آرش طاهر کلاته ۸۸۲۹۸۰

ویروس **Duqu**

در ابتدا توسط شرکت سمانتیک کشف و خطوط صنعتی تشخیص داده شد . به عقیده این کارشناسان این ویروس دنبال‌ای بر ویروس استاکس اینترنت بود و نویسنده این دو یک فرد یا سازمان بود است . هرچند شک و شبهاتی در این زمینه موجود است . شباهت اصلی این دو برنامه در روش رمز گذاری و قرار دادن فایل بر روی کامپیوتر قربانی است .
وظیفه اصلی این ویروس جم آوری اطلاعات از واحدهای صنعتی بود. احتمال داده میشود که از این داده‌ها برای طراحی ویروس‌های اختصاصی جدید استفاده شده باشد . این ویروس خود صدمه خاصی به سیستم وارد نمیکند .
تعارض کار این ویروس بدین صورت است که پس از آلوده کردن هدف، با یک سرور که در هند قرار داشته (و همکنون دسترسی–ها به آن قطع شده است) ارتباط برقرار میکرد برای گرفتن دستورت جدید . هرچند این ارتباط قطع شده اما امکان دارد این برنامه اقدام به وصل شدن به شبکه در قسمت‌های دیگری را نیز داشته باشد .
تقریبا همه کارشناسان دولت آمریکا و اسرائیل را پشت این حملات می‌بینند .
عدّه‌ای اعتقاد دارند این ویروس صرفاً به دلیل شباهت خود به ویروس استاکس اینترنت بر سر زبان‌ها افتاده و با هزاران ویروس دیگر تفاوت چندانی ندارد .

Viper Virus

این ویروس چندی پیش به جان وزارت نفت افتاد و باعث ایجاد اختلال در قسمت‌های مختلف این سازمان وسیع شد .
نسل دوم این ویروس نیز چندی پیش خود را نشان داد .
در ابتدا وجود این ویروس به علت فعالیت های تخریبی که برای آن بیان شد (مانند سوزاندن مادر بورد و یا پاک کردن غیر قابل بازگشت هارددیسک در محیط ویندوز) توسط بسیاری از کارشناسان مورد تأیید قرار نگرفت امّا تحقیقات فنی تازه، نشان می دهد که نفوذ ویروس "وایپر"و یا

دست کم نفوذ ویروس دیگری با عملکردهای کاملاً شبیه به "وایپر" به برخی مراکز سازمانی کشور امکان پذیر بوده است.

کاربرانی که از برنامه‌های ایمن‌ساز پورت‌های یواس‌بی استفاده نمی‌کنند، به محض اتصال حافظه‌های جانبی حاوی **USBCheck. exe** هدف حمله ویروس **W32/VRBAT** قرار می‌گیرند. در صورتی که کاربر سطح دسترسی بالایی در شبکه نداشته باشد، این ویروس، خود را در فولدر **temp** قرار داده و تمام حافظه‌های جانبی متصل‌شده به سیستم را تا زمان حصول دسترسی مدیریتی آلوده می‌کند. اما در صورت اجرای ویروس با دسترسی سطح بالا، ویروس خود را به فولدر **Windows** و با نام **svchost. exe** منتقل می‌کند. اکنون پس از یک دوره خاموش که ویروس در آن تنها اقدام به انتشار خود از طریق حافظه‌های جانبی محافظت‌نشده می‌کند، مرحله بعدی تخریب آغاز می‌شود: ایجاد تغییر در فایل‌های حیاتی سیستم مانند **Bootmgr**، **Ntldr** و نیز کپی کردن دو فایل دیگر با عنوان **roco. sys** و **roco. bin** در پارتیشن نصب ویندوز، بستر را برای ضربه نهایی آماده می‌کند. حال وقتی در آخرین مرحله، رایانه خود را روشن می‌کنید، به جای سیستم عامل فعلی شما، یک سیستم عامل دیگر توسط ویروس **WIN32/VRBAT** فعال (**Boot**) می‌شود.

StuxNet

احتمال داده میشود که این ویروس به دستور مستقیم رئیس جمهور آمریکا، باری خرابکاری در تاسیسات هسته‌ای ایران ساخته شده باشد .

این ویروس با توجه به حجم بالایی که دارد، یکی از پیچیده‌ترین ویروس‌های نوشته شده شناخت می‌شود. انتقال اولیه این وروس به داخل کشور، احتمالا توسط یک جاسوس دو جانب صورت گرفته است .

این بدافزار با استفاده از نقص امنیتی موجود در میانبرهای ویندوز، با آلوده کردن رایانه‌های کاربران صنعتی، فایل‌های با قالب اسکادا که مربوط به نرم‌افزارهای **WinCC** و **PCS7** شرکت زیمنس می‌باشد را جمع‌آوری کرده و به یک سرور خاص ارسال می‌کند.

این کرم، برای بالا آمدن خود را در رجیستری ویندوز کپی میکرد و برای دور زدن فایروال خود را به مررگر اینترنت اکسپلورر میچسباند .

این کرم به صورت هدفدار پخش شده، به نحوی که بیش از شصت درصد سیستم‌های آلوده شده به این کرم در ایران قرار دارند .