بررسی و تحلیل بدافزار پیشرفته

# INDUSTROYER


شبکه گستر
شرکت مهندسی شبکه گستر

عنوان سند: بررسی و تحلیل بدافزار پیشرفته Industroyer
شناسه سند: SPT-A-0137-01
تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر
تاریخ آخرین بازنگری: ۲۷ خرداد ۱۳۹۶

# فهرست مطالب



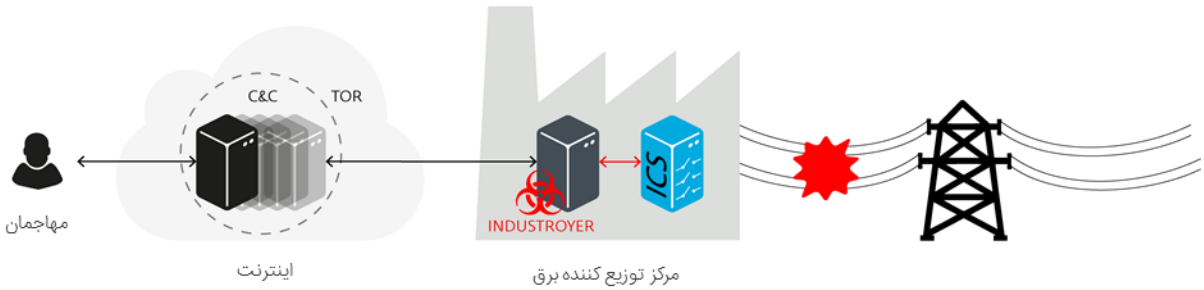
شبکه گستر

# خلاصه مدیریتی

در جریان یکی از حملات سایبری بر ضد اوکراین در سال ۲۰۱۶ میلادی، برق کی‌ف، پایتخت این کشور به مدت یک ساعت قطع شد. قطع برق در اواخر سال ۲۰۱۶ در کشور اوکراین از جهات بسیاری مشابه حمله‌ای بود که در سال قبل از آن منجر به قطع برق نزدیک به ۲۵۰ هزار خانه در چندین شهر این کشور شده بود. بررسی‌های بیشتر منجر به شناسایی بدافزاری موسوم به Industroyer گردید که کالبدشکافی و بررسی دقیق آن ماه‌ها به طول انجامید.

اکنون پس از بررسی‌های مفصل مشخص گردیده که بدافزار مذکور قادر به وارد ساختن آسیب قابل توجه به مراکز توزیع‌کننده برق بوده و حتی ارتقای آن برای هدف قرار دادن دیگر زیرساخت‌های حیاتی نیز امکان‌پذیر است.

با توجه به توانایی Industroyer در کنترل مستقیم سوییچ‌های برق و تجهیزات موسوم به مدارشکن[1]، این بدافزار تهدیدی بسیار خطرناک محسوب می‌شود. Industroyer پودمان‌های ارتباطی صنعتی را که در زیرساخت‌های مراکز توزیع‌کننده برق، سیستم‌های کنترل حمل و نقل و زیرساخت‌های حیاتی دیگر در شبکه‌های تصفیه و انتقال آب و گازرسانی در سراسر جهان مورد استفاده قرار می‌گیرند مورد بهره‌جویی خود قرار می‌دهد.




**شکل ۱: ساختار حمله Industroyer**

سوییچ‌ها و مدارشکن‌های بکار گرفته شده در مراکز توزیع برق معادل دستگاه‌های آنالوگ سنتی هستند. از لحاظ فنی، این تجهیزات می‌توانند به‌نحوی مهندسی و طراحی شوند که توابع متعددی همچون خاموش کردن سیستم توزیع برق، از کاراندازی برخی تجهیزات و حتی اموری به مراتب خطرناک‌تر را در کسری از ثانیه اجرا کنند. بدیهی است که از کاراندازی چنین سیستم‌هایی خود می‌تواند صدمات مستقیم و غیرمستقیم غیر قابل جبرانی را بر روی سرویس‌های حیاتی هر کشور وارد کند.

بخصوص آنکه پودمان‌ها و استانداردهای مورد استفاده در تجهیزات صنعتی دهه‌ها قبل و در دوره‌هایی طراحی شده‌اند که اتصال به شبکه‌های قابل دسترس و اینترنت مفهومی نداشت و به عبارتی دیگر در این پودمان‌های ارتباطی خبری از تنظیمات و سیاست‌های امنیتی نیست.

هر چند Industroyer بدافزاری بسیار پیشرفته و قدرتمند توصیف شده و برخی محققان آن را پس از Stuxnet مخرب‌ترین بدافزار تجهیزات صنعتی معرفی کرده‌اند اما باید در نظر داشت که با وجود اشکالات پودمان‌های رایج فعلی، اجرای حملات مشابه کار چندان دشواری برای مهاجمان حرفه‌ای نخواهد بود.

در این گزارش ساختار و عملکرد بدافزار Industroyer مورد بررسی و تحلیل قرار گرفته است.

[1] Circuit Breaker

# ساختار بدافزار

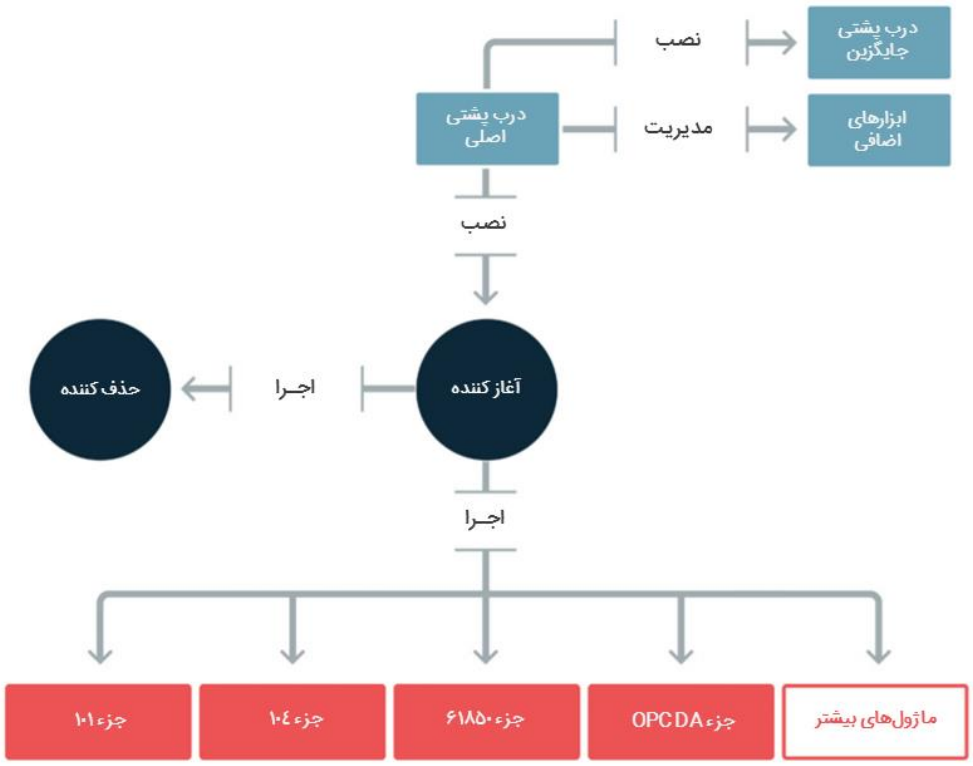
Industroyer بدافزاری با معماری پیمانه‌ای[۲] است. هسته اصلی آن یک درب پشتی[۳] است که مهاجمان از طریق آن حمله را مدیریت می‌کنند. وظیفه این درب پشتی، نصب و کنترل سایر اجزای بدافزار است و با برقراری ارتباط با سرور فرماندهی[۴] فرامین را از مهاجمان دریافت کرده و وضعیت حمله را به آنها گزارش می‌کند.

همچنین این بدافزار حاوی چهار جزء مختلف برای دسترسی یافتن به سوییچ‌ها و مدارشکن‌های مورد استفاده در مراکز توزیع برق است.

هر یک از این چهار جزء پودمان‌های ارتباطی خاصی را هدف قرار می‌دهند. به پودمان‌های مذکور در استانداردهای زیر پرداخته شده است:

- IEC 60870-5-101 معروف به IEC 101
- IEC 60870-5-104 معروف به IEC 104
- IEC 61850
- OLE for Process Control Data Access موسوم به OPC DA

برنامه‌نویسی اجزای مذکور بیانگر توانایی بالا و دانش عمیق نویسندگان Industroyer در زمینه سیستم‌های کنترل صنعتی[۵] است.




شکل ۲: ساختار بدافزار Industroyer

۲ Modular
۳ Backdoor
۴ Command and Control – C&C – C2
۵ Industrial Control System - ICS

بدافزار Industroyer حاوی چند قابلیت دیگر نیز می‌باشد که اهداف آنها مخفی ماندن از دید سیستم‌های امنیتی، ماندگاری بر روی دستگاه و حذف و پاکسازی سوابق و ردپای بدافزار توسط جزیی موسوم به Wiper پس از اتمام ماموریت خود است.

برای مثال، برقراری ارتباط با سرور فرماندهی در بستر سامانه Tor مخفی شده و امکان محدودسازی زمان اجرای آن به ساعات غیرکاری فراهم است. ضمن اینکه با بکارگیری یک درب پشتی جایگزین – در ظاهر برنامه Notepad – حتی در صورت شناسایی و از کار افتادن درب پشتی اصلی دسترسی مهاجمان به دستگاه آلوده شده همچنان برقرار باقی خواهد ماند.

جزء Wiper آن نیز به نحوی طراحی شده که کلیدهای اصلی محضرخانه[۶] را حذف کرده و برخی فایل‌ها را رونویسی کند تا سیستم قادر به راه‌اندازی مجدد نبوده و فرآیند بازگردانی دستگاه آلوده شده با دشواری و در زمان طولانی‌تر قابل انجام باشد.

از دیگر قابلیت‌های این بدافزار پیشرفته می‌توان به توانایی آن در پویش شبکه و شناسایی دستگاه‌های مشابه اشاره کرد. مهاجمان بجای استفاده از ابزارهای آماده خود اقدام به ساخت ابزاری ویژه برای این منظور نموده‌اند.

در نهایت اینکه بدافزار Industroyer قادر است با بهره‌جویی از یک آسیب‌پذیری با شناسه CVE-2015-5374 در تجهیزات Siemens SIPROTEC حملات از کاراندازی سرویس را بر ضد آنها اجرا کرده و سبب از مدار خارج شدن آنها شود.

## درب پشتی اصلی

همانطور که اشاره شد مهاجمان با استفاده از یک درب پشتی سایر اجزای بدافزار را کنترل می‌کنند. مشابه بسیاری از درب‌های پشتی، این جزء از بدافزار Industroyer نیز با استفاده از پودمان امن HTTPS با سرور فرماندهی خود ارتباط برقرار کرده و فرامین را از سمت مهاجمان دریافت می‌کند.

در تمام نمونه‌هایی که مورد تجزیه و تحلیل قرار گرفته‌اند یک نشانی پراکسی به چشم می‌خورد. بنابراین واضح است که این درب پشتی برای یک سازمان خاص طراحی شده است. این نکته نیز قابل توجه است که اکثر سرورهای فرماندهی این بدافزار تنها در سامانه TOR قابل دسترس هستند.

یکی از ویژگی‌های جالب این جزء از بدافزار، امکان تعیین یک ساعت خاص در روز برای فعال شدن درب پشتی توسط مهاجمان است. به عنوان مثال، مهاجمان از این طریق می‌توانند با اعمال تنظیمات لازم سبب برقراری ارتباط درب پشتی با سرور فرماندهی تنها در ساعات غیر کاری شوند. بدیهی است چنین کاری می‌تواند موجب تاخیر در شناسایی بدافزار با استفاده از روش‌هایی نظیر بررسی ترافیک شبکه توسط راهبران امنیت در شبکه سازمان هدف قرار گرفته شده شود. با این حال در تمامی نمونه‌های بررسی شده ارتباطات درب پشتی ۲۴ ساعته فعال بوده است.

[۶] Registry

```
int main_loop()
{
  struct _SYSTEMTIME SystemTime; // [esp+0h] [ebp-14h]@4
  DWORD dwMilliseconds; // [esp+10h] [ebp-4h]@2

  SetLastError(0);
  if ( GetLastError() != ERROR_ALREADY_EXISTS )
  {
    dwMilliseconds = 5000;
    SetUnhandledExceptionFilter(TopLevelExceptionFilter);
    if ( !GetSystemMetrics(SM_CLEANBOOT) )
    {
      if ( create_imapi_handle() )
      {
        while ( 1 )
        {
          do
          {
            Sleep(dwMilliseconds);
            GetLocalTime(&SystemTime);
          }
          while ( SystemTime.wHour >= 24u );
          c2_connect_and_execute_cmd(&dwMilliseconds);
        }
      }
    }
  }
  return 0;
}
```

شکل ۳: کد بررسی کننده زمان در درب پشتی

زمانی که ارتباط با سرور فرماندهی برقرار شود، درب پشتی اقدام به ارسال اطلاعات زیر با استفاده از روش POST می‌کند:

- رشته شناسه منحصر به فرد جهانی[۷] که از اجرای تابع GetCurrentHwProfile حاصل شده است.
- نگارش بدافزار (1.1e)
- شناسه توکار[۸] بدافزار
- نتیجه تمامی دستوراتی که پیش‌تر دریافت شده‌اند.

مهاجمان از شناسه توکار به منظور مشخص کردن سیستم‌های آلوده استفاده می‌کنند. با تجزیه و تحلیل نمونه‌های شناسایی شده، شناسه‌های زیر بدست آمده است:

- DEF
- DEF-C
- DEF-WS
- DEF-EP
- DC-2-TEMP
- DC-2
- CES-McA-TEMP
- CES
- SRV_WSUS
- SRV_DC-2
- SCE-WSUS01

[۷] Globally Unique Identifier - GUID
[۸] hardcoded ID

جدول ۱، دستورات پشتیبانی شده توسط درب پشتی اصلی را نمایش می‌دهد.

| شناسه دستور | شرح |
|---|---|
| 0 | اجرای پروسه |
| 1 | اجرای پروسه تحت حساب کاربری یک کاربر خاص. اطلاعات اصالت‌سنجی[۹] حساب کاربری توسط مهاجمان فراهم می‌شود. |
| 2 | دریافت فایل از سرور فرماندهی |
| 3 | کپی فایل |
| 4 | اجرای یک دستور پوسته‌ای[۱۰] |
| 5 | اجرای یک دستور پوسته‌ای تحت یک حساب کاربری خاص. اصالت‌سنجی حساب کاربری توسط مهاجمان فراهم می‌شود. |
| 6 | خروج |
| 7 | متوقف کردن سرویس |
| 8 | متوقف کردن سرویس تحت یک حساب کاربری خاص. نام کاربری و گذرواژه حساب کاربری توسط مهاجمان فراهم می‌شود. |
| 9 | راه‌اندازی سرویس تحت یک حساب کاربری خاص. نام کاربری و گذرواژه حساب کاربری توسط مهاجمان فراهم می‌شود. |
| 10 | جایگزینی مقدار "Image Path" موجود در محضرخانه برای یک سرویس |

جدول ۱: دستورات پشتیبانی شده توسط درب پشتی اصلی

زمانی که مهاجمان موفق به دست یافتن به سطح دسترسی Administrator بر روی کامپیوتر شوند، قادر خواهند بود تا درب پشتی نصب شده را جهت دسترسی بیشتر و اجرا به عنوان یک سرویس Windows ارتقا دهند. برای انجام این کار، مسیر ImagePath یک سرویس غیر ضروری Windows در محضرخانه با مسیر فایل باینری درب پشتی جایگزین می‌شود.

پس از آن درب پشتی اصلی با دو تغییر کوچک به عنوان یک سرویس Windows فعالیت خواهد کرد؛ نخست، نگارش درب پشتی از 1.1e به 1.1s تغییر می‌یابد. تغییر دوم، مبهم‌سازی[۱۱] کدهاست. کدهای این نگارش از درب پشتی با دستورات اسمبلی زائد ادغام شده است. (شکل ۴)

```
.text:00403FD2 main_func proc near               ; CODE XREF: WinMain(x,x,x,x)+14↑p
.text:00403FD2                                   ; .text:004038C4↑p
.text:00403FD2         call    $+5
.text:00403FD7
.text:00403FD7 loc_403FD7:                       ; CODE XREF: main_func+57↓j
.text:00403FD7                                   ; main_func+5F↓j
.text:00403FD7         add     esp, 4
.text:00403FDA         push    ebp               ; lpOverlapped
.text:00403FDB         mov     ebp, esp
.text:00403FDD         cmp     edx, 142F9F9Ah
.text:00403FE3         jz      short loc_404023
.text:00403FE5         push    ecx
.text:00403FE6         push    ecx
.text:00403FE7         mov     eax, [ebp+10h]
.text:00403FEA         mov     dword_416190, eax
.text:00403FEF         mov     eax, [ebp+8]
.text:00403FF2         mov     dword_416194, eax
.text:00403FF7         mov     eax, [ebp+0Ch]
.text:00403FFA         cmp     edx, 0B5B93EF3h
.text:00404000         jz      short loc_404023
.text:00404002         mov     lpOverlapped, eax
.text:00404007         mov     [ebp-8], eax
.text:0040400A         lea     eax, [ebp-8]
.text:0040400D         push    eax               ; lpServiceStartTable
.text:0040400E         mov     dword ptr [ebp-4], offset ServiceMain
.text:00404015         call    ds:StartServiceCtrlDispatcherW
.text:0040401B         xor     al, al
.text:0040401D         mov     esp, ebp
.text:0040401F         pop     ebp
.text:00404020         retn
```

شکل ۴: کد مبهم‌سازی شده درب پشتی اصلی که در قالب یک سرویس عمل می‌کند

[۹] Credential
[۱۰] Shell Command
[۱۱] Obfuscation

## درب پشـتـی جایـگـزین

درب پشتی دوم در Industroyer، مکانیزمی جایگزین است که به مهاجمان اجازه می‌دهد حتی در صورت غیرفعال شدن درب پشتی اصلی – به دلایلی نظیر شناسایی توسط ضدبدافزار – همچنان دسترسی به دستگاه قربانی را برقرار داشته باشند.

این درب پشتی نسخه‌ای اسب تروا[۱۲] شده از برنامه Windows Notepad است. این نسخه همانند نسخه اصلی کار می‌کند؛ با این تفاوت که نویسندگان بدافزار کدهای آلوده را به آن تزریق کرده‌اند و با هر بار باز شدن برنامه این کدهای مخرب نیز به همراه آن اجرا می‌شوند. هنگامی که مهاجمان دسترسی Administrator را بدست آوردند، می‌توانند برنامه آلوده خود را جایگزین Notepad اصلی نمایند.

کدهای آلوده تزریق شده به شدت مبهم سازی شده‌اند. با رمزگشایی و اجرا، این جزء به سروری فرماندهی متصل می‌شود که نشانی آن متفاوت از سرور مورد استفاده درب پشتی اصلی است. این کدها، کدهای پوسته‌ای هستند که مستقیماً در حافظه بارگذاری و اجرا می‌شوند. علاوه بر آن، کد تزریق شده کد Notepad اصلی Windows را که در انتهای فایل ذخیره شده نیز رمزگشایی و سپس اجرا می‌کند که در نتیجه آن عملکرد برنامه Notepad برای کاربر همچنان حفظ خواهد شد.

```
.text:01004AD5    lea     eax, [ebp+var_50]
.text:01004AD8    push    eax
.text:01004AD9    lea     eax, [ebp+h]
.text:01004ADC    push    eax
.text:01004ADD    push    0B0h
.text:01004AE2    push    hWnd
.text:01004AE8    mov     stru_100A680.lStructSize, 58h
.text:01004AF2    mov     stru_100A680.hwndOwner, edx
.text:01004AF8    mov     stru_100A680.nMaxFile, 104h
.text:01004B02    mov     stru_100A500.lStructSize, 28h
.text:01004B0C    mov     stru_100A500.hwndOwner, edx
.text:01004B12    call    esi ; SendMessageW
.text:01004B14    push    [ebp+var_50]
.text:01004B17    push    [ebp+h]
.text:01004B1A    push    0B1h
.text:01004B1F    push    hWnd
.text:01004B25    call    esi ; SendMessageW
.text:01004B27    push    ebx
.text:01004B28    push    ebx
.text:01004B29    push    0B7h
.text:01004B2E    push    hWnd
.text:01004B34    call    esi ; SendMessageW
.text:01004B36    push    ebx
.text:01004B37    call    ds:GetKeyboardLayout
.text:01004B3D    and     ax, 3FFh
.text:01004B41    cmp     ax, 11h
.text:01004B45    jnz     short loc_1004B58
.text:01004B47    push    1
.text:01004B49    push    1
.text:01004B4B    push    0D8h
.text:01004B50    push    hWnd
.text:01004B56    call    esi ; SendMessageW
```

```
.text:01004AD5    lea     eax, [ebp+var_50]
.text:01004AD8    push    eax
.text:01004AD9    lea     eax, [ebp+h]
.text:01004ADC    push    eax
.text:01004ADD    push    0B0h
.text:01004AE2    push    hWnd
.text:01004AE8    mov     stru_100A680.lStructSize, 58h
.text:01004AF2    mov     stru_100A680.hwndOwner, edx
.text:01004AF8    mov     stru_100A680.nMaxFile, 104h
.text:01004B02    mov     stru_100A500.lStructSize, 28h
.text:01004B0C    mov     stru_100A500.hwndOwner, edx
.text:01004B12    call    esi ; SendMessageW
.text:01004B14    pusha
.text:01004B15    pushf
.text:01004B16    neg     ebx
.text:01004B18    shr     eax, 1
.text:01004B1B    dec     ebx
.text:01004B1C    mov     eax, 17B200AFh
.text:01004B21    mov     edi, 71CFC28h
.text:01004B26    or      edi, dword_10095C7
.text:01004B2C    xor     esi, 1C779E91h
.text:01004B32    xor     eax, eax
.text:01004B34    dec     edi
.text:01004B35    rol     esi, 5
.text:01004B38    and     esi, edi
.text:01004B3A    and     esi, edi
.text:01004B3C    rol     edx, 6
.text:01004B3F    neg     eax
.text:01004B41    xor     esi, eax
.text:01004B43    neg     ebx
.text:01004B45    shr     ebx, 5
.text:01004B48    mov     ecx, 5E95422h
```

شکل ۵: مقایسه بین کد Notepad اصلی (سمت چپ) و کد درب پشتی جایگزین (سمت راست)

## آغـاز کـنـنـده

جزء آغاز کننده Industroyer موسوم به Launcher یک فایل اجرایی مجزا است که اجرا کننده جزء Wiper و دیگر اجزای مخرب بدافزار است.

جزء آغاز کننده شامل تاریخ و زمانی خاص است. نمونه‌های بررسی شده شامل دو تاریخ ۱۷ دسامبر ۲۰۱۶ – مطابق با ۲۷ آذر ۱۳۹۵ – و ۲۰ دسامبر ۲۰۱۶ – مطابق با ۳۰ آذر ۱۳۹۵ – هستند. هنگامی که زمان یکی از تاریخ‌ها فرا برسد، این جزء دو Threat ایجاد می‌کند.

[۱۲] Trojan

Thread اول سعی می‌کند DLL مخرب را بارگذاری کند و Thread دوم یک تا دو ساعت (بسته به نگارش بخش آغازکننده) منتظر مانده و سپس سعی در بارگذاری جزء Wiper می‌کند. اولویت هر دو Thread بر روی THREAD_PRIORITY_HIGHEST تنظیم شده است. این بدان معناست که این دو Thread می‌توانند بیشتر از حد معمول از منابع CPU در بستر سیستم عامل استفاده کنند.

نام DLL آلوده توسط مهاجمان از طریق اجرای یکی از دستورات پوسته موجود در درب پشتی اصلی تعیین می‌شود. دستورات خط فرمان انتظار می‌رود در قالب‌های زیر باشند:

```
%LAUNCHER%.exe %WORKING_DIRECTORY% %PAYLOAD%.dll %CONFIGURATION%.ini
```

هر کدام از پارامترها در خط فرمان نشان‌دهنده موارد زیر است:

- %LAUNCHER%.exe که نام جزء آغاز کننده است.
- %WORKING_DIRECTORY% که به مسیر پوشه‌ای که DLL آلوده و پیکربندی‌ها در آن ذخیره خواهند شد اشاره می‌کند.
- %PAYLOAD%.dll به نام DLL آلوده اشاره می‌کند.
- %CONFIGURATION%.ini، فایلی است که داده‌های پیکربندی یک برنامه مشخص آلوده، در آن ذخیره می‌شود. مسیر این فایل توسط جزء آغاز کننده در اختیار DLL آلوده قرار می‌گیرد.

بخش برنامه آلوده و Wiper فایل‌های DLL استاندارد سیستم عامل Windows هستند که توسط بخش آغاز کننده جهت ساخت یک تابع به نام Crash در حافظه بارگذاری می‌شوند.

```
;
; Export directory for Crash101.dll
;
                dd 0                    ; Characteristics
                dd 5855F8EDh            ; TimeDateStamp: Sun Dec 18 02:48:13 2016
                dw 0                    ; MajorVersion
                dw 0                    ; MinorVersion
                dd rva aCrash101_dll    ; Name
                dd 1                    ; Base
                dd 1                    ; NumberOfFunctions
                dd 1                    ; NumberOfNames
                dd rva off_100355F8     ; AddressOfFunctions
                dd rva off_100355FC     ; AddressOfNames
                dd rva word_10035600    ; AddressOfNameOrdinals
;
; Export Address Table for Crash101.dll
;
off_100355F8    dd rva Crash            ; DATA XREF: .rdata:100355EC↑o
;
; Export Names Table for Crash101.dll
;
off_100355FC    dd rva aCrash           ; DATA XREF: .rdata:100355F0↑o
                                        ; "Crash"
;
; Export Ordinals Table for Crash101.dll
;
word_10035600   dw 0                    ; DATA XREF: .rdata:100355F4↑o
aCrash101_dll   db 'Crash101.dll',0     ; DATA XREF: .rdata:100355DC↑o
aCrash          db 'Crash',0            ; DATA XREF: .rdata:off_100355FC↑o
```

شکل ۶: تابع Crash

## جـزء ۱۰۱

نام فایل این جزء 101.dll است که به نظر می‌رسد بر گرفته از IEC 101 باشد. IEC 101 یک استاندارد بین‌المللی است که در آن به پودمان مربوط به نظارت و کنترل سیستم‌های صنعت برق پرداخته شده است. این پودمان برای برقراری ارتباط بین سیستم‌های کنترل صنعتی و ترمینال ناظر مورد استفاده قرار می‌گیرد. ارتباطات از طریق اتصال سریال انجام می‌شود.

بمحض اجرا شدن، جزء 101، تنظیمات پیکربندی را از فایل INI خود دریافت می‌کند. این تنظیمات شامل ورودی‌های زیر است:

- نام پروسه
- نام‌های دستگاه Windows (معمولا درگاه‌های COM)
- بازه Information Object Address – به اختصار IOA
- مقادیر ابتدا و انتهای IOA برای عدد مشخصی از بازه IOA؛ IOA عددی است که عنصر داده‌ای[۱۳] خاصی را در دستگاه مشخص می‌کند.

شکل ۷ فایل پیکربندی جزء 101 را که با دو بازه IOA، ۱۵-۱۰ و ۲۰-۲۵ تعریف شده نشان می‌دهد.

```
101_config.ini
1  real_process.exe
2  COM1
3  1---
4  COM2
5  2---
6  COM3
7  3---
8  2
9  10
10 15
11 20
12 25
```

**شکل ۷: یک نمونه از فایل پیکربندی DLL آلوده 101**

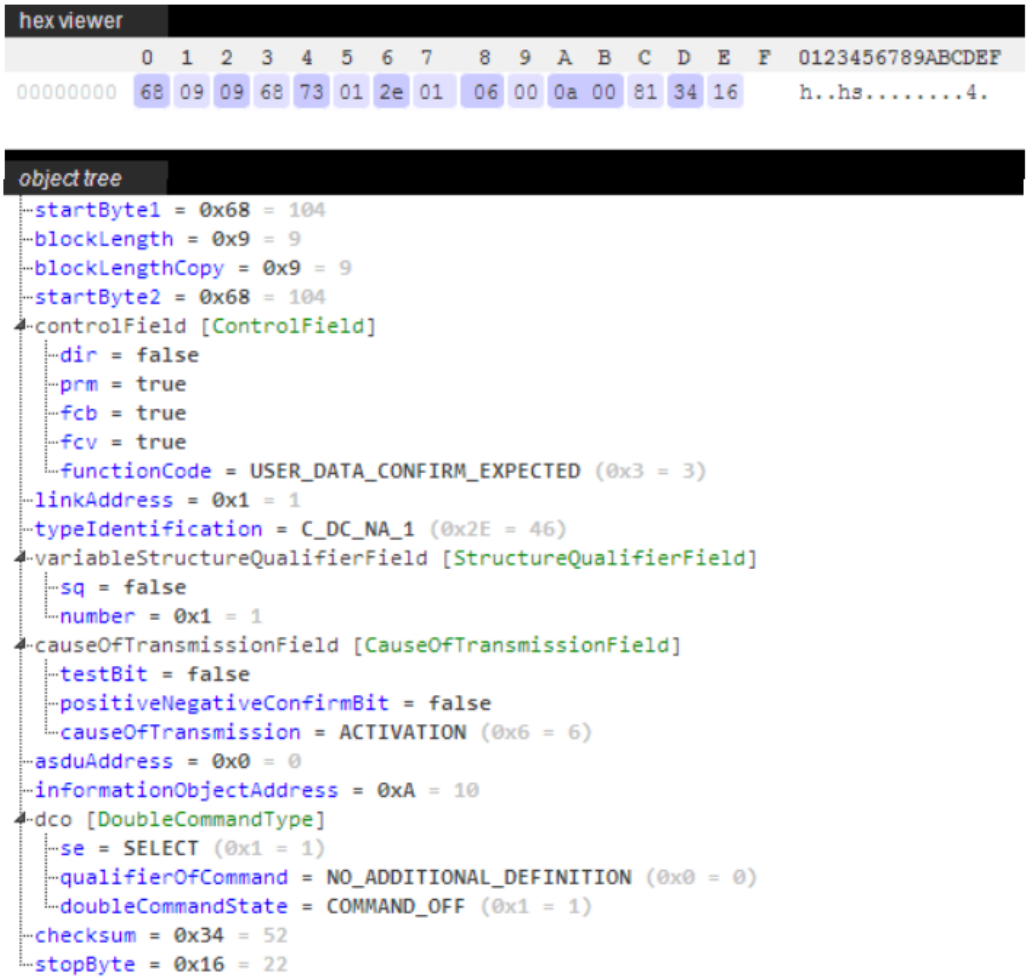
نام پروسه‌ای که در فایل پیکربندی وجود دارد متعلق به برنامه‌ای است که گمان می‌رود توسط مهاجمان بر روی سیستم قربانی اجرا می‌شود. این برنامه به احتمال زیاد ابزاری است که از آن برای ارتباط با ترمینال ناظر از طریق اتصال سریال استفاده می‌شود. جزء 101 سعی می‌کند پروسه مشخصی را خاتمه داده و شروع به برقراری ارتباط با دستگاه تعریف شده از طریق توابع API زیر در سیستم عامل Windows کند:

- CreateFile
- WriteFile
- ReadFile

از اولین درگاه COM موجود در فایل پیکربندی به منظور برقراری ارتباط استفاده شده و دو درگاه دیگر برای جلوگیری از دسترسی سایر پروسه‌ها به آنها باز می‌شوند. به این ترتیب، جزء 101 می‌تواند کنترل ترمینال ناظر را در اختیار بگیرد.

[۱۳] Data Element

این جزء تمامی IOAهای تعریف شده در بازه IOA را تکرار می‌کند. برای هر IOA دو بسته "select and execute"، یکی با یک فرمان C_SC_NA_1 و دیگری با دو فرمان C_DC_NA_1 ایجاد گردیده و سپس به ترمینال ناظر ارسال می‌شود. هدف اصلی این جزء برای تغییر وضعیت روشن/خاموش فرامین IOA است. به طور مشخص، جزء 101 شامل سه مرحله است؛ در مرحله اول این بخش سعی می‌کند وضعیت IOA را در وضعیت خاموش (غیرفعال) قرار دهد. در مرحله دوم تلاش می‌کند وضعیت IOAها را به روشن (فعال) تغییر دهد و در مرحله سوم و پایانی این بخش می‌کوشد تا وضعیت IOA را در حالت خاموش (غیرفعال) قرار دهد.

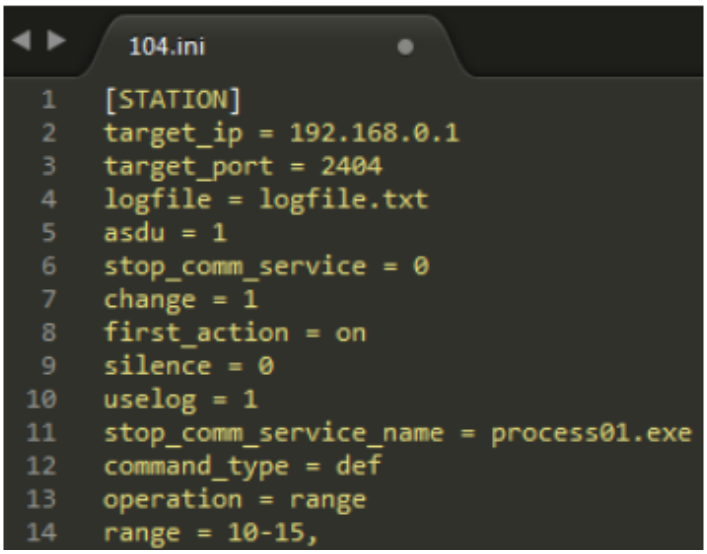



شکل ۸: نمونه‌ای از یک بسته جزء 101

## جـزء ۱۰۴

فایل این بخش مخرب 104.dll نام دارد که برگرفته از عنوان استاندارد IEC 104 است. IEC 104 گسترش یافته استاندارد IEC 101 است که در آن به نحوه انتقال اطلاعات از طریق پودمان TCP/IP پرداخته می‌شود.

با توجه به ماهیت قابل پیکربندی آن، این جزء می‌تواند توسط مهاجمان برای بسترهای مختلف سفارشی شود. شکل ۹ فایل پیکربندی این جزء را نمایش می‌دهد.




**شکل ۹: فایل پیکربندی DLL آلوده 104**

در زمان اجرا، DLL آلوده 104 اقدام به خواندن فایل پیکربندی خود می‌کند. همانطور که ذکر شد، مسیر فایل پیکربندی توسط جزء آغاز کننده تعیین می‌شود.

فایل پیکربندی شامل بخشی با عنوان STATION است که در ادامه به ویژگی‌هایی که جزء 104 جهت فعال شدن به آنها نیاز دارد، اشاره شده است. فایل پیکربندی شامل چندین ورودی STATION است. جدول ۲، ویژگی‌های آنها را نمایش می‌دهد.

| ویژگی | مقدار مورد انتظار | هدف |
|---|---|---|
| target_ip | نشانی IP | نشانی IP که از آن برای برقراری ارتباط با استفاده از پودمان استاندارد IEC 104 استفاده می‌شود. |
| target_port | شماره درگاه | شماره درگاه برای برقراری ارتباط |
| Uselog | 1 یا 0 | فعال یا غیرفعال نمودن ذخیره لاگ‌ها در فایل |
| Logfile | نام فایل | مشخص کردن نام فایلی که لاگ‌ها در آن ذخیره می‌شوند - در صورتی که ذخیره لاگ فعال باشد. |
| stop_comm_service | 1 یا 0 | فعال یا غیر فعال نمودن متوقف کردن پروسه |
| stop_comm_service_name | نام پروسه | معرفی نام پروسه‌ای که باید به آن خاتمه داد. |
| timeout | زمان وقفه به میلی ثانیه | مشخص کردن زمان وقفه میان ارسال و دریافت فراخوانی‌ها. مقدار پیش‌فرض ۱۵،۰۰۰ میلی ثانیه است. |
| socket_timeout | زمان وقفه به میلی ثانیه | مشخص کردن زمان وقفه دریافت. مقدار پیش‌فرض ۱۵،۰۰۰ میلی ثانیه است. |
| silence | 1 یا 0 | فعال یا غیرفعال نمودن خروجی کنسول |
| asdu | عدد | مشخص کردن نشانی ADSU (Application Service Data Unit) که با عنوان سکتور نیز شناخته می‌شود. |
| first_action | روشن یا خاموش | مشخص کردن مقدار پارامتر بسته ASDU در اولین تکرار |
| change | 1 یا 0 | مشخص کردن مقدر پارامتر که در بسته ASDU در زمان تکرار باید معکوس شود. |
| command_type | def, short, long, persist | مشخص کردن مدت زمان پالس برای کنترل دستور |
| operation | بازه، توالی یا تغییر مکان | مشخص کردن نوع تکرار IOAها |
| range | قالب مشخصی از IOA ها | مشخص کردن بازه‌ای از IOAها |

| ویژگی | مقدار مورد انتظار | هدف |
|---|---|---|
| sequence | قالب مشخصی از IOA ها | مشخص کردن بازه‌ای از IOAها |
| shift | قالب مشخصی از IOA ها | مشخص کردن بازه‌ای از IOAها |

جدول ۲: ویژگی‌های موجود در فایل پیکربندی جزء 104

هنگامی که فایل پیکربندی خوانده می‌شود، جزء 104 یک Thread برای هر بخش STATION که در فایل پیکربندی تعریف شده ایجاد می‌کند. در هر Thread، جزء 104 سعی می‌کند با نشانی IP تعیین شده از طریق پودمان IEC 104 ارتباط برقرار کند. قبل از برقراری تماس، جزء 104 تلاش می‌کند به پروسه‌هایی که مسئول برقراری ارتباط از طریق پودمان IEC 104 هستند، خاتمه دهد. این امر در صورتی انجام می‌شود که در فایل پیکربندی ویژگی stop_comm_service تعریف شده باشد. به صورت پیش‌فرض، جزء 104 پروسه‌ای با نام D2MultiCommService.exe و پروسه‌هایی که نام آنها در فایل پیکربندی مشخص شده است را خاتمه می‌دهد.

ایده اصلی جزء 104 تقریبا ساده است. این جزء به نشانی IP تعیین شده متصل شده و سپس شروع به ارسال بسته‌ها با نشانی ASDU که در فایل پیکربندی تعریف شده‌اند، می‌کند. هدف این ارتباط تعامل با یک IOA از نوع تک فرمانی است.

در فایل پیکربندی، مهاجمان می‌توانند ویژگی operation را برای مشخص کردن دقیق اینکه IOA از نوع تک فرمانی چگونه باید تکرار شود، تعیین کنند.

اولین حالت operation، range است که مهاجمان از آن به منظور یافتن IOAهای ممکن بر روی سیستم هدف استفاده می‌کنند. از آنجا که در پودمان استاندارد IEC 104 متدی برای دریافت چنین اطلاعاتی تعریف نشده مهاجمان خود اقدام به پیاده‌سازی این روش کرده‌اند.

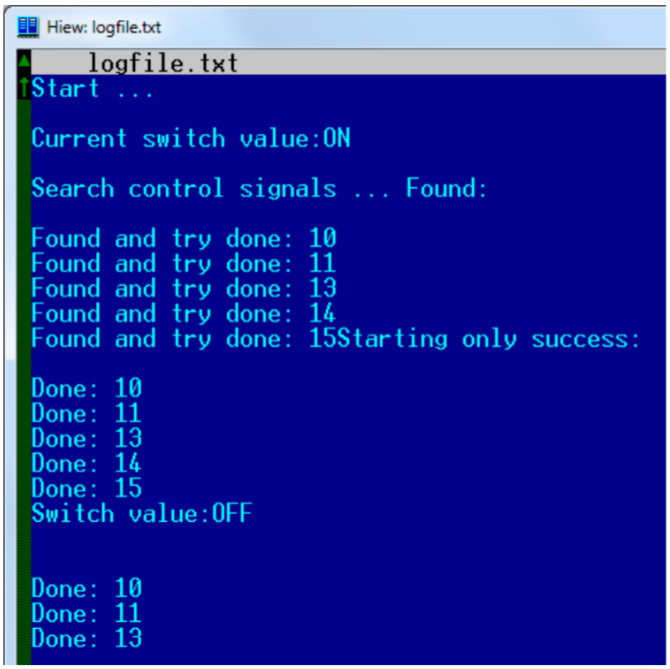
حالت range شامل دو مرحله است. در اولین مرحله، بمحض حاصل شدن محدوده IOAها بر اساس فایل تنظیمات، جزء 104 اقدام به برقراری ارتباط با نشانی IP هدف قرار گرفته شده کرده و شروع به تکرار بر اساس IOAهای تعیین شده می‌کند. در هر IOA، جزء 104 اقدام به ارسال بسته‌های "select and execute" می‌کند تا وضعیت را تغییر داده و اطمینان حاصل کند که IOA متعلق به یک نوع تک فرمان است.

```
▷ Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
▷ Transmission Control Protocol, Src Port: 2404, Dst Port: 49168, Seq: 39, Ack: 45, Len: 16
▷ IEC 60870-5-104-Apci: -> I (2,2)
◢ IEC 60870-5-104-Asdu: ASDU=1 C_SC_NA_1 ActTerm IOA=10 'single command'
    TypeId: C_SC_NA_1 (45)
    0... .... = SQ: False
    .000 0001 = NumIx: 1
    ..00 1010 = CauseTx: ActTerm (10)
    .0.. .... = Negative: False
    0... .... = Test: False
    OA: 0
    Addr: 1
  ◢ IOA: 10
      IOA: 10
    ◢ SCO: 0x01
          .... ...1 = ON/OFF: On
          .000 00.. = QU: No pulse defined (0)
          0... .... = S/E: Execute
```

شکل ۱۰: نمونه ای از بسته شبکه ای جزء 104

بمحض تکرار تمامی IOAهای تعیین شده در محدوده مورد نظر، جزء 104 وارد دومین مرحله از range می‌شود. در صورت فعال بودن لاگ‌گیری، این جزء عبارت "Starting only success" را در لاگ ثبت می‌کند. باقی این مرحله حلقه‌ای بی‌پایان[۱۴] است که از IOAهای شناسایی شده تک فرمان استفاده می‌کند. در حلقه، جزء 104 دائماً بسته‌های "select and execute" را ارسال می‌کند. علاوه بر آن چنانچه تغییر وضعیت نیز تعریف شده باشد این جزء اقدام به روشن / خاموش کردن وضعیت در بین مراحل حلقه می‌کند.

شکل ۱۱ نمونه لاگی را نمایش می‌دهد که توسط جزء 104 تولید شده است.



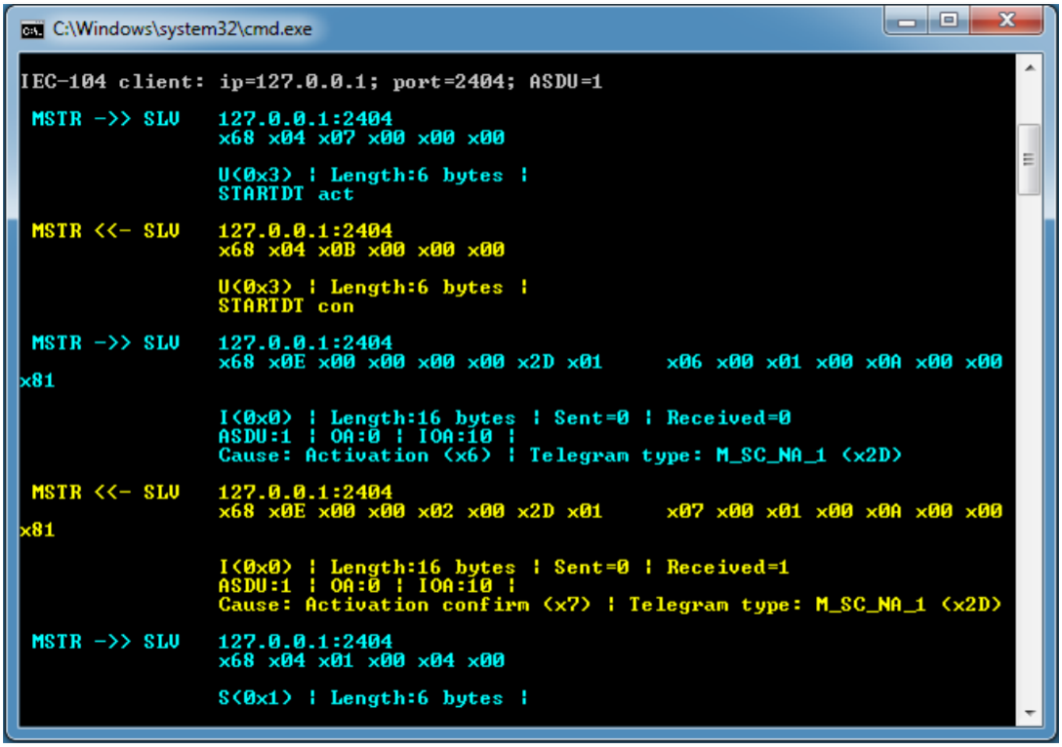

**شکل ۱۱: نمونه ای از لاگ جزء 104**

operation دوم، shift نام دارد که عملکردی مشابه range دارد. مهاجمان در فایل تنظیمات بازه‌ای از IOAها و مقادیر shift را تعریف می‌کنند. بمحض فعال شدن جزء 104 این حالت نیز مشابه حالت range مراحل خود را پیش می‌برد. اما با تکرار تمامی IOAها در محدوده تعیین شده، این حالت شروع به تکرار در بازه‌ای جدید می‌کند. بازه جدید بر اساس اضافه شدن مقادیر shift به مقادیر پیش‌فرض حاصل می‌شود.

حالت سوم operation، squaence نام دارد. مهاجمان می‌توانند از این حالت در هنگامی که از مقادیر تمامی IOAهای تک‌فرمانی پشتیبانی شده توسط دستگاه متصل شده آگاهی دارند استفاده کنند. در این حالت در یک حلقه بی‌پایان بسته‌های "select and execute" به IOAهای تعریف شده در فایل پیکربندی ارسال می‌شود.

علاوه بر قابلیت ثبت لاگ، جزء 104 قادر است اطلاعاتی در خصوص دیباگ که نمونه‌ای از آن در شکل ۱۲ نمایش داده شده است تولید کند.

[۱۴] Infinite Loop




شکل ۱۲: خروجی دیباگ جزء 104

## جـزء ٦١٨٥٠

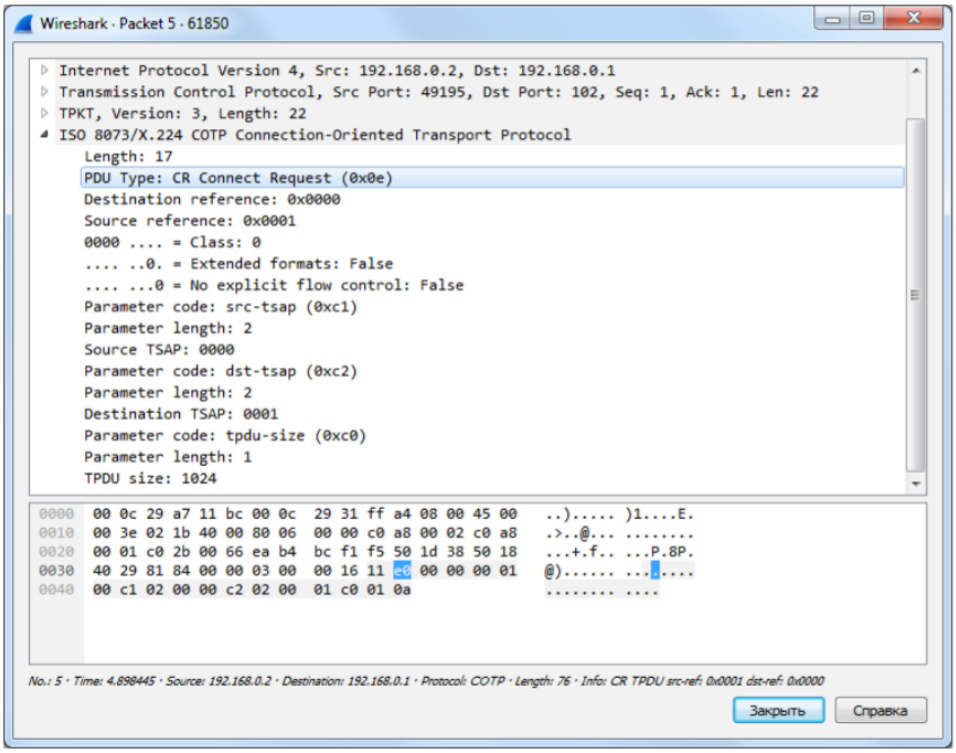
جزء 61850 به‌عنوان یک ابزار مخرب مستقل فعالیت می‌کند. این جزء متشکل از دو فایل 61850.exe و 61850.dll است. نامگذاری آن نیز احتمالاً از استاندارد IEC 61850 برگرفته شده است. این استاندارد پودمان ارتباطی میان دستگاه‌هایی که حفاظت، اتوماسیون، اندازه‌گیری، رصد کردن و کنترل سیستم‌های توزیع برق را بر عهده دارند تعریف می‌کند. در حالی که این پودمان مبانی پیچیده و مفصلی را شامل می‌شود، جزء 61850 بدافزار Industroyer تنها به بخش کوچکی از آن برای رسیدن به اهداف مخرب خود پرداخته است.

بمحض اجرا شدن، جزء 61850 اقدام به خواندن فایل تنظیمات در مسیر تعیین شده از سوی آغاز کننده می‌کند. انتظار می‌رود که فایل تنظیمات حاوی فهرستی از نشانی‌های IP دستگاه‌هایی باشد که قابلیت برقراری ارتباط از طریق پودمان‌های شرح داده شده در استاندارد IEC 61850 را در خود دارند.

جزء 61850 نشانی‌های تخصیص داده شده به کارت‌های شبکه را شناسایی و فهرستی از زیرشبکه‌های مرتبط را تولید می‌کند. در ادامه تلاش می‌کند تا از طریق درگاه 102 به آنها متصل شود.

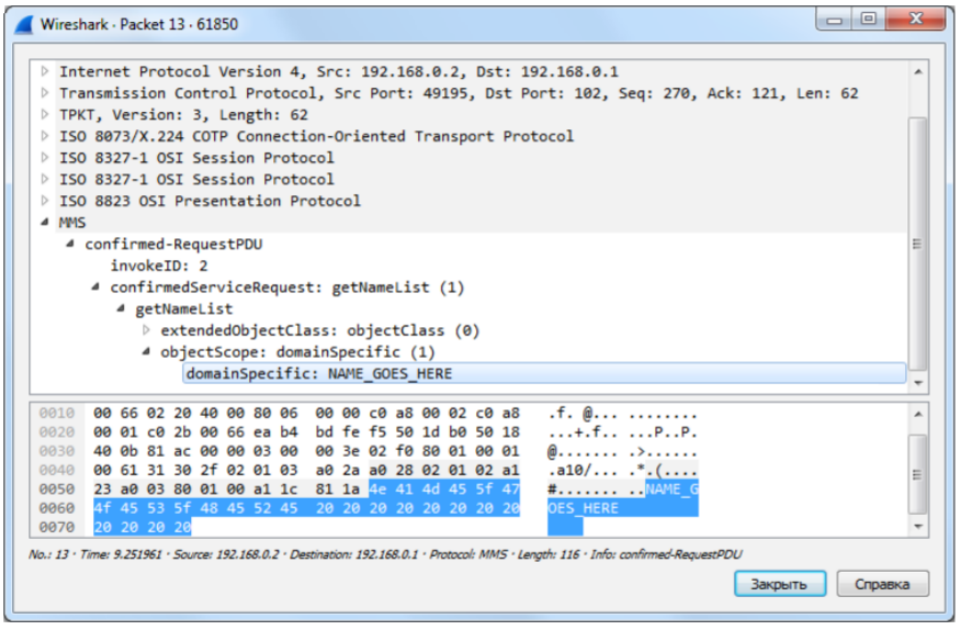
چنانچه فایل تنظیمات نیز در دسترس باشد، علاوه بر تلاش برای برقراری ارتباط با نشانی‌های یافت شده نسبت به برقراری ارتباط با نشانی‌های IP تعیین شده در فایل تنظیمات نیز اقدام می‌کند.

بمحض برقراری ارتباط با دستگاه هدف قرار گرفته شده بسته درخواست Connection Request در قالب Connection Oriented Transport Protocol ارسال می‌شود. (شکل ۱۳)




شکل ۱۳: نمونه‌ای از بسته درخواست در جزء 61850

در صورت دریافت پاسخ صحیح از سوی دستگاه هدف قرار گرفته شده، جزء 61850 اقدام به ارسال بسته InitiateRequest در قالب Manufacturing Message Specification – به اختصار MMS – خواهد کرد. چنانچه پاسخ مورد انتظار دریافت شود، این جزء ارسال درخواست‌ها را با getNameList ادامه خواهد داد که در نتیجه آن فهرستی از نام‌های استفاده شده در قالب Virtual Manufacturing Device ایجاد خواهد شد.




شکل ۱۴: نمونه ای از بسته درخواست MMS getNameList در جزء 61850

در ادامه این جزء داده‌های دریافت شده را بررسی کرده و آنها را برای متغیرهایی بر اساس شرایط زیر مورد تجسس قرار می‌دهد:

- CSW، CF، Pos و Model
- CSW، ST، Pos و stVal
- CSW، CO، Pos، Oper اما نه $T
- CSW، CO، Pos، SBO اما نه $T

رشته CSW به نقاط منطقی اشاره دارد که از آنها برای کنترل مدارشکن‌ها و سوییچ‌ها استفاده می‌شود.

برای متغیرهایی که شامل Model یا stVal هستند 61850 درخواست MMS read اضافی می‌فرستد. برای برخی متغیرها، این جزء ممکن است درخواست‌های MMS Write را نیز صادر کند که منجر به تغییر وضعیت خواهد شد.

جزء 61850 لاگی شامل نشانی‌های IP، دامنه های MMS، متغیرها و وضعیت نقاط (باز یا بسته) اهداف خود تهیه می‌کند.

## جزء OPC DA

جزء OPC DA کلاینتی برای پودمان OPC Data Access ایجاد می‌کند. OPC که برگرفته از OLE for Process Control است استانداردی نرم‌افزاری است که مبتنی بر فناوری‌های شرکت مایکروسافت نظیر OLE، COM و DCOM فعالیت می‌کند. DA (Data Access) بخشی از ویژگی‌های OPC است که تبادل بلادرنگ[۱۵] داده‌ها را بین اجزای مختلف بر اساس الگوی کلاینت – سروری فراهم می‌کند.

این جزء از بدافزار Industroyer به صورت یک ابزار مخرب مستقل در فایلی با نام OPC.exe و یک فایل DLL با نام OPCClientDemo.dll اجرا می‌شود. بر اساس نام فایل می‌توان حدس زد که این جزء از پروژه کد باز[۱۶] OPC Client برداشت شده است.

```
;
; Export Address Table for OPCClientDemo.dll
;
off_10039678    dd rva Crash            ; DATA XREF: .rdata:1003966C↑o
;
; Export Names Table for OPCClientDemo.dll
;
off_1003967C    dd rva aCrash           ; DATA XREF: .rdata:10039670↑o
                                        ; "Crash"
```

شکل ۱۵: بازگردانی نام DLL داخلی در جزء OPC DA

جزء OPC DA نیاز به هیچ تنظیمی نداشته و بمحض اجرا شدن با روش ICatInformation::EnumClassesOfCategories – و با بکارگیری CATID_ OPCDAServer20 و IOPCServer::GetStatus – اقدام به شناسایی تمامی سرورهای OPC می‌کند.

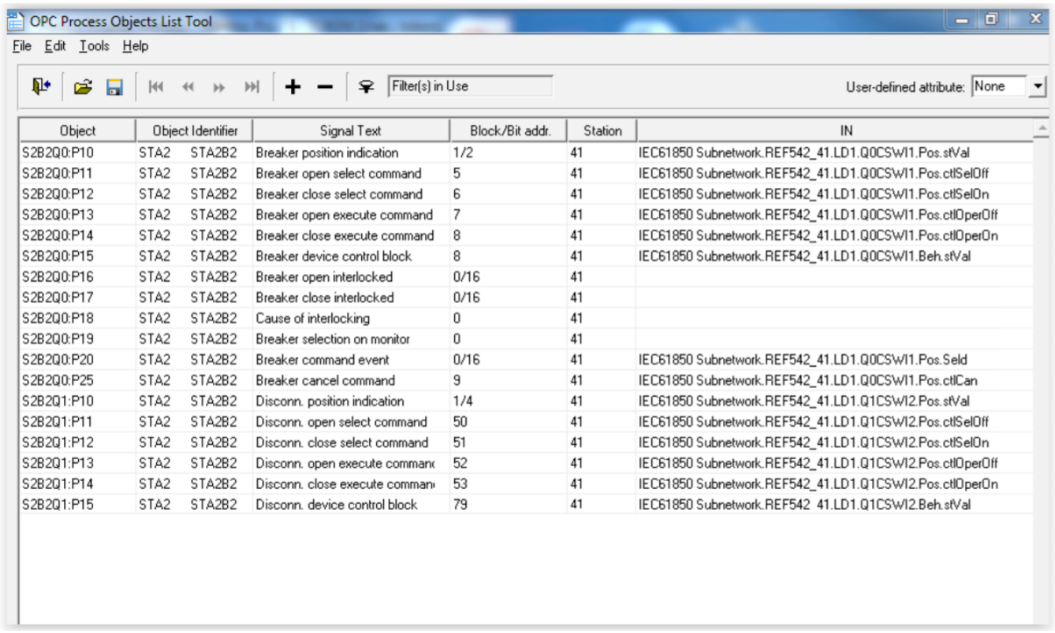
[۱۵] Real-time

[۱۶] Open Source Project

در ادامه با استفاده از IOPCBrowseServerAddressSpace تمامی رکوردهای OPC بر روی سرور شناسایی می‌شوند. این جزء به طور خاص وجود رکوردهایی که در نام آنها عبارات زیر باشد را مورد بررسی قرار می‌دهد:

- ctlSelOn
- ctlOperOn
- ctlSelOff
- ctlOperOff
- \Pos and stVal

بر اساس عبارات مذکور می‌توان اینطور نتیجه‌گیری کرد که مهاجمان بدنبال رکوردهای OPC آن دسته از سرورهایی هستند که از راهکارهای ABB نظیر MicroSCADA Pro استفاده می‌کنند. شکل ۱۶ نمونه فهرستی از رکوردهای OPC جمع‌آوری شده را نشان می‌دهد.




| Object | Object Identifier | Signal Text | Block/Bit addr. | Station | IN |
|---|---|---|---|---|---|
| S2B2Q0:P10 | STA2 STA2B2 | Breaker position indication | 1/2 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.stVal |
| S2B2Q0:P11 | STA2 STA2B2 | Breaker open select command | 5 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.ctlSelOff |
| S2B2Q0:P12 | STA2 STA2B2 | Breaker close select command | 6 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.ctlSelOn |
| S2B2Q0:P13 | STA2 STA2B2 | Breaker open execute command | 7 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.ctlOperOff |
| S2B2Q0:P14 | STA2 STA2B2 | Breaker close execute command | 8 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.ctlOperOn |
| S2B2Q0:P15 | STA2 STA2B2 | Breaker device control block | 8 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Beh.stVal |
| S2B2Q0:P16 | STA2 STA2B2 | Breaker open interlocked | 0/16 | 41 | |
| S2B2Q0:P17 | STA2 STA2B2 | Breaker close interlocked | 0/16 | 41 | |
| S2B2Q0:P18 | STA2 STA2B2 | Cause of interlocking | 0 | 41 | |
| S2B2Q0:P19 | STA2 STA2B2 | Breaker selection on monitor | 0 | 41 | |
| S2B2Q0:P20 | STA2 STA2B2 | Breaker command event | 0/16 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.SeId |
| S2B2Q0:P25 | STA2 STA2B2 | Breaker cancel command | 9 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q0CSWI1.Pos.ctlCan |
| S2B2Q1:P10 | STA2 STA2B2 | Disconn. position indication | 1/4 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q1CSWI2.Pos.stVal |
| S2B2Q1:P11 | STA2 STA2B2 | Disconn. open select command | 50 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q1CSWI2.Pos.ctlSelOff |
| S2B2Q1:P12 | STA2 STA2B2 | Disconn. close select command | 51 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q1CSWI2.Pos.ctlSelOn |
| S2B2Q1:P13 | STA2 STA2B2 | Disconn. open execute comman | 52 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q1CSWI2.Pos.ctlOperOff |
| S2B2Q1:P14 | STA2 STA2B2 | Disconn. close execute comman | 53 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q1CSWI2.Pos.ctlOperOn |
| S2B2Q1:P15 | STA2 STA2B2 | Disconn. device control block | 79 | 41 | IEC61850 Subnetwork.REF542_41.LD1.Q1CSWI2.Beh.stVal |

شکل ۱۶: فهرستی از رکوردهای OPC

مهاجمان در زمان اضافه کردن یک گروه OPC جدید از رشته‌ای با عنوان Abdul استفاده کرده‌اند.

```
.text:6B269BC8 push    edi                             ; ppUnk
.text:6B269BC9 push    offset IID_IOPCGroupStateMgt    ; riid
.text:6B269BCE push    [ebp+pRevisedUpdateRate]        ; pRevisedUpdateRate
.text:6B269BD1 mov     ecx, [eax+4]
.text:6B269BD4 lea     eax, [ebx+18h]
.text:6B269BD7 push    eax                             ; phServerGroup
.text:6B269BD8 push    0                               ; dwLCID
.text:6B269BDA lea     eax, [ebp+pPercentDeadband]
.text:6B269BDD mov     edx, [ecx]
.text:6B269BDF push    eax                             ; pPercentDeadband
.text:6B269BE0 movzx   eax, [ebp+arg_4]
.text:6B269BE4 push    0                               ; pTimeBias
.text:6B269BE6 push    0                               ; hClientGroup
.text:6B269BE8 push    [ebp+ppAddResults]              ; dwRequestedUpdateRate
.text:6B269BEB push    eax                             ; bActive
EIP .text:6B269BEC push    esi                         ; esi szName
.text:6B269BED push    ecx                             ; This
.text:6B269BEE call    [edx+IOPCServerVtbl.AddGroup]
.text:6B269BF1 test    eax, eax                            aAbdul_0:
.text:6B269BF3 jns     short loc_6B269C30                                  unicode 0, <Abdul>,0
.text:6B269BF5 push    offset aFailedToAddGro          ; "Failed to Add group"
.text:6B269BFA lea     ecx, [ebp+lpMultiByteStr]
.text:6B269BFD call    error_
```

شکل ۱۷: اشاره به رشته Abdul در کد جزء OPC DA

در آخرین مرحله، جزء OPC DA تلاش خواهد کرد تا وضعیت موارد OPC شناسایی شده را با استفاده از رابط IOPCSyncIO و درج دو بار مقدار 0x01 تغییر دهد.

```
.text:004034FE        mov     eax, VT_I2
.text:00403503        mov     word ptr [ebp+pItemValues.anonymous_0], ax
.text:0040350A        mov     eax, 1
.text:0040350F        mov     word ptr [ebp+pItemValues.anonymous_0+8], ax
.text:00403516        lea     eax, [ebp+pItemValues]
.text:0040351C        push    eax                     ; pItemValues
.text:0040351D        mov     eax, [ebp+OPC_items]
.text:00403523        mov     ecx, [eax+esi*4]
.text:00403526        call    IOPCSyncIO_Write
.text:0040352B        cmp     esi, edi
.text:0040352D        jb      short loc_403539
.text:0040352F        push    80070057h
.text:00403534        call    throw_exception
```

شکل ۱۸: اشاره به رابط IOPCSyncIO در کد جزء OPC DA

این جزء نام سرور OPC، عنوان رکورد OPC، کد کیفیت و مقدار آن را در لاگ ثبت می‌کند. مقادیر لاگ شده با سرآیندهای زیر جدا می‌شوند:

- [*ServerName: %SERVERNAME%] [State: Before]
- [*ServerName: %SERVERNAME%] [State: After ON]
- [*ServerName: %SERVERNAME%] [State: After OFF]

## جزء حذف کننده

جزء موسوم به Wiper در بدافزار Industroyer در مرحله نهایی مورد استفاده قرار می‌گیرد. مهاجمان از این جزء برای حذف ردپای خود و دشوار نمودن بازگردانی دستگاه‌ها به حالت پیش از آلودگی استفاده می‌کنند.

نام فایل جزء Wiper، haslo.dat یا haslo.exe است. این جزء می‌تواند توسط جزء اجرا کننده یا خود به تنهایی اجرا شود.

بمحض اجرا شدن Wiper تمامی کلیدهای ثبت شده در مسیر زیر در محضرخانه سیستم عامل را شناسایی می‌کند.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
```

در ادامه تلاش می‌کند تا در هر نتیجه یافت شده، کلید ImagePath را فاقد مقدار کند. در نتیجه این اقدام دستگاه از طریق سیستم عاملی که به محضرخانه آن دست‌درازی شده غیرقابل راه‌اندازی خواهد شد.

در مرحله بعد فایل‌های با هر یک از پسوندهای زیر در تمامی درایوهای متصل به دستگاه از C:\ تا Z:\ شناسایی و حذف می‌شوند:

- *.ldf
- *.pcmt
- *.log
- *.XRF
- *.prj
- *.7z
- *.cid
- *.mdf
- *.pcmi
- *.bkp
- *.paf
- *.CIN
- *.tar
- *.bak
- *.epl
- *.pcmp
- *.bk
- *.PL
- *.xml
- *.rar
- *.SCL
- *.elb
- *.dll
- *.v
- *.ini
- *.zip
- *.trc
- *.cxm
- *.exe
- *.scd

برخی از این پسوندها نظیر scl.، cid. و scd. توسط سیستم‌های کنترل صنعتی مورد استفاده قرار می‌گیرند. برخی دیگر همچون paf. توسط محصولات ABB بکار گرفته می‌شوند. شایان ذکر است در این مرحله در صورت شناسایی فایلی با نام SYS_BASCON.COM، اقدام به حذف آن خواهد شد.

همچنین این جزء از فایل‌هایی که در مسیر آنها کلمه Windows وجود دارد صرف‌نظر می‌کند.

این جزء محتوای فایل‌های شناسایی شده را با داده‌هایی بی‌معنی جایگزین می‌کند. به منظور افزایش اطمینان، فرآیند رونویسی به دو صورت انجام می‌شود. اولین تلاش بمحض شناسایی فایل انجام می‌شود. در صورت عدم موفقیت در این مرحله تلاش دوم شروع می‌شود. اما قبل از آن تمامی پروسه‌ها بجز آنهایی که در شکل ۱۹ فهرست شده‌اند متوقف می‌شوند.

همچنین برای افزایش سرعت عملیات رونویسی، این جزء تنها بخش ابتدای فایل را رونویسی می‌کند. میزان رونویسی هر فایل به اندازه فایل بستگی دارد. برای مثال برای فایل‌های با اندازه یک مگابایت یا کمتر ۴۰۹۶ بایت رونویسی می‌شود. حال آنکه برای فایل‌های تا ۱۰ مگابایت، ۳۲۷۶۸ بایت رونویسی می‌شود.

در نهایت اینکه این جزء اقدام به متوقف نمودن تمامی پروسه‌ها – شامل پروسه‌های سیستمی – بجز پروسه‌های خود می‌کند. موضوعی که سبب بی‌پاسخ ماندن دستگاه و در نهایت از کار افتادن آن می‌شود.

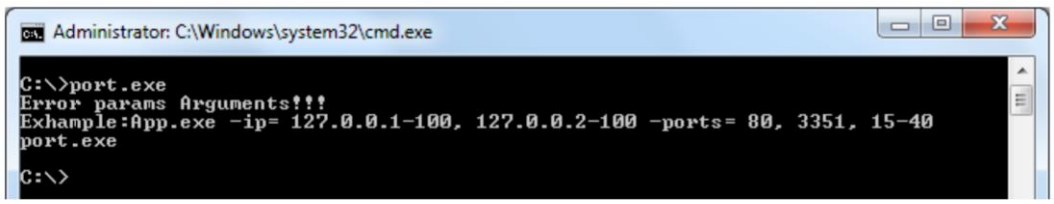
```
off_10010E88    dd offset aAudiodg_exe  ; DATA XREF: _terminate_processes:loc_10001470↑r
                                        ; "audiodg.exe"
                dd offset aConhost_exe  ; "conhost.exe"
                dd offset aCsrss_exe    ; "csrss.exe"
                dd offset aDwm_exe      ; "dwm.exe"
                dd offset aExplorer_exe ; "explorer.exe"
                dd offset aLsass_exe    ; "lsass.exe"
                dd offset aLsm_exe      ; "lsm.exe"
                dd offset aServices_exe ; "services.exe"
                dd offset aShutdown_exe ; "shutdown.exe"
                dd offset aSmss_exe     ; "smss.exe"
                dd offset aSpoolss_exe  ; "spoolss.exe"
                dd offset aSpoolsv_exe  ; "spoolsv.exe"
                dd offset aSvchost_exe  ; "svchost.exe"
                dd offset aTaskhost_exe ; "taskhost.exe"
                dd offset aWininit_exe  ; "wininit.exe"
                dd offset aWinlogon_exe ; "winlogon.exe"
                dd offset aWuauclt_exe  ; "wuauclt.exe"
```

شکل ۱۹: فهرست پروسه هایی که در مرحله اول رونویسی متوقف نمی شوند.

## اجـزای دیـگـر

### پویشـگـر درگـاه

جزئی از بدافزار Industroyer شامل ابزار پویشگری است که به نظر می‌رسد توسط نویسندگان آن توسعه داده شده است. این ابزار فهرست دستگاه‌های مرتبط را شناسایی می‌کند. شکل ۲۰ پارامترهای پشتیبانی شده توسط این ابزار را نمایش می دهد.




شکل ۲۰: پویشگر درگاه

## از کـاراندازی سـرویس

جزئی دیگر در بدافزار Industroyer، ابزاری است که با بهره‌جویی از آسیب‌پذیری از کار اندازی سرویس[۱۷] با شناسه CVE-2015-5374 در تجهیزات Siemens SIPROTEC سبب از کاراندازی آنها می‌شود.

مهاجمان نشانی‌های IP این تجهیزات را در کد تزریق کرده‌اند که پس از اجرا شدن ابزار مذکور بسته‌های دستکاری شده را در قالب بسته‌های UDP به درگاه 50000 آنها ارسال می‌کند که در نتیجه آن دستگاه از کار افتاده و عملاً از مدار خارج می‌شود. این بسته‌های UDP تنها شامل ۱۸ بایت هستند. (شکل ۲۱)

```
00000000:  11 49 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000010:  28 9E
```

شکل ۲۱: محتوای بسته UDP در هنگام بهره‌جویی از آسیب‌پذیری CVE-2015-5374

[۱۷] Denial of Service

## فـهـرسـت: درهـم‌سـازها[۱۸] و سـرورهـای فـرمـانـدهـی*

| درهم‌ساز SHA1 | نـــام شـنـاسـایی | |
|---|---|---|
| | McAfee | Bitdefender |
| F6C21F8189CED6AE150F9EF2E82A3A57843B587D | RDN/Generic.dx | Gen:Variant.Razy.117270 |
| CCCCE62996D578B984984426A024D9B250237533 | RDN/Generic.dx | Gen:Variant.Razy.117270 |
| 8E39ECA1E48240C01EE570631AE8F0C9A9637187 | RDN/Generic.dx | Trojan.GenericKD.5333238 |
| 2CB8230281B86FA944D3043AE906016C8B5984D9 | RDN/Generic.dx | Trojan.GenericKD.4154204 |
| 79CA89711CDAEDB16B0CCCCFDCFBD6AA7E57120A | RDN/Generic.hra | Trojan.GenericKD.4110889 |
| 94488F214B165512D2FC0438A581F5C9E3BD4D4C | RDN/Generic.dx | Trojan.GenericKD.5333249 |
| 5A5FAFBC3FEC8D36FD57B075EBF34119BA3BFF04 | RDN/Generic.dx | Trojan.GenericKD.5333249 |
| B92149F046F00BB69DE329B8457D32C24726EE00 | RDN/Ransom | Trojan.GenericKD.4048694 |
| B335163E6EB854DF5E08E85026B2C3518891EDA8 | RDN/Generic.dx | Trojan.GenericKD.5333253 |

**سرورهای فرماندهی**

- 195.16.88[.]6
- 46.28.200[.]132
- 188.42.253[.]43
- 5.39.218[.]152
- 93.115.27[.]57

* سرور فرماندهی این بدافزار در سامانه Tor قابل دسترس بوده‌اند و ممکن است مسدود نمودن این نشانی‌ها سبب بروز خطای تشخیص ناصحیح[۱۹] شود.

[۱۸] Hash
[۱۹] False Positive

شبکه گستر

با همکاری و مشارکت

کهکشان نو

# سمینار کالبدشکافی باج‌افزار WannaCry

زمان: دوشنبه، ۱۲ تیر ماه ۱۳۹۶، از ساعت ۹ الی ۱۳

مکان: مؤسسه آموزشی کهکشان
تهران، یوسف‌آباد، خیابان سی‌ویکم، نبش خیابان ابن‌سینا، شماره ۱۱۱

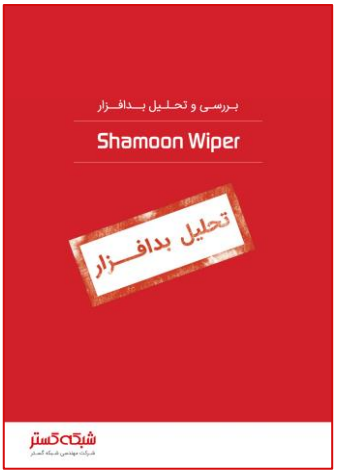
هزینه: ۲ میلیون ریال

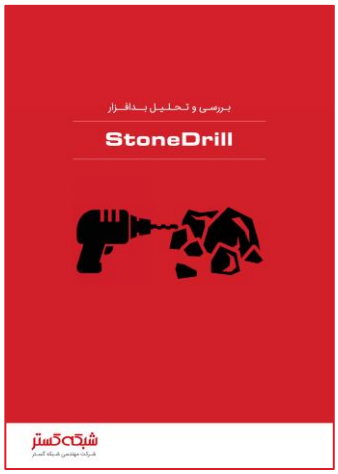
علاقمندان می توانند جهت شرکت در این سمینار با شماره ۴۲۰۵۲-۰۲۱ تماس حاصل نمایند.

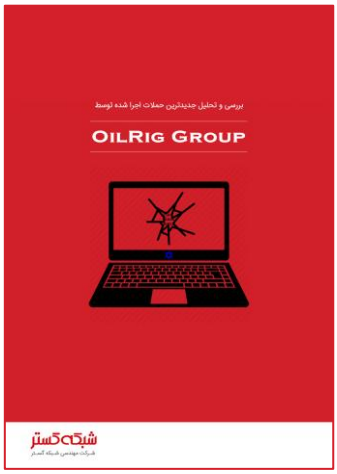

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳
تلفن / دورنگار ۴۲۰۵۲-۰۲۱
تارنمای شرکت www.shabakeh.net
مرکز آموزش events.shabakeh.net
اتاق خبر newsroom.shabakeh.net

## منابع


- https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet
- https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
- https://www.dragos.com/blog/crashoverride
- https://www.dragos.com/blog/crashoverride/CrashOverride-01.pdf
- http://new.abb.com/substation-automation/products/software/microscada-pro
- https://www.theguardian.com/technology/2017/jun/13/industroyer-malware-virus-bring-down-power-networks-infrastructure-wannacry-ransomware-nhs
- https://www.theregister.co.uk/2017/06/12/industroyer_malware
- https://www.bleepingcomputer.com/news/security/new-industroyer-malware-targets-power-grids
- https://www.usatoday.com/story/tech/news/2017/06/12/malware-discovered-could-threaten-electrical-grid/102775998


## شبکه گستر

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به‌عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد.

پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. در حال حاضر نیز شرکت شبکه گستر به‌عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات درایران اقدام می‌نماید.

در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی و انحصاری شرکت آلمانی Astaro، سازنده محصولات "مدیریت یکپارچه تهدیدات" ( Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر به‌عنوان نماینده شرکت Sophos ادامه فعالیت داده و اکنون محصولات Astaro سابق را تحت نام جدید Sophos و دیگر محصولات امنیت شبکه این شرکت را در ایران عرضه می‌نماید.

از سال ۱۳۹۱ نیز، شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به‌عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران، آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه است. ضد ویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظاراتی بودند که برخی کاربران و مدیران شبکه‌های کوچک و متوسط داشتند و با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد.

شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های طراحی، نصب، راه‌اندازی و طولانی مدت‌ترین خدمات نگهداری و پشتیبانی محصولات نرم‌افزاری ضدویروس و سخت‌افزاری فایروال در کشور بوده است.

این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

ISO 9001:2008
Cert No 9150.C528

شبکه گستر

شرکت مهندسی شبکه گستر


تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

تلفن / دورنگار ۰۲۱-۴۲۰۵۲

تارنمای شرکت www.shabakeh.net

سامانه پشتیبانی help.shabakeh.net

خدمات پس از فروش my.shabakeh.net

مرکز آموزش events.shabakeh.net

اتاق خبر newsroom.shabakeh.ne