



POSITIVE
TECHNOLOGIES

Плагин grstop для DRAKVUF. О пользе перехвата межпроцессного взаимодействия в PT Sandbox

Алексей Вишняков
Эксперт PT ESC



ptsecurity.com

Содержание

The logo consists of the letters 'PT' in a stylized, bold, sans-serif font, positioned within a white square.

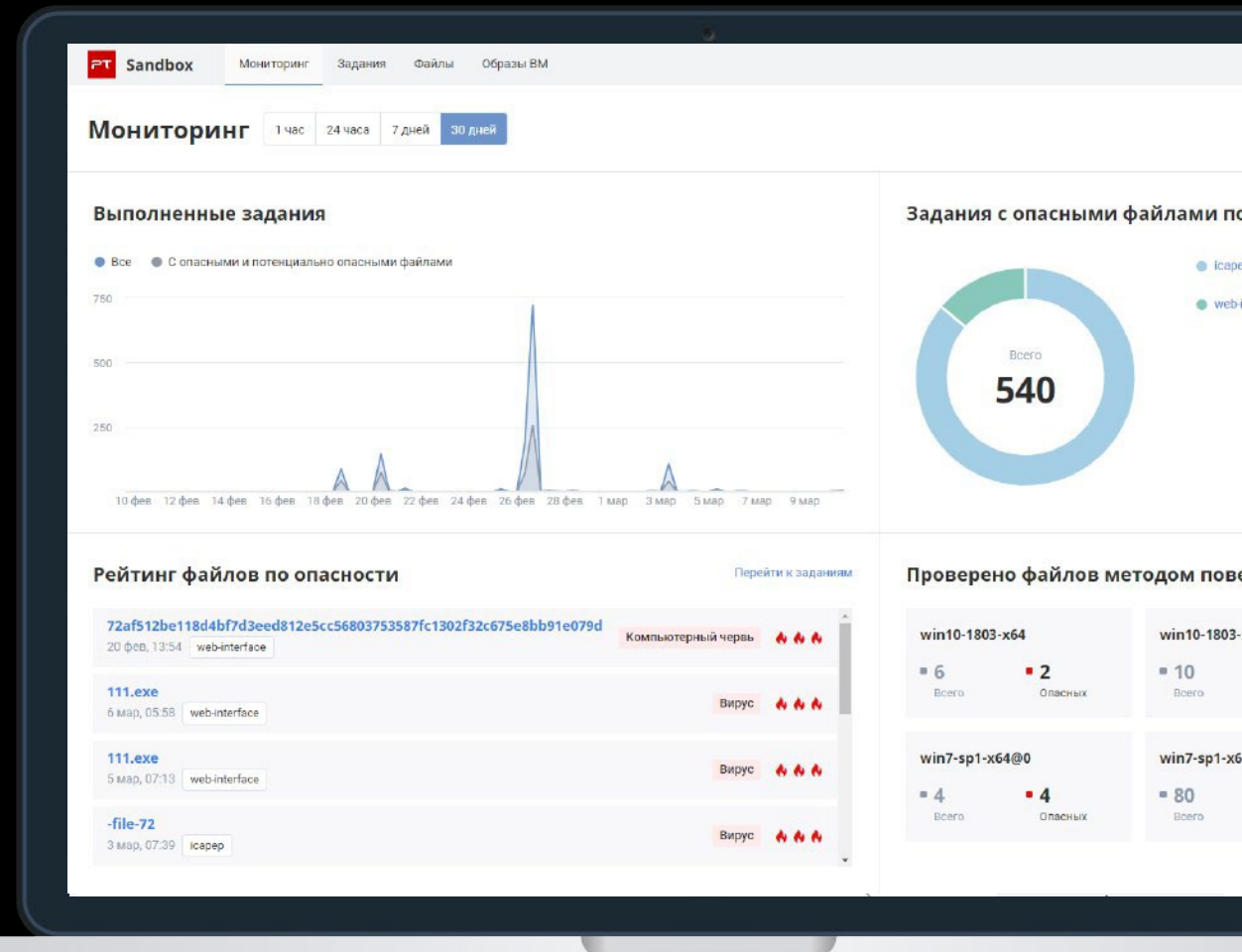
- Коротко о PT Sandbox
- Что такое RPC
- Плагин grstop для DRAKVUF
- Примеры вредоносных техник

PT Sandbox



Песочница для защиты от целевых и массовых атак с применением неизвестного вредоносного ПО и угроз нулевого дня.

- Обеспечивает комплексный анализ файлов и трафика (включая зашифрованный)
- Поддерживает гибкую настройку виртуальных сред и защищена от техник обхода песочниц
- Использует уникальные и наиболее актуальные знания для выявления угроз



Содержание

The logo consists of the letters 'PT' in a stylized, bold, sans-serif font, positioned within a white square.

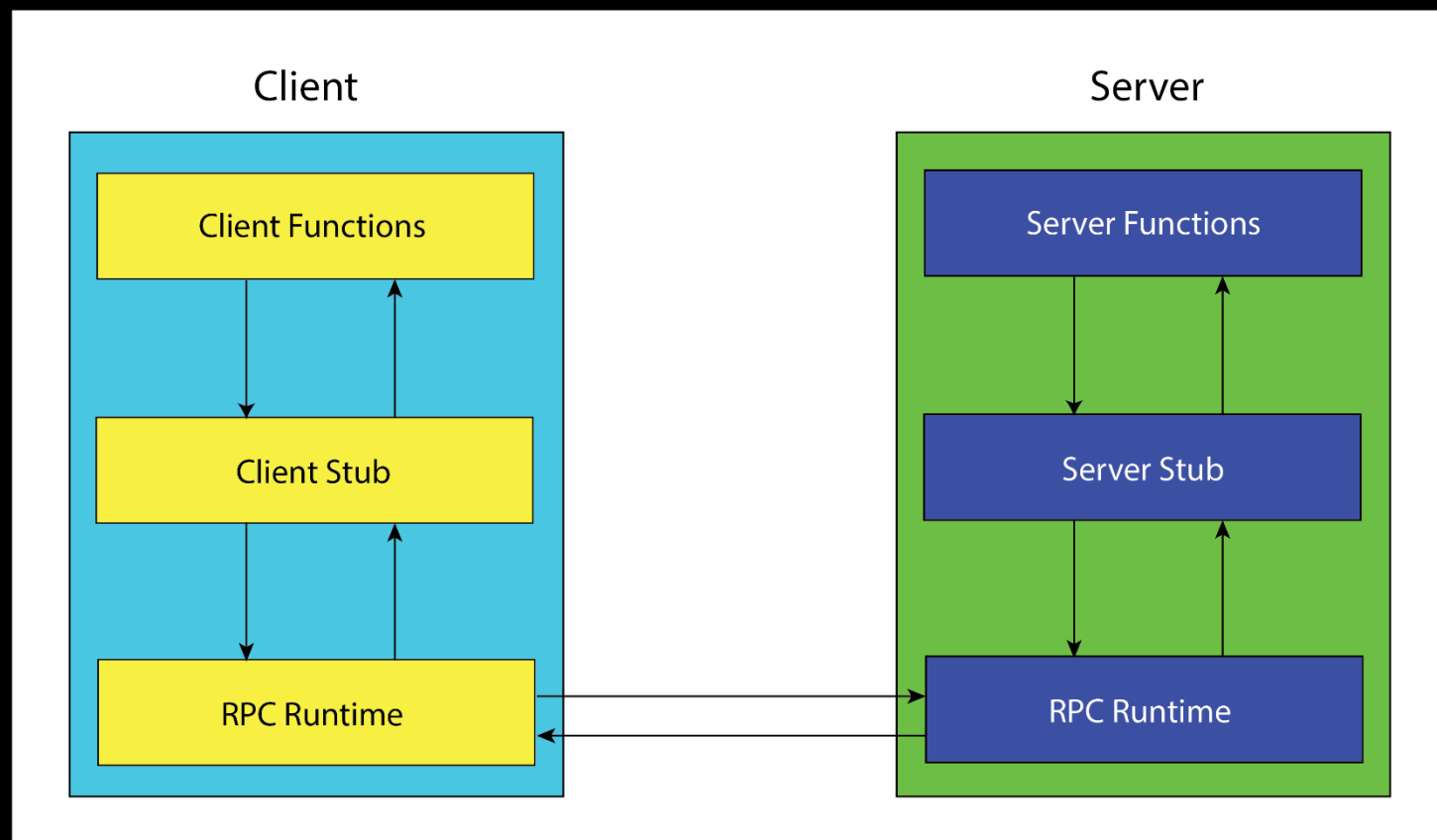
- Коротко о PT Sandbox
- Что такое RPC
- Плагин grstop для DRAKVUF
- Примеры вредоносных техник

Что такое RPC

- Как могут передаваться данные между процессами?
 - Файлы, реестр
 - Именованные каналы
 - Разделяемая память (shared memory)
 - Component Object Model (COM)
 - **Remote Procedure Call (RPC)**

Что такое RPC

- Архитектура: клиент—сервер
- Вызов функций через передачу сообщений
- В общем случае подразумевается передача данных между различными машинами

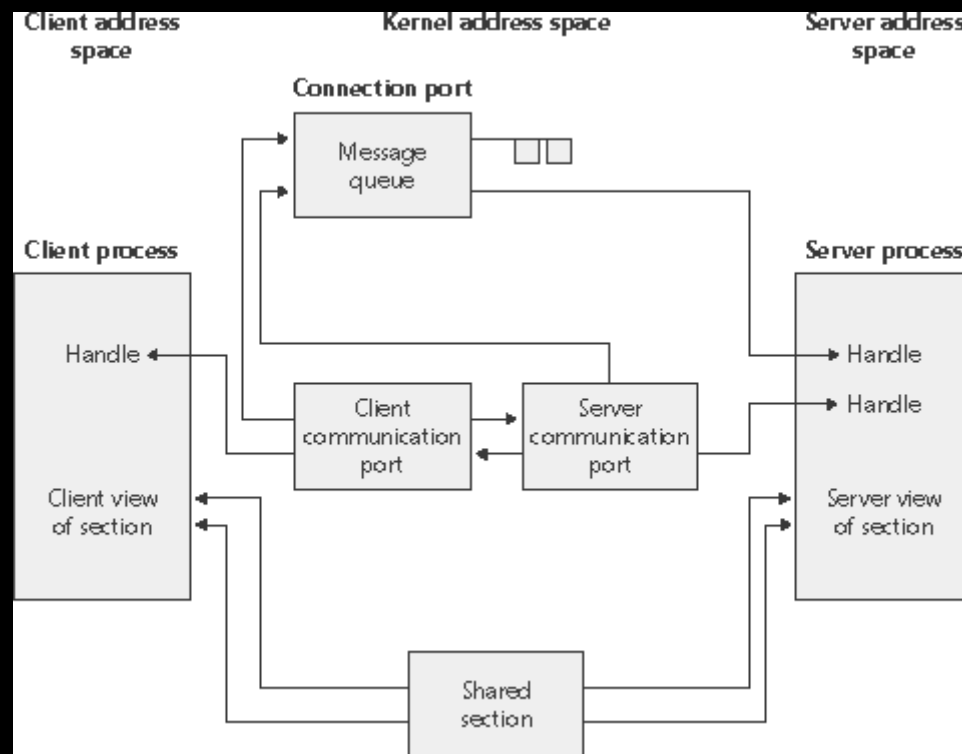


Что такое RPC



- Как устроен транспорт на одной машине между процессами?
 - Используется LPC (Local Inter-Process Communication)
 - Взаимодействие через LPC-порты
 - Данные передаются LPC-сообщениями или через общую секцию в памяти

Что такое RPC



<https://flylib.com/books/en/4.491.1.36/1/>

Что такое RPC



- А что происходит уровнем выше?
 - Используется MIDL-интерфейс (Microsoft Interface Definition Language) для клиент-серверного взаимодействия
 - Используется NDR-протокол (Network Data Representation) для передачи данных

Что такое RPC

PT

NdrClientCall4 function (rpcndr.h)

12/05/2018 • 2 minutes to read

[NdrClientCall4 is not supported and may be altered or unavailable in the future]

NdrClientCall2 function (rpcndr.h)

12/05/2018 • 2 minutes to read

The NdrClientCall2 function is the client-side entry point for the /Oicf

Syntax

```
C++  
  
CLIENT_CALL_RETURN RPC_VAR_ENTRY NdrClientCall2(  
    PMIDL_STUB_DESC pStubDescriptor,  
    PFORMAT_STRING pFormat,  
    ...  
);
```

NdrClientCall3 function (rpcndr.h)

12/05/2018 • 2 minutes to read

[NdrClientCall3 is not supported and may be altered or unavailable in the future]

NdrClientCall function (rpcndr.h)

12/05/2018 • 2 minutes to read

The NdrClientCall function is the client-side entry point for the /Oicf mode stub.

Syntax

```
C++  
  
CLIENT_CALL_RETURN RPC_VAR_ENTRY NdrClientCall(  
    PMIDL_STUB_DESC pStubDescriptor,  
    PFORMAT_STRING pFormat,  
    ...  
);
```

Что такое RPC



- Структура MIDL_STUB_DESC

MIDL_STUB_DESC structure (rpcndr.h)

12/05/2018 • 2 minutes to read

The `MIDL_STUB_DESC` structure is a MIDL-generated structure that contains information about the interface stub regarding RPC calls between the client and server.

Syntax

C++

Copy

```
typedef struct _MIDL_STUB_DESC {  
    void * pInterfaceInformation;  
    void * )(size_t)  
    void()(void *)  
    union {  
        * pfnAllocate;  
        * pfnFree;
```

Что такое RPC



- Структура `RPC_CLIENT_INTERFACE`

The `RPC_CLIENT_INTERFACE` structure is part of the private interface between the run-time libraries and the stubs. Most distributed applications that use Microsoft RPC do not need this structure.

The data structure is defined in the header file `Rpcdcep.h`. See the header file for syntax block and member definitions.

Syntax

C++


Copy

```
typedef struct _RPC_CLIENT_INTERFACE {  
    unsigned int Length;  
    RPC_SYNTAX_IDENTIFIER InterfaceId;  
    RPC_SYNTAX_IDENTIFIER TransferSyntax;
```

Что такое RPC

- Структура «заголовка форматной строки»

Procedure Header Descriptor


05/31/2018 • 2 minutes to read • 

The header has been extended several times over the life of the NDR engine. The current compiler still generates different headers depending on the mode of the compiler. However, more recent headers are a superset of the older ones.

The Old –Oi Header

The header has the following format:

syntax

 Copy

```
handle_type<1>
Oi_flags<1>
[rpc_flags<4>]
proc_num<2>
stack_size<2>
[explicit_handle_description<>]
```

<https://docs.microsoft.com/en-us/windows/win32/rpc/procedure-header-descriptor>

Содержание

The logo consists of the letters 'PT' in a stylized, bold, sans-serif font, positioned within a white square.

- Коротко о PT Sandbox
- Что такое RPC
- Плагин `grstop` для `DRAKVUF`
- Примеры вредоносных техник

Плагин grstmon для DRAKVUF

PT

В предыдущих
сериях

SetResponse Плагин exploitmon для DRAKVUF PT Sandbox обнаружил эксплуатацию ядра
Плагин exploitmon для DRAKVUF. Обнаружение эксплуатации ядра ОС с п...

Смотреть позже Поделиться

DRAKVUF. Black-box Binary Analysis System

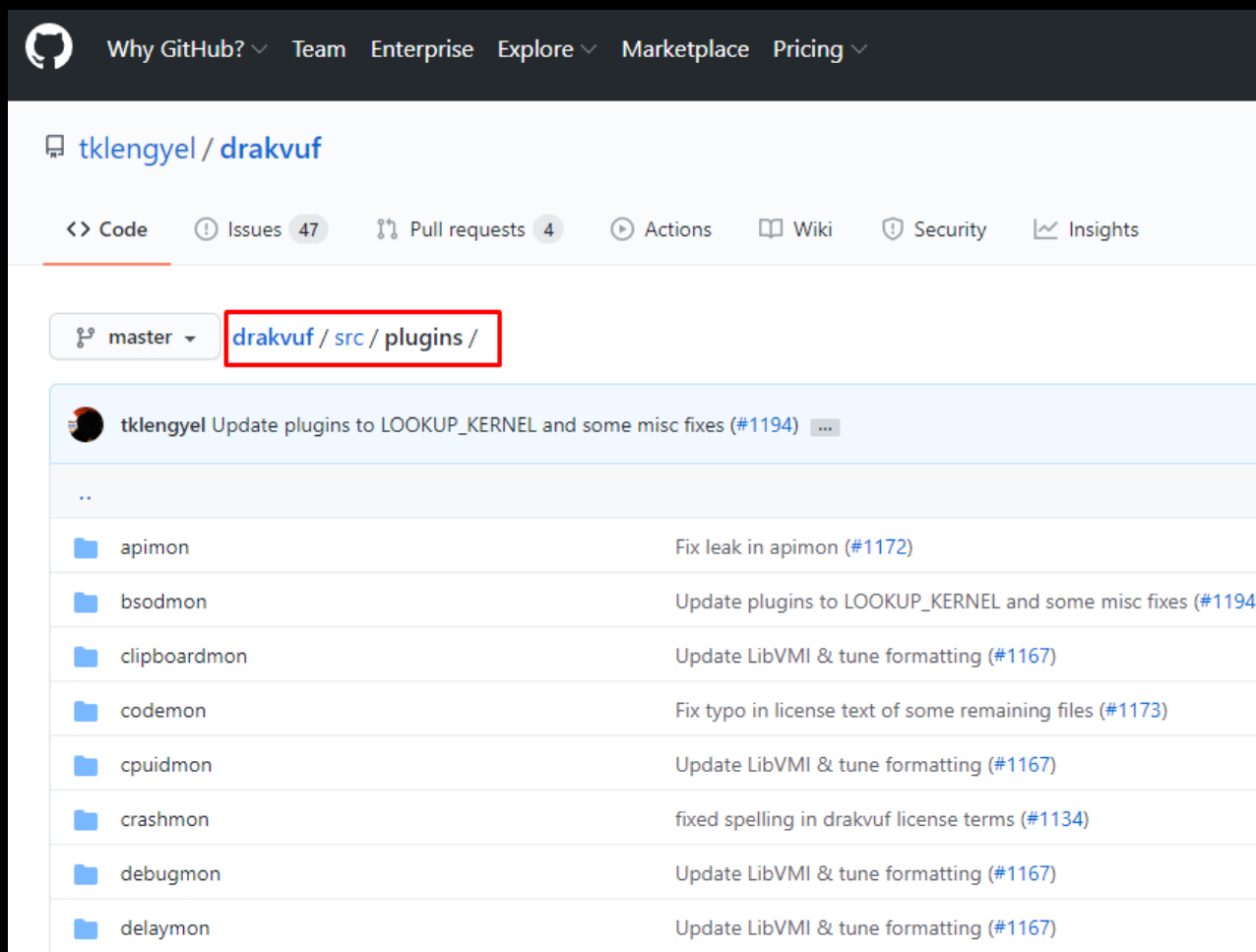
- Фреймворк для скрытного динамического анализа
- API не зависит от гостевой операционной системы
- Легко расширяется с помощью плагинов
- Использует LibVMi для мониторинга и изменения состояния виртуальной системы

ПОКАЗАТЬ ДРУГИЕ ВИДЕО

10:03 / 46:51 YouTube

Плагин грстоп для DRAKVUF

PT



<https://github.com/tklengyel/drakvuf/tree/master/src/plugins>

Плагин rpcmon для DRAKVUF



Перехватываемые API

```
533     if (!drakvuf_are_userhooks_supported(drakvuf))
534     {
535         PRINT_DEBUG("[RPCMON] Usermode hooking not supported.\n");
536         return;
537     }
538
539     const auto log = HookActions::empty().set_log();
540     wanted_hooks.add_hook("rpcrt4.dll", "NdrAsyncClientCall", log, rpc_call_args());
541     wanted_hooks.add_hook("rpcrt4.dll", "NdrAsyncClientCall2", log, rpc_call_args());
542     wanted_hooks.add_hook("rpcrt4.dll", "NdrClientCall", log, rpc_call_args());
543     wanted_hooks.add_hook("rpcrt4.dll", "NdrClientCall2", log, rpc_call_args());
544     wanted_hooks.add_hook("rpcrt4.dll", "NdrClientCall3", log, rpc_call3_args());
545     wanted_hooks.add_hook("rpcrt4.dll", "NdrClientCall4", log, rpc_call_args());
546     wanted_hooks.add_hook("rpcrt4.dll", "I_RpcReceive", log, i_rpc_args());
547     wanted_hooks.add_hook("rpcrt4.dll", "I_RpcSend", log, i_rpc_args());
548     wanted_hooks.add_hook("rpcrt4.dll", "I_RpcSendReceive", log, i_rpc_args());
549
550     usermode_cb_registration reg =
551     {
552         .pre_cb = on_dll_discovered,
553         .post_cb = on_dll_hooked,
554         .extra = (void*)this
555     };
```

<https://github.com/tklengyel/drakvuf/blob/master/src/plugins/rpcmon/rpcmon.cpp>

Плагин rpcmon для DRAKVUF



Описания структур данных

```
152 struct _RPC_CLIENT_INTERFACE
153 {
154     uint32_t Length;
155     RPC_SYNTAX_IDENTIFIER InterfaceId;
156     RPC_SYNTAX_IDENTIFIER TransferSyntax;
157 } __attribute__((packed, aligned(4)));
158
159 struct _MIDL_STUB_DESC
160 {
161     addr_t RpcInterfaceInformation;
162 } __attribute__((packed, aligned(4)));
163
164 struct _MIDL_STUB_DESC_32
165 {
166     uint32_t RpcInterfaceInformation;
167 } __attribute__((packed, aligned(4)));
168
169 struct _MIDL_STUBLESS_PROXY_INFO
```

<https://github.com/tklengyel/drakvuf/blob/master/src/plugins/rpcmon/rpcmon.cpp>

Плагин rpcmon для DRAKVUF



Извлечение идентификатора интерфейса

```
246 static std::optional<rpc_info_t> parse_MIDL_STUB_DESC(drakvuf_t drakvuf, drakvuf_trap_info* info, addr_t arg)
247 {
248     addr_t rpc_interface_information_addr = get_rpc_interface_information_addr(drakvuf, info, arg);
249     if (!rpc_interface_information_addr)
250         return {};
251
252     ACCESS_CONTEXT(ctx,
253         .translate_mechanism = VMI_TM_PROCESS_DTB,
254         .dtb = info->regs->cr3,
255         .addr = rpc_interface_information_addr
256     );
257
258     auto vmi = vmi_lock_guard(drakvuf);
259
260     auto rpc_iface = read_struct<_RPC_CLIENT_INTERFACE>(vmi, &ctx);
261     if (!rpc_iface)
262         return {};
263
264     return {{rpc_iface->InterfaceId.SyntaxGuid.str(), rpc_iface->TransferSyntax.SyntaxGuid.str()}};
265 }
```

<https://github.com/tklengyel/drakvuf/blob/master/src/plugins/rpcmon/rpcmon.cpp>

Плагин rpcmon для DRAKVUF



Извлечение номера процедуры

```
}
else if (std::string("pFormat") == (*printer)->get_name())
{
    auto r = parse_FORMAT_STRING(drakvuf, info, *arg);
    if (!r) continue;

    fmt_extra_num.push_back(std::make_pair("ProcedureNumber", fmt::Nval(*r)));
}
else if (std::string("RpcMessage") == (*printer)->get_name())
{
    auto r = parse_RPC_MESSAGE(drakvuf, info, *arg);
    if (!r) continue;

    fmt_extra_num.push_back(std::make_pair("ProcNum", fmt::Nval(r->ProcNum)));
    fmt_extra.push_back(std::make_pair("InterfaceId", r->InterfaceIdGuid));
}
```

```
285     uint8_t oi_flags;
286     ctx.addr = arg + Oi_FLAGS_FIELD_OFFSET;
287     if (VMI_SUCCESS != vmi_read_8(vmi, &ctx, &oi_flags))
288         return {};
289
290     int proc_num_field_offset = (oi_flags & Oi_HAS_RPCFLAGS)
291         ? Oi_PROCNUM_FIELD_OFFSET_WITH_RPCFLAGS
292         : Oi_PROCNUM_FIELD_OFFSET_WITHOUT_RPCFLAGS;
293
294     uint16_t proc_num;
295     ctx.addr = arg + proc_num_field_offset;
296     if (VMI_SUCCESS != vmi_read_16(vmi, &ctx, &proc_num))
297         return {};
298
299     return proc_num;
300 }
```

Содержание

PT

- Коротко о PT Sandbox
- Что такое RPC
- Плагин grstop для DRAKVUF
- Примеры вредоносных техник

Примеры вредоносных техник

PT

SetResponse

Закрепление и уклонение от обнаружения

Закрепление и уклонение от обнаружения: детектирование техник на при...

Смотреть позже

Поделиться

PT

POSITIVE TECHNOLOGIES

Алексей

модуль аудио и видео

ЧАТ

Positive Technologies

Всем добрый день! Видеозапись вебинара и презентация будут опубликованы на следующий день на сайте компании — [ptecsecurity.com/en](https://www.ptecsecurity.com/en)

Добрый день! :) Звук, видео - в норме. :)

Режим текстовых вопросов и ответов включен

Модерация чата включена

Люлин Александр

Добрый день)

Александр Александр

syswow64?

Руслан Корнев

sys - ш... н дл...уппы

YouTube

Техники автозапуска

CreateServiceA (Advapi32.dll -> sechost.dll) -> NdrClientCall4 (RPCRT4.dll)

```
84 if ( !v30 )
85     goto LABEL_51;
86 if ( lpServiceName && !sub_1002440A(&v24)
87     || lpDisplayName && !sub_1002440A(&v23)
88     || lpBinaryPathName && !sub_1002440A(&v22)
89     || lpLoadOrderGroup && !sub_1002440A(&v21)
90     || lpServiceStartName && !sub_1002440A(&v20) )
91 {
92     goto LABEL_10;
93 }
94 as_exc.registration.TryLevel = 1;
95 v16 = NdrClientCall4(
96     &off_10001080,
97     dword_10003AAC,
98     hSQManager,
99     v24,
100     v23,
101     dwDesiredAccess,
102     dwServiceType,
103     dwStartType,
104     dwErrorControl,
105     v22,
```

ПОКАЗАТЬ ДРУГИЕ ВИДЕО

В предыдущих
сериях (1/2)

Примеры вредоносных техник

PT

SetResponse Закрепление и уклонение от обнаружения

Закрепление и уклонение от обнаружения: детектирование техник на при...

Смотреть позже Поделиться

POSITIVE TECHNOLOGIES

Алексей

Модуль аудио и видео

ЧАТ

Positive Technologies

Всем добрый день! Видеозапись вебинара и презентация будут опубликованы на следующий день на сайте компании — [ptec.ru/](https://www.ptec.ru/)

Добрый день! :) Звук видео - в норме. :)

Режим текстовых вопросов и ответов включен

Модерация чата включена

Люлин Александр

Добрый день)

Александр Александр

syswow64?

Руслан Корнев

sys - ш... н дл... уппы

YouTube

Техники автозапуска

1FF70682-0A51-30E8-076D-740BE8CEE98B - ATSvc UUID version 1.0

docs.microsoft.com/en-us/openspecs/windows_protocols/ms-tschr/fbab083e-f79f-4216-af4c-d5104a913d40

```
.text:10001488 44 00 00 00 dword_10001488 dd 44h ; DATA_XREF: .text:off_10001008f0
.text:1000148C 82 db 82h ; 1ff70682-0a51-30e8-076d-740be8cee98b
.text:1000148D 06 db 6
.text:1000148E F7 db 0F7h ; 4
.text:1000148F 1F db 1Fh
.text:10001490 51 db 51h ; Q
.text:10001491 0A db 0Ah
.text:10001492 E8 db 0E8h ; и
.text:10001493 30 db 30h ; 0
.text:10001494 07 db 7
.text:10001495 6D db 6Dh ; и
.text:10001496 74 db 74h ; t
.text:10001497 00 db 00h
.text:10001498 E8 db 0E8h ; и
.text:10001499 CE db 0CEh ; O
.text:1000149A E9 db 0E9h ; и
.text:1000149B 8B db 8Bh ; c
```

ПОКАЗАТЬ ДРУГИЕ ВИДЕО

В предыдущих
сериях (2/2)

Примеры вредоносных техник

РТ

T1529: System Shutdown/Reboot

The screenshot displays the MITRE ATT&CK website interface. The top navigation bar is orange and contains the MITRE | ATT&CK logo, a search bar, and links for Matrices, Tactics, Techniques, Mitigations, Groups, and Software. The left sidebar lists various technique categories with expandable arrows. The main content area shows the breadcrumb path Home > Techniques > Enterprise > System Shutdown/Reboot, followed by the title 'System Shutdown/Reboot'. The description explains that adversaries may shutdown/reboot systems to interrupt access or aid in destruction, and provides examples of commands used for this purpose.

MITRE | ATT&CK®

Matrices Tactics Techniques Mitigations Groups Software

Search

TECHNIQUES

- Enterprise ^
- Reconnaissance v
- Resource Development v
- Initial Access v
- Execution v
- Persistence v
- Privilege v

Home > Techniques > Enterprise > System Shutdown/Reboot

System Shutdown/Reboot

Adversaries may shutdown/reboot systems to interrupt access to, or aid in the destruction of, those systems. Operating systems may contain commands to initiate a shutdown/reboot of a machine. In some cases, these commands may also be used to initiate a shutdown/reboot of a remote computer.^[1] Shutting down or rebooting systems may disrupt access to computer resources for legitimate users.

Adversaries may attempt to shutdown/reboot a system after impacting it in other ways, such as [Disk Structure Wipe](#) or [Inhibit System Recovery](#), to hasten the intended effects on system availability.^{[2][3]}

Примеры вредоносных техник

PT

```
push [ebp+lpServiceConfig] ; lpServiceConfig
push [ebp+hService] ; hService
call ebx ; QueryServiceConfigW
test eax, eax
jz short loc_4013F5
```

The malware uses the ChangeServiceConfigW API to change the start type to 4 which means: "Disabled: Specifies that the service should not be started."

Additionally, the malware lists mapped file shares and for each share, it will wipe the writable files (using either uninitialized data or 0x00 depending of the file size).

Finally after modifying all the system configuration, the destroyer shutdowns the compromised system.

LEGITIMATE FILE

Additionally, the Olympic Destroyer drops the legitimate, digitally signed, PsExec file in order to perform

<https://blog.talosintelligence.com/2018/02/olympic-destroyer.html>

Вайпер

Olympic Destroyer

Примеры вредоносных техник

РТ

Шифровальщик
REvil



MalwareHunterTeam @malwrhunterteam · 18 мар.

Not remember seeing these before in REvil ransomware samples.



So basically the actors using REvil now can use it to **reboot target machines** into safe mode with networking...

@demonslay335 @VK_Intel

```
push 5 ; uCmdShow
push offset EndLine ; "bootcfg /raw /a /sa
call ds:WinExec
lea eax, [ebp+String]
push eax
push 3Ch
push 4
push 48Ch
push offset unk_410278
call sub_406461
xor eax, eax
add esp, 14h
mov [ebp+var_4], ax
lea eax, [ebp+String]
push eax ; lpString
call ds:strlenW
mov [ebp+var_4], eax
lea eax, ds:2[eax*2]
push eax
lea eax, [ebp+String]
```

6

53

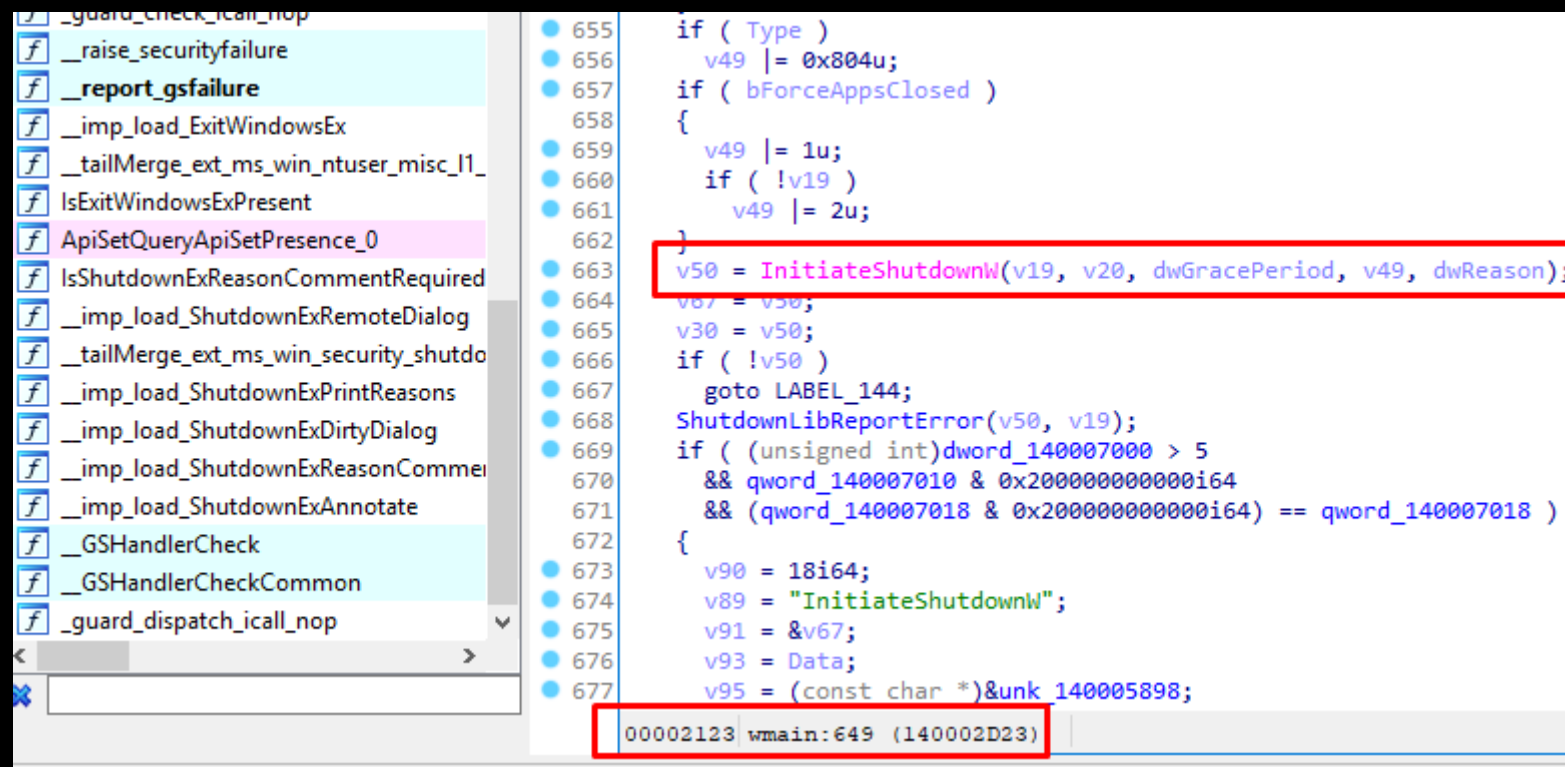
119



<https://twitter.com/malwrhunterteam/status/1372536434125512712>

Примеры вредоносных техник

Рассматриваемая команда: shutdown.exe /s /f /t 0



```
655 if ( Type )
656     v49 |= 0x804u;
657 if ( bForceAppsClosed )
658 {
659     v49 |= 1u;
660     if ( !v19 )
661         v49 |= 2u;
662 }
663 v50 = InitiateShutdownW(v19, v20, dwGracePeriod, v49, dwReason);
664 v67 = v50;
665 v30 = v50;
666 if ( !v50 )
667     goto LABEL_144;
668 ShutdownLibReportError(v50, v19);
669 if ( (unsigned int)dword_140007000 > 5
670     && qword_140007010 & 0x2000000000000000i64
671     && (qword_140007018 & 0x2000000000000000i64) == qword_140007018 )
672 {
673     v90 = 18i64;
674     v89 = "InitiateShutdownW";
675     v91 = &v67;
676     v93 = Data;
677     v95 = (const char *)&unk_140005898;
678 }
00002123 wmain: 649 (140002D23)
```

Примеры вредоносных техник

advapi32! InitiateShutdownW

```
16 v5 = &word_1800723A8;
17 v6 = lpMachineName;
18 v7 = dwShutdownFlags;
19 if ( lpMachineName )
20     v5 = lpMachineName;
21 v8 = dwGracePeriod;
22 v9 = RtlInitUnicodeStringEx(&v12, lpMessage);
23 if ( (v9 & 0x80000000) != 0 )
24     return RtlNtStatusToDosError(v9);
25 if ( (v12 & 0xFFFFEu) >= 0x400 || v8 >= 0x12CC0300 )
26     return 87;
27 result = WsdpInitiateShutdown(v5, (__int64)&v12, v8, v7, dwReason);
28 if ( result == 87 )
29 {
30     if ( v6 )
31         InitiateShutdownW(10 (180018690)
```

Примеры вредоносных техник

PT

advapi32, WsdpInitiateShutdown

Номер процедуры: 0

```
46     HIWORD(v16) = 2 * v10 + 2;
47     }
48     else
49     {
50         LocalFree(hMem);
51         hMem = 0i64;
52     }
53 }
54 v11.Pointer = NdrClientCall3(&stru_180060170, 0, 0i64, Binding, v7, v6, v5, a5, &v16).Pointer;
55 v12 = (unsigned int)v11.Pointer;
56 v15.Pointer = v11.Pointer; CLIENT_CALL_RETURN(MIDL_STUBLESS_PROXY_INFO *pProxyInfo, unsigned int nProcNum,
57 }
```

000270F7 WsdpInitiateShutdown:39 (180027CF7)

Примеры вредоносных техник

ID интерфейса: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D

```
.rdata:00000000180069658 00 00 00 00 00 00 00 align 20h
.rdata:00000000180069660 60 00 00 00 dword_180069660 dd 60h
.rdata:00000000180069664 70 db 70h ; p
.rdata:00000000180069665 FE db 0FEh ; ю
.rdata:00000000180069666 5A db 5Ah ; Z
.rdata:00000000180069667 D9 db 0D9h ; Щ
.rdata:00000000180069668 D5 db 0D5h ; X
.rdata:00000000180069669 A6 db 0A6h ; i
.rdata:0000000018006966A 59 db 59h ; Y
.rdata:0000000018006966B 42 db 42h ; B
.rdata:0000000018006966C 82 db 82h ; ,
.rdata:0000000018006966D 2E db 2Eh ; .
.rdata:0000000018006966E 2C db 2Ch ; ,
.rdata:0000000018006966F 84 db 84h ; „
.rdata:00000000180069670 DA db 0DAh ; Ъ
.rdata:00000000180069671 1D db 1Dh
.rdata:00000000180069672 DB db 0DBh ; Ь
.rdata:00000000180069673 0D db 0Dh
.rdata:00000000180069674 01 db 1
```

Примеры вредоносных техник



```
19  RPC  894de0c0-0d55-11d3-a322-00c04fa321a1 (1.0) -- C:\windows\system32\wininit.exe
20      0 -> s_BaseInitiateShutdown
21      1 -> s_BaseAbortShutdown
22      2 -> s_BaseInitiateShutdownEx
23  RPC  d95afe70-a6d5-4259-822e-2c84da1ddb0d (1.0) -- C:\windows\system32\wininit.exe
24      0 -> s_WsdrInitiateShutdown
25      1 -> s_WsdrAbortShutdown
26      2 -> s_WsdrCheckForHiberboot
27  RPC  76f226c3-ec14-4325-8a99-6a46348418af (1.0) -- C:\windows\system32\wininit.exe
```

<https://gist.github.com/enigma0x3/2e549345e7f0ac88fad130e2444bb702>

rpcmon Time = 1234567890.123456, PID = 3900, PPID = 3624, TID = 3504, ProcessName =
"\\Device\\HarddiskVolume2\\Windows\\System32\\shutdown.exe", Method = **NdrClientCall3**, Event =
"api_called", CalledFrom = 0x7FEFE9E2E9E, ReturnValue = 0x0, pStubProxy = 8791775207072,
ProcedureNumber = 0, InterfaceId = "D95AFE70-A6D5-4259-822E-2C84DA1DDB0D",
TransferSyntax = "8A885D04-1CEB-11C9-9FE8-08002B104860"

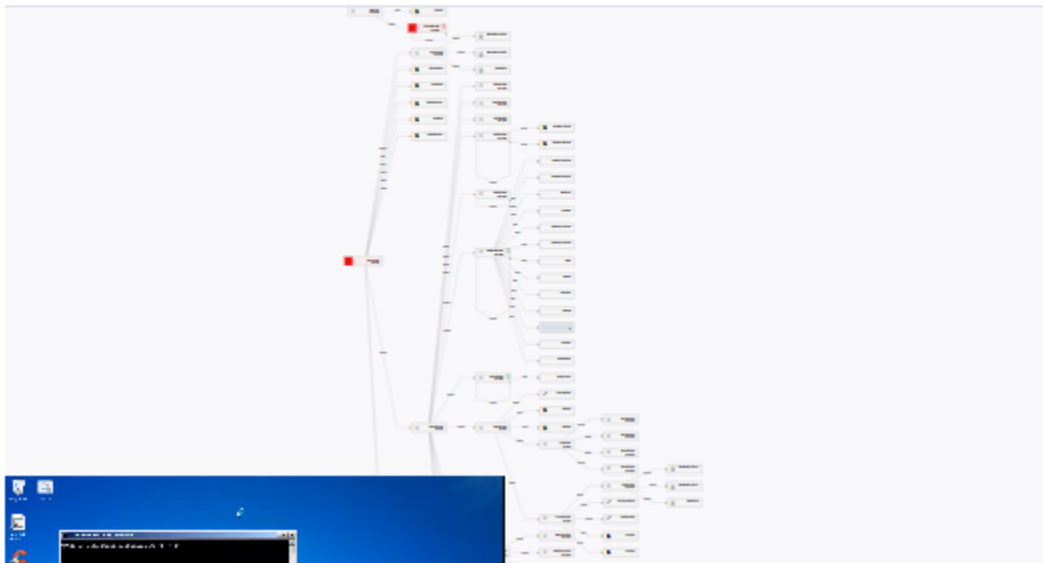
Примеры вредоносных техник

PT

Delete.System.ShutDown.Destruction в PT Sandbox

Поведенческий анализ...
Образ win7-sp1-x64

Скачать результаты анализа



Результат поведенческого анализа

Троян

Поведенческий анализ

Обнаруженное опасное ПО

Троян
Trojan.Win32.Generic.a

Потенциально опасное поведение

Delete.System.ShutDown.Destruction

Примеры вредоносных техник

PT

T1087: Account Discovery

The screenshot displays the MITRE ATT&CK website interface. The top navigation bar is orange and contains the MITRE logo, the ATT&CK logo, and a search bar. To the right of the search bar are links for Matrices, Tactics, Techniques, Mitigations, Groups, and Software. The left sidebar is white and lists various technique categories under the heading 'TECHNIQUES'. The main content area is white and shows the breadcrumb path 'Home > Techniques > Enterprise > Account Discovery > Local Account'. The title 'Account Discovery: Local Account' is prominently displayed. Below the title is a dropdown menu labeled 'Other sub-techniques of Account Discovery (4)'. The main text describes how adversaries might attempt to get a listing of local system accounts and provides examples of commands like 'net user', 'net localgroup', 'id', and 'groups' on macOS and Linux, as well as the '/etc/passwd' file on Linux.

MITRE | ATT&CK®

Matrices Tactics Techniques Mitigations Groups Software

Search 🔍

TECHNIQUES

Enterprise ^

Reconnaissance v

Resource Development v

Initial Access v

Execution v

Persistence v

Privilege Escalation v

Home > Techniques > Enterprise > Account Discovery > Local Account

Account Discovery: Local Account

Other sub-techniques of Account Discovery (4) v

Adversaries may attempt to get a listing of local system accounts. This information can help adversaries determine which local accounts exist on a system to aid in follow-on behavior.

Commands such as `net user` and `net localgroup` of the `Net` utility and `id` and `groups` on macOS and Linux can list local users and groups. On Linux, local users can also be enumerated through the use of the `/etc/passwd` file.

Примеры вредоносных техник

In addition to document stealing, the operators also run many commands to gather information about the Active Directory groups or users, the network or Microsoft Windows configurations such as the group policies. Figure 6 is a list of commands executed by Turla operators.

```
gpreresult /z
gpreresult /v
gpreresult
net view
net view /domain
netstat
netstat -nab
netstat -nao
nslookup 127.0.0.1
ipconfig /all
arp -a
net share
net use
systeminfo
net user
net user administrator
net user /domain
net group
net group /domain
net localgroup
net localgroup
net localgroup Administrators
net group "Domain Computers" /domain
net group "Domain Admins" /domain
net group "Domain Controllers" /domain
dir "%programfiles%"
net group "Exchange Servers" /domain
net accounts
net accounts /domain
net view 127.0.0.1 /all
net session
route print
ipconfig /displaydns
```

Turla APT,
ComRAT v4

Примеры вредоносных техник

РТ

ProjectSauron APT

uninstdll	<i>Pre-packaged core platform with a script tasked for removing all the traces of the malicious components in the system</i>
users	Dump user list [options] Options: -f <pattern> Display only users where the name matches <pattern>. -s <server> Display users on <server>. Default is localhost.

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07190156/The-ProjectSauron-APT_Technical_Analysis_KL.pdf

Примеры вредоносных техник

Рассматриваемая команда: net user

```
141     _setmode(v21, 0x4000);
142     Tokptr = (__int64)Tokstack;
143     Tokmax = (__int64)Tokstack;
144     lexor(Tokstack, v22);
145     XXtoken = dword_14000ECA8;
146     XXnode = Tokstack[0];
147     xx_parser(0, &S_orstack, 0, v23);
148     NetcmdExit(0);
149 }
150 ErrorPrint(v17);
151 NetcmdExit(2);
152 }
153 ErrorPrint(v15);
154 NetcmdExit(2);
155 }
```

000006D8 main:126 (1400012D8)

```
v29 = v28 + 266;
v30 = NetApiBufferAllocate(2 * v29, &Buffer);
if ( !v30 )
{
    v31 = GetSystemDirectoryW((LPWSTR)Buffer, 0x104u);
    if ( v31 )
    {
        wcscpy_s((wchar_t *)Buffer + v31, v29 - v31, L"\\net1");
        if ( v27 )
            wcscat_s((wchar_t *)Buffer, v29, v27);
        if ( CreateProcessW(0i64, (LPWSTR)Buffer, 0i64, 0i64, 1,
            {
                CloseHandle(ProcessInformation.hThread);
                WaitForSingleObject(ProcessInformation.hProcess, 0xFFFF
00000C48 xx_parser:226 (140001848)
```

Примеры вредоносных техник

net1.exe, user_enum

```
33 {
34     wcsncpy_s(&Dst, 0x105ui64, *(const wchar_t **)Buffer);
35     NetApiBufferFree(Buffer);
36 }
37 v2 = GetSAMLocation(servername, 0);
38 if ( v2 )
39 {
40     ErrorPrint(v2);
41     NetcmdExit(2);
42 }
43 v3 = NetUserEnum(servername, 0, 0x300u, &bufptr, 0xFFFFFFFF, &entriesread, &totalentries, 0i64);
44 if ( v3 == 254 )
45 {
46     v1 = 1;
47 }
48 else if ( v3 )
49 {
50     user_enum:26 (1400160EB)
```

Примеры вредоносных техник

РТ

netapi32! NetUserEnum

```
    ; Exported entry 237. NetUserEnum
    public NetUserEnum
    ; DWORD __stdcall NetUserEnum(LPCWSTR servername
53 41 4D 43 4C 49 2E 4E+NetUserEnum    db 'SAMCLI.NetUserEnum',0
65 74 55 73 65 72 45 6E+                ; DATA X
4E 65 74 55 73 65 72 47+aNetusergetgrou db 'NetUserGetGroups',0 ; DATA X
    ; Exported entry 238. NetUserGetGroups
    public NetUserGetGroups
    ; DWORD __stdcall NetUserGetGroups(LPCWSTR serve
53 41 4D 43 4C 49 2E 4E+NetUserGetGroups db 'SAMCLI.NetUserGetGroups',0
65 74 55 73 65 72 47+aNetusergetgrou db 'NetUserGetGroups',0
```

net1.exe - PID: E54 - Модуль: samcli.dll - Thread: Главный поток E58 - x64dbg [Elevated]

Файл Вид Отладка Трассировка Модули Избранное Параметры Справка Mar 10 2019

CPU График Журнал Заметки Точки останова Карта памяти

Адрес	Диспетчер	Комментарий
000007FEFA9F63A0	48:8BC4	mov rax, rsp
000007FEFA9F63A3	48:8958 08	mov qword ptr ds:[rax+8], rbx
000007FEFA9F63A7	4C:8948 20	mov qword ptr ds:[rax+20], r9
000007FEFA9F63AB	55	push rbp
000007FEFA9F63AC	56	push rsi
000007FEFA9F63AD	57	push rdi
000007FEFA9F63AE	41:54	push r12
000007FEFA9F63B0	41:55	push r13
000007FEFA9F63B2	41:56	push r14
000007FEFA9F63B4	41:57	push r15
000007FEFA9F63B6	48:81EC D0000000	sub rsp, D0
000007FEFA9F63B8	4C:8BC4 48010000	mov r15, qword ptr ss:[rsp+14]

rax=0
sp=0000000000015EF40
text: 000007FEFA9F63A0 samcli.dll:\$63A0 #59A0 <NetUserEnum>

Дамп 1	Дамп 2	Дамп 3	Дамп 4	Дамп 5	Просмотр 1
Адрес	Шестнадцатеричное	Шестнадцатеричное	Шестнадцатеричное	Шестнадцатеричное	ASCII
000000077361000	00 00 00 00 85 1C 6E 5C	00 00 00 00 02 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000077361010	22 00 00 00 D4 B2 00 00	D4 A6 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
000000077361020	C8 68 38 77 00 00 00 00	28 69 38 77 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	èh;w...
000000077361030	E8 68 38 77 00 00 00 00	08 69 38 77 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	èh;w...
000000077361040	28 69 38 77 00 00 00 00	28 69 38 77 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	(i;w...

Примеры вредоносных техник

PT

samcli! NetUserEnum

```
318 while ( 1 )
319 {
320     if ( v65 )
321     {
322         v32 = v34;
323     }
324     else if ( v33 )
325     {
326         v53 = UserpComputeSamPrefMaxLen(v11, v28, v36, v30);
327         v54 = v53;
328         v55 = SamEnumerateUsersInDomain(v61, &v63, v18, &v65, v53, &v62);
329         v35 = v78;
330         v30 += v54;
331         v32 = v55;
332         v59 = v30;
333         v37 = v77;
334     }
335 }
00002574 NetUserEnum:315 (180003174)
```

Instruction Data Unexplored External symbol Lumina function			
IDA View-A Pseudocode-A Hex View-1 Structures			
Address	Ordinal	Name	Library
000000018...		SamEnumerateUsersInDomain	SAMLIB

Примеры вредоносных техник

PT

samlib! SamEnumerateUsersInDomain

Номер процедуры: 13 и 72

```
55  if ( v15 )
56  {
57      if ( v15 != 1 )
58          return 3221225659i64;
59      LODWORD(v27) = v11;
60      LODWORD(v25) = v12;
61      LODWORD(v24) = v31;
62      v16.Pointer = NdrClientCall13(&pProxyInfo, 72u, 0i64, v28.Simple, v8, v24, v25, &hMem, v27, v14).Pointer;
63      v17 = (unsigned int)v16.Pointer;
64      v28.Pointer = v16.Pointer;
65  }
66  else
67  {
68      LODWORD(v26) = v11;
69      LODWORD(v24) = v31;
70      v29.Pointer = NdrClientCall13(&pProxyInfo, 13u, 0i64, v28.Simple, v8, v24, &hMem, v26, v14).Pointer;
71      v17 = (unsigned int)v29.Pointer;
72  }
73  v18 = hMem;
74  if ( hMem )
75  {
0000FF0 SamEnumerateUsersInDomain:52 (180001BF0)
```


Примеры вредоносных техник

ID интерфейса: 12345778-1234-ABCD-EF00-0123456789AC

```
00 00 00 00 00 00 00 00 align 10h
60 00 00 00 dword_1800122B0 dd 60h

78 db 78h ; x
57 db 57h ; W
34 db 34h ; 4
12 db 12h
34 db 34h ; 4
12 db 12h
CD db 0CDh ; H
AB db 0ABh ; «
EF db 0EFh ; n
00 db 0
01 db 1
23 db 23h ; #
45 db 45h ; E
67 db 67h ; g
89 db 89h ; %
AC db 0ACh ; -
01 db 1
```

Примеры вредоносных техник

PT

Filter by title

Technical Documents

Technical Documents

▼ [MS-SAMR]: Security

Account Manager (SAM)

Remote Protocol (Client-to-Server)

[MS-SAMR]: Security

2.1 Transport

04/07/2021 • 2 minutes to read

This protocol configures the RPC runtime to perform a strict [Network Data Representation \(NDR\)](#) data consistency check at target level 5.0, as specified in [\[MS-RPCE\]](#) section 3.

This protocol uses [UUID 12345778-1234-ABCD-EF00-0123456789AC](#) to id interface.

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-samr/084da2e7-0ba0-44fc-8f17-e8a200c69eb5

3.1.5.2.5 SamrEnumerateUsersInDomain (Opnum 13)

02/14/2019 • 2 minutes to read

The [SamrEnumerateUsersInDomain](#) method enumerates all users.

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-samr/6bdc92c0-c692-4ffb-9de7-65858b68da75

rpcmon Time = 1234567890.123456, PID = 264, PPID = 3876, TID = 3864, ProcessName =
"\\Device\\HarddiskVolume2\\Windows\\System32\\net1.exe", Method = **NdrClientCall3**, Event =
"api_called", CalledFrom = 0x7FEFC1C46B1, ReturnValue = 0x0, pStubProxy = 0x7fefc1ce640,
ProcedureNumber = 13, **InterfaceId = "12345778-1234-ABCD-EF00-0123456789AC"**,
TransferSyntax = "8A885D04-1CEB-11C9-9FE8-08002B104860"

PT

Поведенческий анализ

Образ win7-sp1-x64

[Скачать результаты анализа](#)

The diagram illustrates the execution of a process named 'net.exe' (pid 2676) which creates another process 'net.exe' (pid 266). This second process then performs several actions: it creates three processes named 'pipe.exe' (pids 267, 268, and 269), reads files 'lsrpe', 'smrv', and 'wlaavc', and writes to files 'lsrpe' and 'lsrpe'. The diagram also shows a 'delete' action on the 'net.exe' (pid 266) process.

Результат поведенческого анализа

Угроз не обнаружено

Поведенческий анализ

Потенциально опасное поведение

Create.Process.Net.SystemManagement

Read.System.SAMserv.AccountManipulation

Примеры вредоносных техник



T1563/002: Remote Service Session Hijacking: RDP Hijacking

MITRE | ATT&CK

MatricesTacticsTechniquesMitigationsGroupsSoftwareResourcesBlogContribute

Search

TECHNIQUES

- Enterprise
- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion

Home > Techniques > Enterprise > Remote Service Session Hijacking > RDP Hijacking

Remote Service Session Hijacking: RDP Hijacking

Other sub-techniques of Remote Service Session Hijacking (2)

Adversaries may hijack a legitimate user's remote desktop session to move laterally within an environment. Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).^[1]

Adversaries may perform RDP session hijacking which involves stealing a legitimate user's remote session. Typically, a user is notified when someone else is trying to steal their session. With System permissions and using Terminal Services Console,

```
c:\windows\system32\tscon.exe [session number to be stolen], an adversary can
```

ID: T1563.002

Sub-technique of: T1563

Tactic: Lateral Movement

Platforms: Windows

Permissions Required: SYSTEM

Data Sources: Authentication logs, Netflow/Enclave netflow, Process monitoring

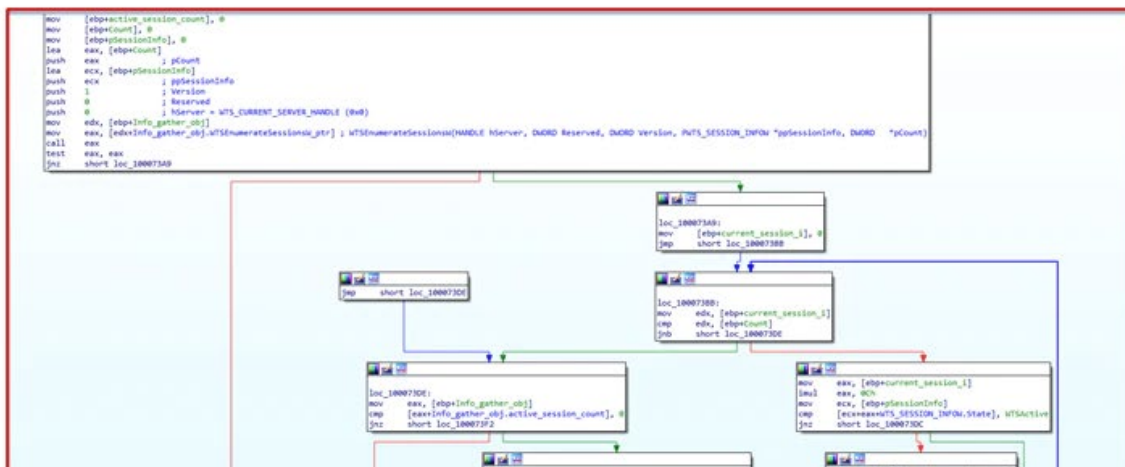
Version: 1.0

Created: 25 February 2020

PT

3. It keeps track of the number of drives previously seen and will return 1 if the number has increased

The RDP session tracking function operates the same as the drive tracking. If the number increases by one it then returns 1. It uses `WTSEnumerateSessionsW` to get a list of sessions, iterates through them to count active ones.



Операция North Star

Torisma

<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-behind-the-scenes/>

Примеры вредоносных техник

Червь WannaCry

- t.wnry, encrypted using the WANACRY! encryption format, where "WANACRY!" is the file header
- taskdl.exe, (hash 4a468603fdb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79), file deletion tool
- taskse.exe, (hash 2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d), enumerates Remote Desktop Protocol (RDP) sessions and executes the malware on each session
- u.wnry (hash b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25), "@WanaDecryptor@.exe" decrypter file

After dropping these files to its working directory, the malware attempts to change the attributes of all the files to "hidden" and grant full access to all files in the current directory and any directories below. It does this by executing "attrib +h .", followed by "icacls . /grant Everyone:F /T /C /Q".

```
push    ebx                ; lpExitCode
push    ebx                ; dwMilliseconds
push    offset CommandLine ; "attrib +h ."
call    sub_401064
push    ebx                ; lpExitCode
push    ebx                ; dwMilliseconds
push    offset aIcacs_GrantEv ; "icacls . /grant Everyone:F /T /C /Q"
call    sub_401064
add     esp, 20h
```

<https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/>

Примеры вредоносных техник

Рассматриваемая команда: вызов API-функции `WTSEnumerateSessionsW` из библиотеки `wsapi32.dll`


```
25 v5 = 0;
26 v6 = a4;
27 v25 = 0i64;
28 if ( a2 || a3 != 1 )
29 {
30     SetLastError(0x57u);
31     v7 = a5;
32 }
33 else
34 {
35     v7 = a5;
36     if ( a4 && a5 )
37     {
38         if ( (unsigned __int3)WinStationEnumerateW(a1, &v25, &v26) )
39         {
40             if ( v25 && v26 )
41             {
42                 v8 = 0;
43                 v9 = v25 + 4;
44                 v10 = v26;
45             }
46         }
47     }
48 }
```

00001220 WTSEnumerateSessionsW:23 (130001E20)

Примеры вредоносных техник

winsta! WinStationEnumerateW

```
1 unsigned __int8 __fastcall WinStationEnumerateW(CPublicBinding *this,
2 {
3     unsigned int *v3; // rdi
4     struct _SESSIONIDW **v4; // rsi
5     CPublicBinding *v5; // rbp
6     int v6; // eax
7     int v7; // ebx
8     DWORD v9; // eax
9
10    v3 = a3;
11    v4 = a2;
12    v5 = this;
13    v6 = _tsrpcEnumerate(this, a2, a3);
14    v7 = v6;
15    if ( v6 == -2147023174 )
16        return Legacy_WinStationEnumerateW(v5, v4, v3);
17    if ( v6 >= 0 )
18        return 1;
19    _DbgPrintMessage(8, "_tsrpcEnumerate failed: 0x%x in %s", (unsigned
20    v9 = ConvertHRESULT2WIN32(v7);
21    SetLastError(v9);
22    return 0;
23 }
```



Примеры вредоносных техник

winsta, _tsrpcEnumerate


```
501 LABEL_56:  
502 v26 = CEnum::Open((CEnum *)&v99, v25);  
503 LODWORD(v4) = v26;  
504 if ( (v26 & 0x80000000) != 0 )  
505 {  
506     _DbgPrintMessage(8, "Enum->Open failed: 0x%x in %s", v26, "_tsrpcEnumerate");  
507     v40 = v85;  
508     goto LABEL_116;  
509 }  
510 v27.Pointer = CEnum::GetEnumResult((CEnum *)&v99, 1, (struct _SESSIONENUM **)&v27);  
511 LODWORD(v4) = v27.Pointer;  
512 if ( SLODWORD(v27.Pointer) < 0 )  
513 {  
514     _DbgPrintMessage(8, "GetEnumResult failed: 0x%x in %s", LODWORD(v27.Pointer),  
515     v40 = v85;  
516     goto LABEL_116;  
517 }  
00004BE8 ?_tsrpcEnumerate@@YAJPEAXPEAPEAU_SESSIONIDW@@PEAK@Z:502 (1800057E8)
```

Примеры вредоносных техник

winsta, CEnum::GetEnumResult

Номер процедуры: 5

```
1 CLIENT_CALL_RETURN __fastcall CEnum::GetEnumResult(CEnum *this, int a2, struct _SESSIONENUM **a3, u
2 {
3     CLIENT_CALL_RETURN result; // rax
4     int v5; // [rsp+28h] [rbp-30h]
5
6     v5 = a2;
7     result.Pointer = NdrClientCall3(&stru_180030190, 5u, 0i64, *(_QWORD *)this, a3, v5, a4).Pointer;
8     return (CLIENT_CALL_RETURN)LODWORD(result.Pointer);
9 }
```



PT

ID интерфейса: 88143FD0-C28D-4B2B-8FEF-8D882F6A9390

```

60 00 00 00      dword_180032330 dd 60h
D0               db 0D0h ; P
3F               db 3Fh ; ?
14               db 14h
88               db 88h ; €
8D               db 8Dh ; Ĭ
C2               db 0C2h ; B
2B               db 2Bh ; +
4B               db 4Bh ; K
8F               db 8Fh ; Ÿ
EF               db 0EFh ; n
8D               db 8Dh ; Ĭ
88               db 88h ; €
2F               db 2Fh ; /
6A               db 6Ah ; j
93               db 93h ; “
90               db 90h ; ħ
01               db 1

```

Примеры вредоносных техник

PT

LSM Enumeration (tspubrpc.idl)<8>	{ 88143fd0-c28d-4b2b-8fef-8d882f6a9390 }	\PIPE\LSM_API_service \PIPE\UNIFIED_API_service<9>
--------------------------------------	--	---

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-tsts/4f5ff568-2887-4c50-8b36-38bb85170b58

RpcGetEnumResult	Returns a structure of the type PSESSIONENUM containing the list of sessions currently running on the terminal server after applying the specified filter.
Opnum: 5	

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-tsts/635a479c-7213-426f-b6be-ffbe381c6302

rpcmon Time = 1234567890.123456, PID = 412, PPID = 2376, TID = 3152, ProcessName =
"\\Device\\HarddiskVolume2\\Users\\malware.exe", **Method** = **NdrClientCall3**, Event = "api_called",
CalledFrom = 0x7FEFD6E2A22, ReturnValue = 0x0, pStubProxy = 0x7fef700500,
ProcedureNumber = **5**, **InterfaceId** = **"88143FD0-C28D-4B2B-8FEF-8D882F6A9390"**,
TransferSyntax = "8A885D04-1CEB-11C9-9FE8-08002B104860"

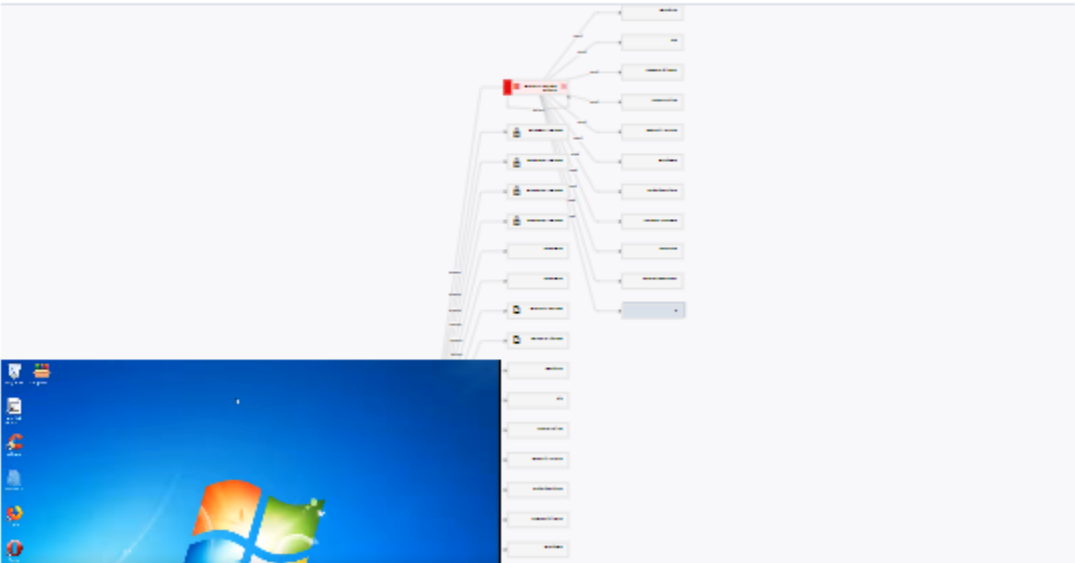
Примеры вредоносных техник

PT

Read.System.RDPSessions.Enumeration в PT Sandbox

Поведенческий анализ
Образ win7-sp1-x64

Скачать результаты анализа



Результат поведенческого анализа

Троян

Поведенческий анализ

Обнаруженное опасное ПО

Троян
Trojan.Win32.Generic.a

Потенциально опасное поведение

Read.System.RDPSessions.Enumeration

Полезные ссылки

PT



PT Sandbox

ptsecurity.com/ru-ru/products/sandbox/



PT ESC Threat Intelligence blog

ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/



PT ESC Incident Response Alert

ptsecurity.com/ru-ru/services/esc/



Вопросы

webinar@ptsecurity.com

Alexey Vishnyakov
avishnyakov@ptsecurity.com
Twitter: @Vishnyak0v

Повышение привилегий в системе:
детектирование техник на примере PT
Sandbox

<https://www.ptsecurity.com/ru-ru/research/webinar/povyshenie-privilegij-v-sisteme-detektirovanie-tehnik-na-primere-pt-sandbox/>

Плагин exploitmon для DRAKVUF.
Обнаружение эксплуатации ядра ОС с
помощью PT Sandbox

<https://www.ptsecurity.com/ru-ru/research/webinar/plugin-exploitmon-dlya-drakvuf-obnaruzhenie-ehkspluatacii-yadra-os-s-pomoshchyu-pt-sandbox/>