



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 کاملاً پنهانی بود که از چندین آسیب‌پذیری روز صفر استفاده کرده بود. ما کاملاً اطمینان داریم یک نهاد دولتی در پشت این حمله قرار داشته است.»

اکسلویت روز صفر چیست؟

برای آن‌هایی که ممکن است با اصطلاح آسیب‌پذیری روز صفر آشنایی نداشته باشند باید بگوییم اکسلویت 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. [در باره 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 تقریباً 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

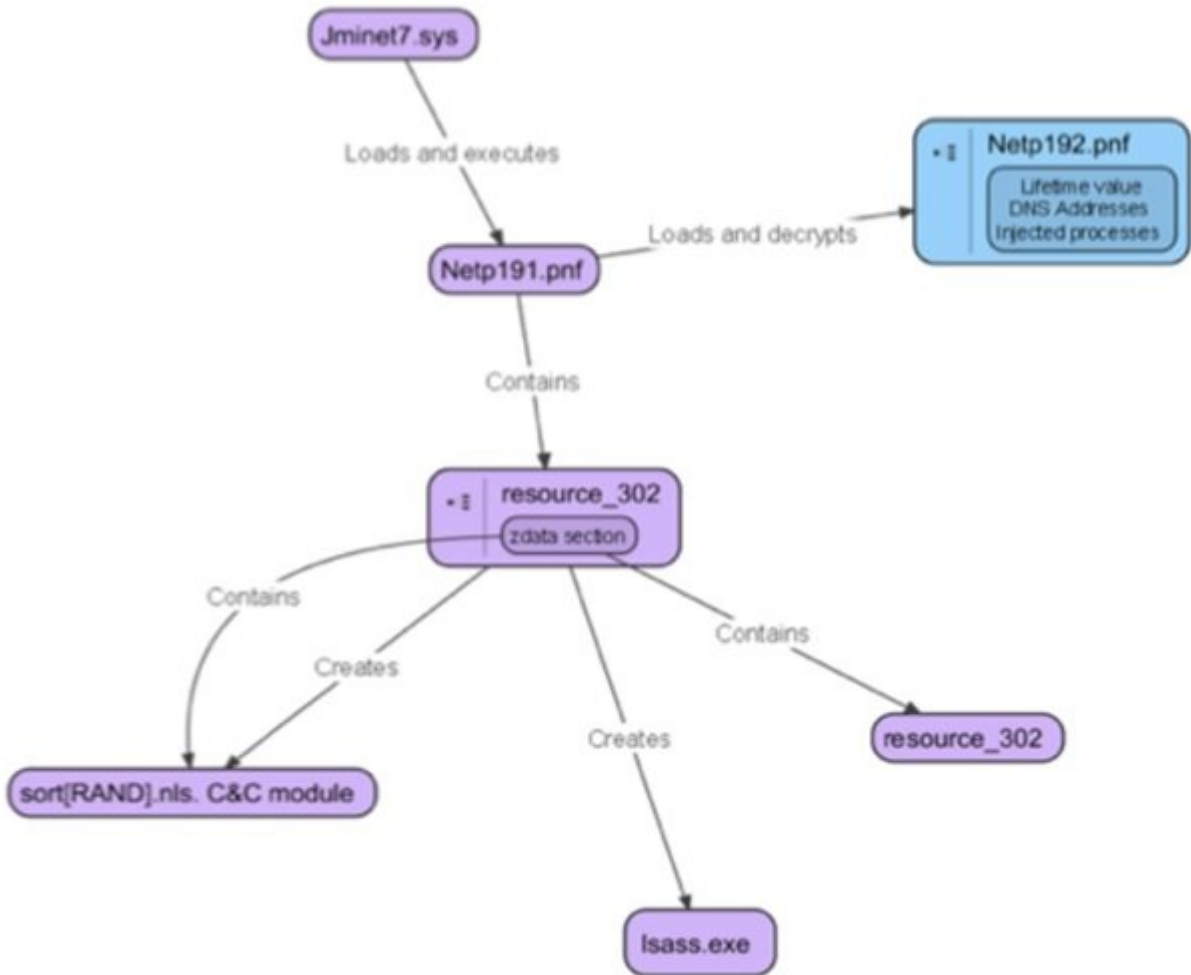
loc_100125B3:    ; CODE XREF: ...
    xor     eax, eax
    pop     esi
    retn

; -----
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 نام C-Media Electronics Incorporation ارائه شده بود که بعدها زمانی که سیمانتک آن را 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.

```

3000:100F40      push    1             ; char
3000:100F42      push    0             ; lpString2
3000:100F44      push    0             ; int
3000:100F46      push    3C4005617    ; int
3000:100F48      push    3E807043E    ; int
3000:100F4A      push    347B992CF    ; int
3000:100F4C      mov     ebx, eax
3000:100F4E      call   class17_ctor_from_string_and_date
3000:100F50      push    eax
3000:100F52      push    ebx
3000:100F54      call   dword ptr ds:(class_11.logger_log + class_11.logger_log)
3000:100F56      or     [esi+class_18.Socket], 0FFFFFFFh
3000:100F58      add     esp, 20h
3000:100F5A      push    [ebp+arg_listen_address] ; lpString2
3000:100F5C      lss    eax, [esi+class_18.listen_address]
3000:100F5E      push    eax
3000:100F60      call   ds!strncpyW
3000:100F62      mov     ax, [ebp+arg_access_port]
3000:100F64      word ptr [esi+class_18.listen_port_number], ax
3000:100F66      lea    eax, [ebp+var_4.some_obj?]
3000:100F68      push    eax
3000:100F6A      push    esi
3000:100F6C      push    offset class18_listen_address
3000:100F6E      push    edi
3000:100F70      mov     [esi+class_18.p_class12], edi
3000:100F72      call   [edi+class_12.exec_func]
3000:100F74      add     esp, 10h
3000:100F76      test   eax, eax
3000:100F78      jz     short loc_100FDC3
3000:100F7A      mov     edi, [esi+class_18.p_class11]
3000:100F7C      push    1             ; char
3000:100F7E      xor     ebx, ebx
3000:100F80      push    ebx
3000:100F82      push    ebx
3000:100F84      push    ebx
3000:100F86      push    569E08E8h    ; int
3000:100F88      push    3E807043E    ; int
3000:100F8A      push    347B992CF    ; int
3000:100F8C      call   class17_ctor_from_string_and_date
3000:100F8E      push    eax
3000:100F90      push    edi
3000:100F92      call   [edi+class_11.logger_log]
3000:100F94      add     esp, 20h
3000:100F96      mov     [ebp+var_4.some_obj?], ebx
3000:100F98      cmp     short loc_100FDC3
3000:100F9A      jnz    short loc_100FDC3
3000:100F9C      loc_100FDC3:
3000:100F9E      ; CODE XREF: class18_ctor+35J
3000:100FA0      ; class18_ctor+39J
3000:100FA2      push    esi
3000:100FA4      call   class18_ctor
3000:100FA6      pop     ecx
3000:100FA8      loc_100FDCA:
3000:100FAC      loc_100FDCA:
3000:100FAE      xor     eax, eax
3000:100FB0      jmp    short loc_100FDC3
3000:100FB2      loc_100FDC3:
3000:100FB4      ; CODE XREF: class18_ctor+35J
3000:100FB6      ; class18_ctor+39J
3000:100FB8      push    esi
3000:100FBA      call   sub_10018394
3000:100FBC      pop     ecx
3000:100FBE      jmp    short loc_100FDC3
3000:100FC0      loc_100FDC3:
3000:100FC2      ; CODE XREF: class18_ctor+35J
3000:100FC4      ; class18_ctor+39J
3000:100FC6      push    esi
3000:100FC8      call   sub_10018394
3000:100FCA      pop     ecx
3000:100FCC      jmp    short loc_100FDC3
3000:100FCE      loc_100FDC3:
3000:100FD0      ; CODE XREF: class18_ctor+35J
3000:100FD2      ; class18_ctor+39J
3000:100FD4      push    esi
3000:100FD6      call   sub_10018394
3000:100FD8      pop     ecx
3000:100FDE      jmp    short loc_100FDC3
3000:100FDF      loc_100FDC3:
3000:100FE0      ; CODE XREF: class18_ctor+35J
3000:100FE2      ; class18_ctor+39J
3000:100FE4      push    esi
3000:100FE6      call   sub_10018394
3000:100FE8      pop     ecx
3000:100FEA      jmp    short loc_100FDC3
3000:100FEC      loc_100FDC3:
3000:100FEE      ; CODE XREF: class18_ctor+35J
3000:100FF0      ; class18_ctor+39J
3000:100FF2      push    esi
3000:100FF4      call   sub_10018394
3000:100FF6      pop     ecx
3000:100FF8      jmp    short loc_100FDC3
3000:100FFA      loc_100FDC3:
3000:100FFC      ; CODE XREF: class18_ctor+35J
3000:100FFE      ; class18_ctor+39J
3000:100FF0      test   eax, eax
3000:100FF2      jz     loc_1001B12C
3000:100FF4      mov     esi, [eax]
3000:100FF6      mov     ecx, 08507043h
3000:100FF8      push    1
3000:100FFA      push    0
3000:100FFC      push    0
3000:100FFE      push    5040C561h
3000:101000      mov     ecx, 347B992CF
3000:101002      call   Log
3000:101004      push    eax
3000:101006      push    dword ptr [edi+0Ch]
3000:101008      call   dword ptr [esi]
3000:10100A      cr     dword ptr [edi+8Ch], 0FFFFFFFh
3000:10100C      lea    eax, [edi+10h]
3000:10100E      add     esp, 18h
3000:101010      push    [!bo+lpString2] ; lpString2
3000:101012      push    eax
3000:101014      call   clstrncpyW
3000:101016      mov     ax, [ebp+var_2]
3000:101018      lea    ecx, [ebp+var_1]
3000:10101A      push    ecx
3000:10101C      mov     [edi+90h], ax
3000:10101E      mov     [edi+8], ebx
3000:101020      mov     eax, [ebp+4]
3000:101022      push    edi
3000:101024      offset sub_1001B13C
3000:101026      push    ebx
3000:101028      call   dword ptr [eax+8]
3000:10102A      add     esp, 10h
3000:10102C      test   eax, eax
3000:10102E      jz     short loc_1001B12C
3000:101030      mov     eax, [edi+00h]
3000:101032      mov     ecx, 08507043h
3000:101034      push    1
3000:101036      push    0
3000:101038      push    0
3000:10103A      mov     esi, [eax]
3000:10103C      mov     ecx, 347B992CF
3000:10103E      push    569E08E8h
3000:101040      call   Log
3000:101042      push    eax
3000:101044      push    dword ptr [edi+0Ch]
3000:101046      call   dword ptr [esi]
3000:101048      add     esp, 10h
3000:10104A      cmp     [!bo+var_1], 0
3000:10104C      jz     short loc_1001B12C
3000:10104E      mov     edi, esi
3000:101050      jmp    short loc_1001B135
3000:101052      loc_101B12C:
3000:101054      loc_101B12C:
3000:101056      push    edi
3000:101058      call   sub_10018394
3000:10105A      pop     ecx
3000:10105C      jmp    short loc_1001B135
3000:10105E      loc_101B135:
3000:101060      xor     eax, eax

```

Duqu 2011

Duqu 20

عاقله 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 به دست آورند. 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 به وجود 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. عاقله 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 به دست 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 به دست 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>