بازگشت Duqu به درون شبکه یکی از بزرگ‌ترین شرکت‌های نرم‌افزاری امنیتی

حمله هکری پیچیده و پنهانی به شرکت کسپرسکی

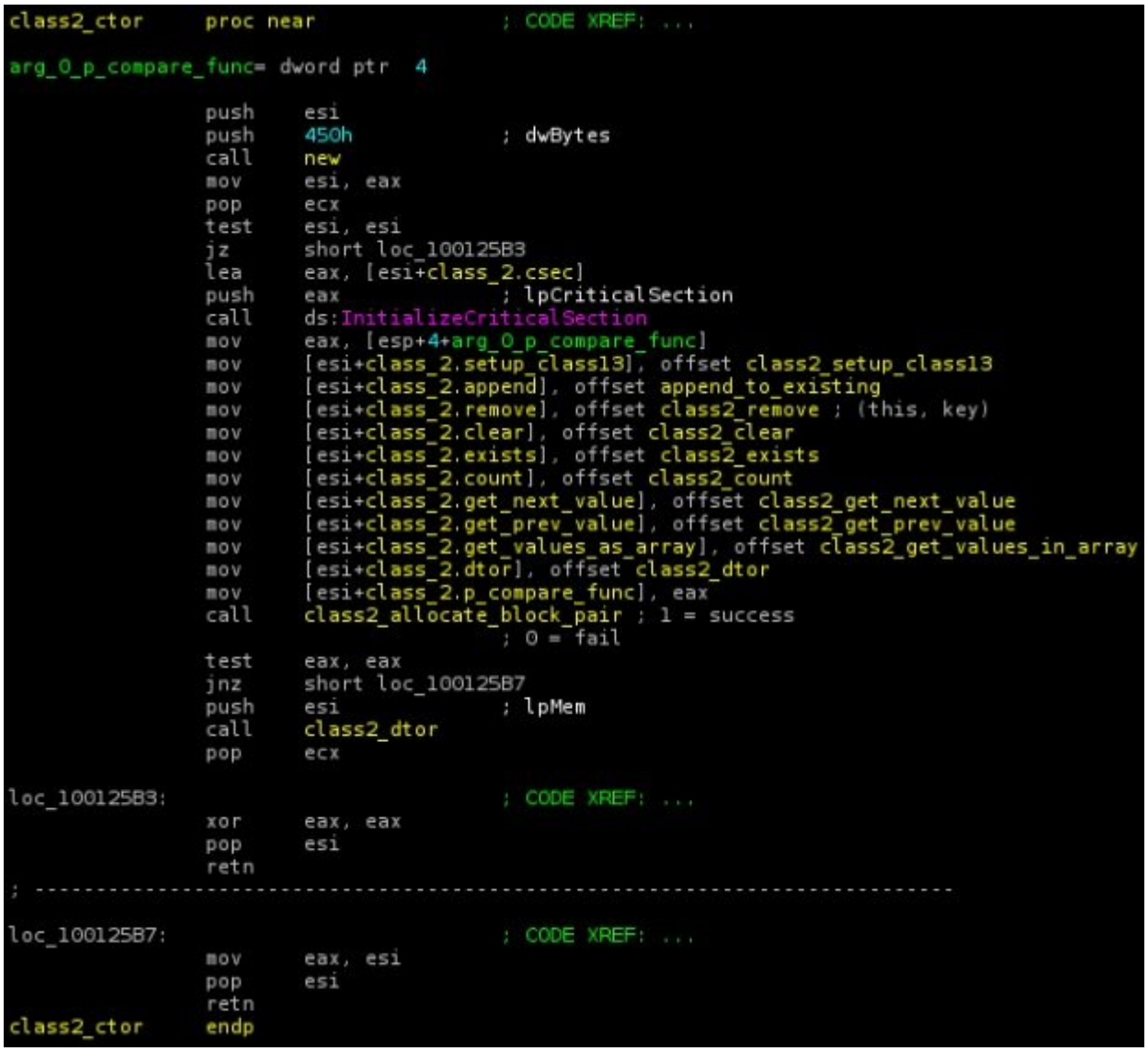
Duqu بازگشته است! آزمایشگاه کسپرسکی یکی از بزرگ‌ترین شرکت‌های تحقیقاتی و فعال در زمینه امنیت رایانه‌ها تأیید کرد که دیروز مورد حمله هکری قرار گرفته است. یوجین کسپرسکی؛ مدیرعامل این شرکت در رابطه با این حمله نوشت: « ما از یک حمله پیشرفته به شبکه‌های داخلی کسپرسکی اطلاع پیدا کردیم. این یک حمله پیچیده و کاملا پنهانی بود که از چندین آسیب‌پذیری روز صفر استفاده کرده بود. ما کاملا اطمینان داریم یک نهاد دولتی در پشت این حمله قرار داشته است.»

اکسپلویت روز صفر چیست؟

برای آن‌هایی که ممکن است با اصطلاح آسیب‌پذیری روز صفر آشنایی نداشته باشند باید بگوییم اکسپلویت روز صفر (Zero-Day) درست در همان روزی که ضعفی در یک نرم‌افزار کشف می‌شود مورد بهره‌برداری قرار می‌گیرد. در این نقطه، قبل از آن‌که اصلاحیه مورد نیاز توسط سازنده نرم‌افزار ارائه شود، این آسیب‌پذیری مورد بهره‌برداری قرار می‌گیرد. درباره حملات روز صفر اینجا بیشتر بخوانید.

Duqu چه بود؟

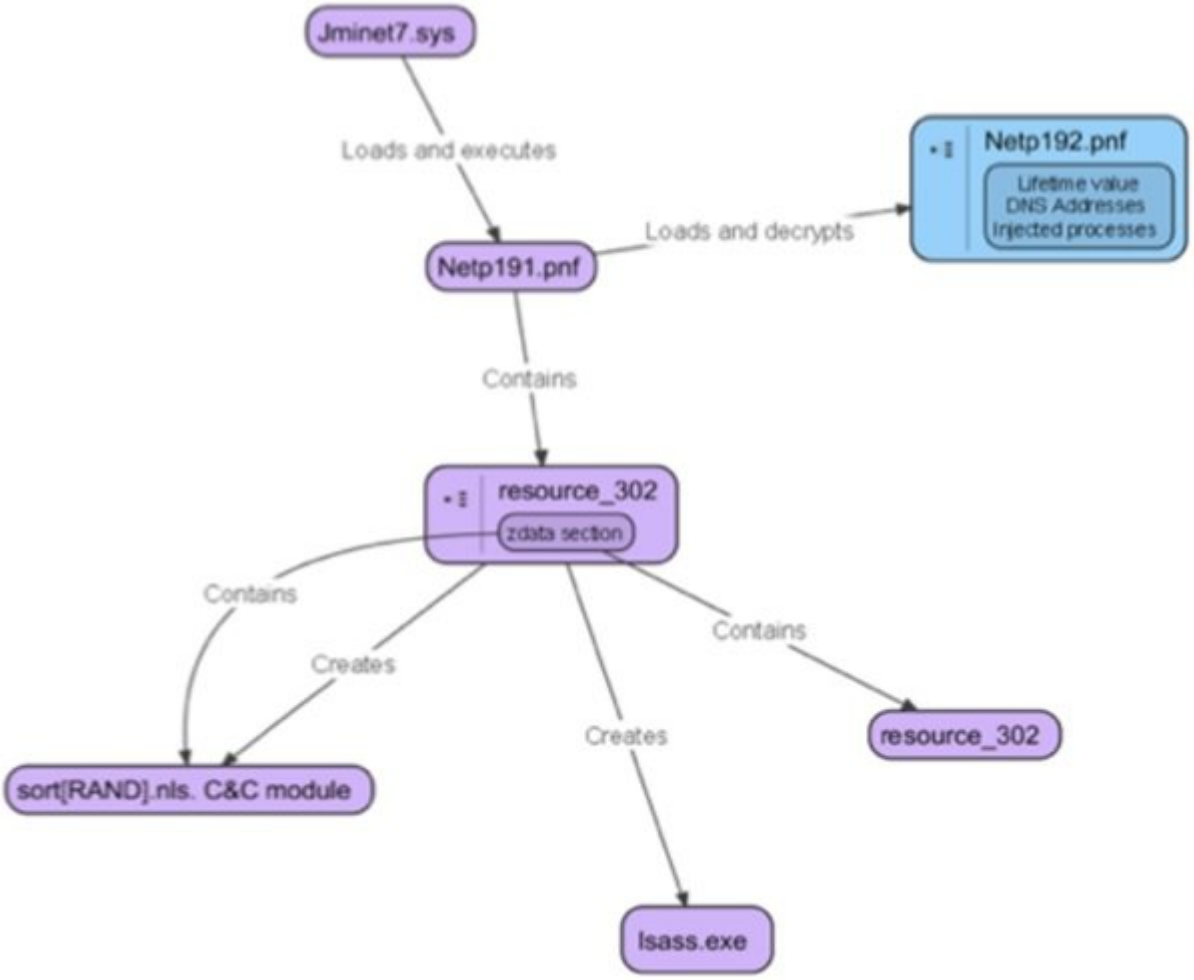
اخبار حاکی از آن است که یک حمله هکری پیشرفته روی شبکه‌های داخلی کسپرسکی اتفاق افتاده است. حمله‌ای پیچیده که از بالاترین مکانیزم اختفاء بهره برده است. کسپرسکی نام این حمله را Duqu 2.0 نام نهاده است. زیرا تروجان جدید ردپایی از سلسله حملات گسترده‌ای دارد که در سال 2011 به وقوع پیوست. یک سال بعد از آن که کرم استاکس‌نت شناسایی شد، سیمانتک قطعه جدیدی از این بدافزار که با استفاده از آن همان فناوری سیستم‌هایی را در اروپا آلوده ساخت شناسایی کرد. این تروجان جدید در آن روزگار Duqu نام گرفت که تقریبا مشابه به استاکس‌نت بود و به نظر می‌رسید حداقل کسی که دسترسی مستقیم به کدهای منبع استاکس‌نت داشته، این تروجان را طراحی کرده است. در آن روزگار اعلام شد Duqu با استفاده از یک زبان برنامه‌نویسی نامشخص نوشته شده است. به طوری که کسپرسکی ضمن درخواست کمک از برنامه‌نویسان اعلام کرد ما صد در صد اعتقاد داریم این بدافزار به زبان Visual C++ نوشته نشده است.



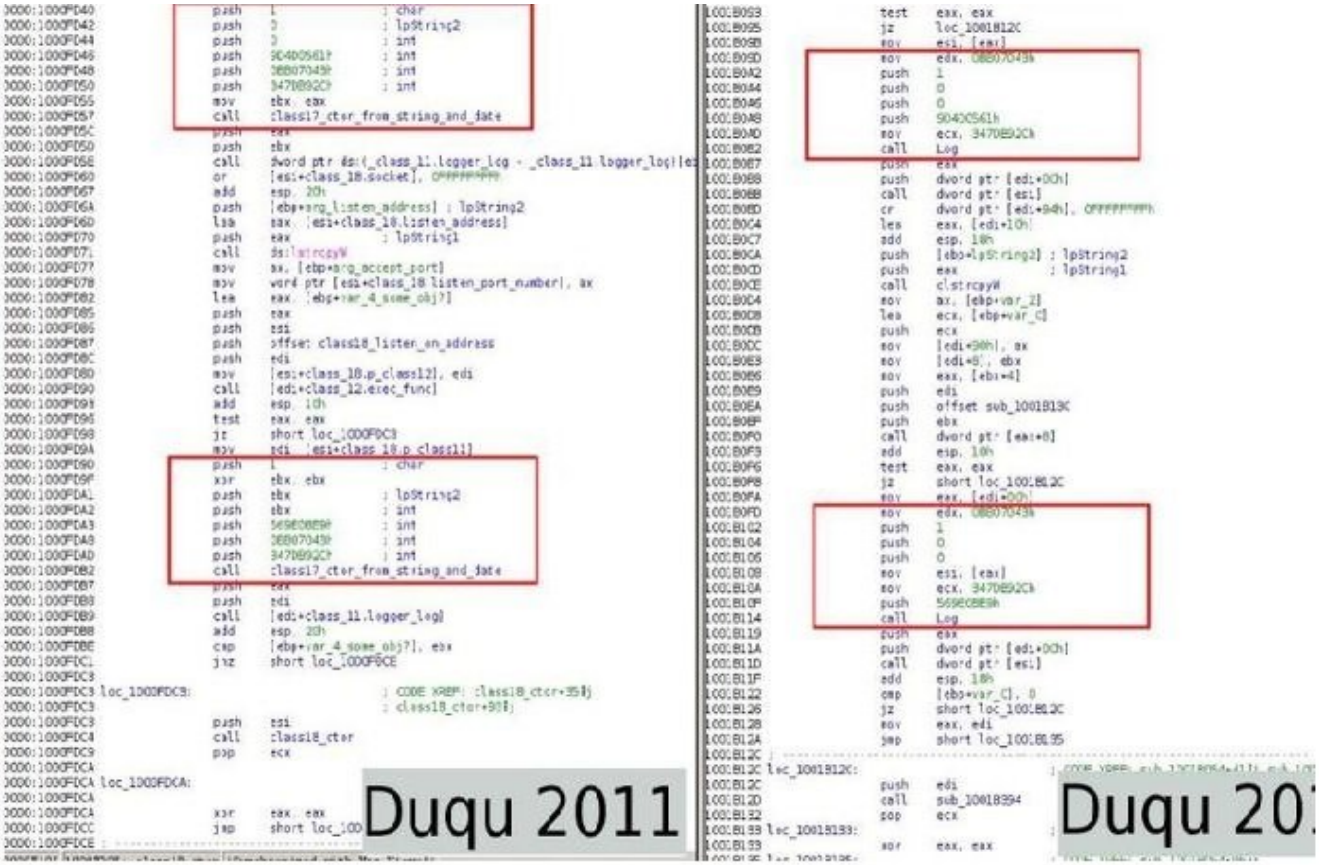
```
class2_ctor     proc near               ; CODE XREF: ...

arg_0_p_compare_func= dword ptr  4

                push    esi
                push    450h            ; dwBytes
                call    new
                mov     esi, eax
                pop     ecx
                test    esi, esi
                jz      short loc_100125B3
                lea     eax, [esi+class_2.csec]
                push    eax             ; lpCriticalSection
                call    ds:InitializeCriticalSection
                mov     eax, [esp+4+arg_0_p_compare_func]
                mov     [esi+class_2.setup_class13], offset class2_setup_class13
                mov     [esi+class_2.append], offset append_to_existing
                mov     [esi+class_2.remove], offset class2_remove ; (this, key)
                mov     [esi+class_2.clear], offset class2_clear
                mov     [esi+class_2.exists], offset class2_exists
                mov     [esi+class_2.count], offset class2_count
                mov     [esi+class_2.get_next_value], offset class2_get_next_value
                mov     [esi+class_2.get_prev_value], offset class2_get_prev_value
                mov     [esi+class_2.get_values_as_array], offset class2_get_values_in_array
                mov     [esi+class_2.dtor], offset class2_dtor
                mov     [esi+class_2.p_compare_func], eax
                call    class2_allocate_block_pair ; 1 = success
                                        ; 0 = fail
                test    eax, eax
                jnz     short loc_100125B7
                push    esi             ; lpMem
                call    class2_dtor
                pop     ecx

loc_100125B3:                           ; CODE XREF: ...
                xor     eax, eax
                pop     esi
                retn
; ---------------------------------------------------------------------------

loc_100125B7:                           ; CODE XREF: ...
                mov     eax, esi
                pop     esi
                retn
class2_ctor     endp
```

Duqu همانند استاکس‌نت خود را به عنوان یک قطعه کد نرم‌افزاری قانونی که یک فایل درایور دارای گواهی نامه دیجیتالی معتبر بود نشان داد. این گواهی‌نامه معتبر از طرف یک شرکت تایوانی به نامC-Media Electronics Incorporation ارائه شده بود که بعدها زمانی که سیمانتک آن‌را به عنوان یک بدافزار شناسایی کرد، اعتبار آن ساقط شد. Duqu هدفش کشورهای سوئیس، هلند، سودان، ویتنام،، هند، فرانسه و اوکراین بود و در سال 2011 این کشورها را مورد حمله قرار دارد.

دیاگرامی که سیمانتک برای Duqu تشریح کرده بود را در تصویر زیر مشاهده می‌کنید:



کسپرسکی کدهای مورد استفاده در Duqu و Duqu 2.0 را مورد بررسی و مقایسه قرار داده است. تصویر زیر نتیجه این مقایسه را نشان می‌دهد.



عاقلانه نیست از فناوری پیشرفته‌ای که هرگز مورد استفاده قرار نگرفته برای جاسوسی روی یک شرکت امنیتی استفاده شود

در پستی که توسط کسپرسکی منتشر شده است، می‌گوید: « حمله‌کنندگانی که در پشت Duqu 2.0 قرار داشتند امیدوار بودند به شبکه‌های کسپرسکی برای کسب اطلاعات بیشتر در مورد سرویس‌های این شرکت نفوذ کنند. این گروه علاقمند بودند تا اطلاعاتی را در رابطه با فناوری‌های Secure Operating System, Kaspersky Fraud Prevention, Kaspersky Security Network, Anti-APT solution به‌دست آوردند. کسپرسکی می‌گوید: « گروهی که در پشت Duqu 2.0 قرار دارند، در نظر داشتند، چند هدف برجسته را مورد جاسوسی قرار دهند. هر چند اعتقاد داریم این حمله قرار بود در سطح گسترده‌تر و اهداف بالاتری را مورد تخریب قرار دهد.»

کسپرسکی می‌افزاید: « اوضاع به‌وجود آمده ترکیبی از خبرهای خوب و خبرهای بد است. قسمت بد این اتفاق کاملا مشخص است، یک شرکت امنیتی هک شده است. اما خبر خوب این است که هیچ یک از سرویس‌های این شرکت به خطر نیافتاده‌اند. عاقلانه نیست از فناوری پیشرفته‌ای که هرگز مورد استفاده قرار نگرفته برای جاسوسی روی یک شرکت امنیتی استفاده شود. به دلیل این‌که کسپرسکی خود اقدام به فروش فناوری‌های ویژه‌ای می‌کند که به آن‌ها تجهیز است.»

کسپرسکی در ادامه افزود: « این حمله به ما کمک کرد تا دانش جدیدی در این زمینه به‌دست آورده و سطح فناوری‌های دفاعی خود را بهبود بخشیم.» هدف حمله‌کنندگان از نفوذ به کسپرسکی، تلاش برای به دست آوردن تحقیقاتی بود که این شرکت در زمینه نسل بعدی فناوری‌های جاسوسی که هکرها در حال طراحی آن هستند، انجام داده است. کسپرسکی می‌گوید: « ما از یک فناوری و چهارچوب بسیار پیچیده و گران قیمت که سال‌ها در حال توسعه آن بودیم استفاده کردیم.» این شرکت امنیتی همچنان در حال بررسی Duqu 2.0 است تا حقایق بیشتری درباره Duqu 2.0 به‌دست آورد. هر چند این شرکت انگشت اتهام خود را به سوی هیچ نهادی که احتمال می‌رود در پشت این حمله قرار داشته باشد نشانه نرفته، اما از سازمان‌های فدرال برای آغاز تحقیقات جنایی درخواست کمک کرده است.

کسپرسکی گزارش شناسایی آسیب‌پذیری‌های روز صفر را برای مایکروسافت ارسال کرده و مایکروسافت به‌تازگی

وصله‌های لازم در زمینه رفع این آسیب‌پذیری‌ها را ارائه کرده است. دو مورد از این آسیب‌پذیری‌ها در سطح کرنل بوده و بحرانی هستند. فهرست آسیب‌پذیری‌های شناسایی شده در نرم‌افزارها به شرح زیر هستند:

- Windows Kernel, win32k.sys (MS15-061)
- Internet Explorer – *critical*
- Windows Media Player – *critical*
- Microsoft Common Controls
- Microsoft Office
- Active Directory Federation Services
- Exchange Server

برای کسب اطلاعات بیشتر درباره این وصله‌ها به آدرس Microsoft Security Updates June 2015 مراجعه کنید.

تاریخ انتشار:
22 خرداد 1394

نشانی منبع: https://www.shabakeh-mag.com/security/835