آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

خبرنامه تحلیلی رویدادهای امنیتی (روزانه)

سه‌شنبه دوازدهم آذر ماه ۱۳۹۸

آلودگی بیش از هشتاد هزار رایانه توسط بدافزار[1] دِکسفُت[2]

نسخه ۱,۰,۰

نویسنده : مونا رضا زاده **سردبیر :** محمد پیشدار

[1]-Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network.

[2]-Dexphot

هشتاد هزار رایانه ویندوزی تحت تاثیر بدافزار دِکسفُت قرار گرفته‌اند

تاریخ: ۲۶/ نوامبر/ ۲۰۱۹

بررسی اجمالی :

بتازگی کارشناسان حوزه امنیت اطلاعات خبری را در رابطه با کشف یک بدافزار جدید در رایانه‌های ویندوز منتشر کرده‌اند. این بدافزار دِکسفُت نام داشته و با استفاده از منابع پردازشی قربانیان خود به استخراج ارزهای دیجیتال[۱] می‌پردازد. اوج فعالیت دِکسفُت در ژوئن ۲۱۰۹ بوده و تا کنون بیش از هشتاد هزار رایانه را آلوده کرده است [۱].

نگاه کلی :

سیستم‌های آسیب‌پذیر	رایانه‌های ویندوز		
شدت خطر	**در دولت**	**در تجارت**	**کاربران خانگی**
	بالا	**بالا**	**بالا**
راه‌های نفوذ	دریافت نرم‌افزار از منابع نامعتبر توسط قربانی، اجرای کِرَک[۳]های مخرب توسط قربانی		
هدف	استخراج غیرمجاز ارز دیجیتال با سوءاستفاده از منابع پردازشی قربانیان		

توضیحات فنی :

بتازگی کارشناسان حوزه امنیت اطلاعات شرکت مایکروسافت[۳] بدافزاری به نام دِکسفُت را در بسیاری از رایانه‌های ویندوزی شناسایی کرده‌اند. طبق گفته یک تحلیلگر بدافزار به نام هازل کیم[۴]، دِکسفُت همیشه فعال بوده و هدف آن

[1]-A cryptocurrency (or crypto currency) is a digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets.

[3]-Crack is the modification of software to remove or disable features which are considered undesirable by the person cracking the software especially copy protection features or software annoyances like nag screens and adware.

استفاده از منابع قربانیان برای استخراج ارزهای دیجیتال است. این بدافزار با وجود هدف ساده، از پیچیدگی و تکامل بالایی برخوردار بوده که فراتر از تهدیدهای روزمره اینترنتی می‌باشد. روش‌های پیشرفته اجرای بدون فایل[۳]، تکنیک‌های چند شکلی[۴] و مکانیزم‌های ماندگاری چند لایه از جمله رویکردهای مورد استفاده در دِکسفُت هستند [۱].

از آنجایی که دِکسفُت قابلیت نصب بر روی رایانه‌ها آلوده به بدافزار آی.سی.لودر[۶] را داشته محققان از اصطلاح پیلود دو مرحله‌ای[۷] برای تعریف آن استفاده می‌کنند. بدافزار آی.سی.لودر معمولا بصورت افزونه در کنار بسته‌های نرم‌افزاری بر روی سیستم قربانی نصب می‌گردد. دریافت نرم‌افزار از منابع نامعتبر و استفاده از سرویس‌های کرک شده احتمال آلودگی به این بدافزار را افزایش می‌دهد [۱]. در ادامه به بررسی رویکردهای پیشرفته مورد استفاده در بدافزار دکسفُت پرداخته شده است.

اجرای بدون فایل بدافزار:

طبق گفته مایکروسافت فقط فایل نصاب دِکسفُت به مدت کوتاهی بر روی دیسک نوشته شده و بقیه بخش‌های آن با استفاده از روش "اجرای بدون فایل" در حافظه سیستم اجرا می‌شوند. روشی که هدف اصلی آن مخفی‌سازی بدافزار بر روی سیستم قربانی است. به این ترتیب دِکسفُت می‌تواند بدون شناسایی و با استفاده از فرایندهای صحیح و معتبر ویندوز مانند msiexec.exe, unzip.exe, rundll32.exe, schtasks.exe, powershell.exe به اجرای کدهای مخرب خود بپردازد [۱].

تکنیک‌های چند شکلی بدافزار:

یکی دیگر از پیچیدگی‌های دِکسفُت استفاده از روش‌های چند شکلی است. در این روش بدافزار بطور مدوارم اطلاعات خود را تغییر می‌دهد. طبق گفته مایکروسافت اپراتورهای دِکسفُت هر ۲۰ الی ۳۰ دقیقه یک بار، نام فایل و یو.آر.اِل‌های[۸] مورد استفاده در فرایند آلودگی را تغییر می‌دهند. با بهره‌گیری از این روش، ضد ویروس‌ها قادر به شناسایی بدافزار نبوده، زیرا الگوهای تشخیص پس از مدت کوتاهی فاقد اعتبار می‌شوند [۱].

---

[1]-Microsoft Corporation is an American multinational technology company with headquarters in Redmond, Washington. It develops, manufactures, licenses, supports and sells computer software, consumer electronics, personal computers, and related services.

[2]-Hazel Kim

[3]-Fileless malware is a variant of computer related malicious software that exists exclusively as a computer memory-based artifact i.e.

[4]-Polymorphic malware is a type of malware that constantly changes its identifiable features in order to evade detection.

[6]-ICLoader is the generic detection name for a family of bundlers that install adware on the affected Windows systems.

[7]-Second stage payload

[8]-A Uniform Resource Locator (URL), colloquially termed a web address, is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.

رویکرد ماندگاری چند لایه:

با وجود این رویکرد در صورت حذف یکی از لایه‌های بدافزار، امکان آلودگی مجدد سیستم همچنان وجود خواهد داشت. در واقع دِکسفُت پس از نفوذ به سیستم قربانی سریعاً با استفاده از روش "نخلیه فرایندها[1]"، دو فرایند مجاز ویندوز به نام‌های svchost.exe و nslookup.exe را اجرا و محتوای آن‌ها را با کدهای مخرب جایگذاری می‌کند. بدین روش کدهای مخرب از طریق فرایندهای مذکور اجرا شده و توسط سیستم مجاز شمرده می‌شوند. این دو فرایند به عنوان زیرمجموعه‌ای از دِکسفُت فعالیت کرده، و نگهبان اجرای صحیح تمام بخش‌های بدافزار می‌شوند. حتی در صورت توقف یکی از آن‌ها، دیگری به عنوان پشتیبان وارد عمل شده و دوباره فرایند را اجرا می‌کند [۱].

از قابلیت‌های دیگر این بدافزار آلودگی مجدد سیستم طی هر راه‌اندازی مجدد (۹۰ الی ۱۱۰ دقیقه) است. از آنجایی که دوره زمانی منظمی برای اجرای وظایف در نظر گرفته شده عوامل دِکسفُت قادر به بروزرسانی سیستم‌های آلوده خواهند بود. به عبارت دیگر در هر دوره زمانی فایلی از خدمات‌رسان مهاجم دریافت شده که حاوی دستورالعمل‌های بروزرسانی برای بدافزار است [۱].

پیشنهادات [۱]

- دریافت برنامه‌ها از منابع معتبر

منابع :

1. The Hacker News Website
https://www.zdnet.com/article/microsoft-says-new-dexphot-malware-infected-more-than-80000-computers/

[1]-Process Hollowing or Hollow Process Injection is a code injection technique in which the executable section of a legitimate process in the memory is replaced with malicious code (mostly malicious executable)