روش های شناسایی بدافزار Duqu :

۱- برقراری ارتباط سیستمهای شبه سازمان با سرورهای کنترل و فرماندهی به آدرس های ۲۰۶.۱۸۳.۱۱۱.۹۷ و ۷۷.۲۴۱.۹۳.۱۶۰

۲- وجود کلید رجیستری

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURENTVERSION\INTERNETS ETTINGS\ZONES\۴\"CFID"

۳- مشاهده درایوری ناشناس در مسیر %SYSTEM%\DRIVERS

۴- مشاهده وظایف ناشناس برنامه ریزی شده در وظایف سیستم که از طریق فولدر TASKS سیستم قابل بررسی می باشد.

تحلیل بخش های مختلف بدافزار:

۱- بر اساس تحلیل انجام شده Duqu دارای درایور ، بخش DLL و فایل CONFIGURATION می باشد و فایل INSTALLER که منجر به نصب فایل های مذکور و و فعال سازی درایور در سرویس سیستم می باشد.

۲- Duqu از ارتباطات http و https به منظور ارتباط با سرورهای کنترل و فرماندهی به آدرس ۲۰۶.۱۸۳.۱۱۱.۹۷ که در کشور هندوستان و ۷۷.۲۴۱.۹۳.۱۶۰ که در کشور بلژیک هاست شده است استفاده می نمایند و به راحتی از آن عبور می کند. پس از ارتباط با سرور کنترل و فرماندهی فایل های اجرایی دیگر به منظور سرقت اطلاعات ، بررسی شبکه سازمان ، ثبت اطلاعات کیبورد و جمع آوری اطلاعات سیستم بر روی سیستم قربانی دانلود می گردد. این اطلاعات بر روی فایل کوچک رمز و فشرده شده و با فرمت jpg ذخیره می گردد.

۳- این بدافزار قابلیت اشتراک گذاری در شبکه های سازمانی استفاده می نماید بدین معنا که بدافزار توسط فایل پیکربندی خود از ارتباطات peer۲peer به منظور ارتباط با سیستم های آلوده در شبکه محلی به عنوان سرور کنترل و فرماندهی خود استفاده می نماید بنابراین بدافزار می تواند سیستم هایی را که به اینترنت دسترسی ندارند و در بخش های امنیتی شبکه سازمان قرار گرفته اند را نیز آلوده نماید.

۴- بدافزار امکان تغییر مدت ماندگاری بر سیستم را دارا می باشد.

روش های پیشنهادی اولیه درخصوص کاهش پیامد بدافزار:

۱- نصب ابزار شناسایی بدافزار ارسالی از پلیس فضای تولید و تبادل اطلاعات استان سمنان

۲- بررسی ترافیک ارسالی از کاربران به سرور کنترل فرماندهی با آدرس ۲۰۶.۱۷۳.۱۱۱.۹۷ و ۷۷.۲۴۱.۹۳.۱۶۰

۳- بررسی ارتباط با سرور کنترل و فرماندهی بر روی پورت ۴۴۳ بدون استفاده از پروتکل https

۴- بررسی وجود فایل هایی با نام DQ در فولدر TEMP ویندوز کاربران

۵- درک تهدیدات مهندسی اجتماعی به منظور کاهش امکان انتشار بدافزار همچون عدم کلیک بر روی لینک های نامه های الکترونیک

۶- بررسی و اسکن فایل ها در سیستم ایزوله (virtual machine) ، فایل هایی از نوع Microsoft word و ارسال شده از منابع نامعتبر

راهنمای نصب ابزار شناسایی بدافزار Duqu:

۱- کپی فولدر Duqu-removal tool-v۱۰ از روی cd بر روی سیستم

۲- اجرای ابزار شناسایی بدافزار (Duqu-patternscan.exe) بر روی سیستم (حداقل زمان مورد نیاز برای اسکن ۳۰ دقیقه می باشد)

۳- پس از پایان اسکن ذخیره سازی خودکار فایل log در فولدر Duqu-removal tool-v۱۰ با فرمت ذیل توسط ابزار Duqu-rootkit-scanner macaddress.log

۴- ذخیره سازی خودکار فایل های آلوده Duqu-removal tool-v۱۰ با فرمت ذیل توسط ابزار infected_files-macaddress.zip

۵- در صورت مشاهده آلودگی ارسال دو فایل فوق به صورت فشرده با رمز عبور infected به همراه اطلاعات ذیل به این پلیس مراجعه نمایید.

۶- نام سازمان ، شماره تماس و نام مسئول مربوطه درخصوص همکاری با پلیس فضای تولید و تبادل اطلاعات استان سمنان

ردیف	نام فایل	زمان اسکن سیستم

۷- جهت سهولت اجرای ابزار در شبکه سازمان ، می توان از طریق Active Directory و ساخت Map-Drive بر روی کلاینت ها مراحل فوق را انجام داد.