



POSITIVE
TECHNOLOGIES

Закрепление и уклонение от обнаружения: детектирование техник на примере 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.

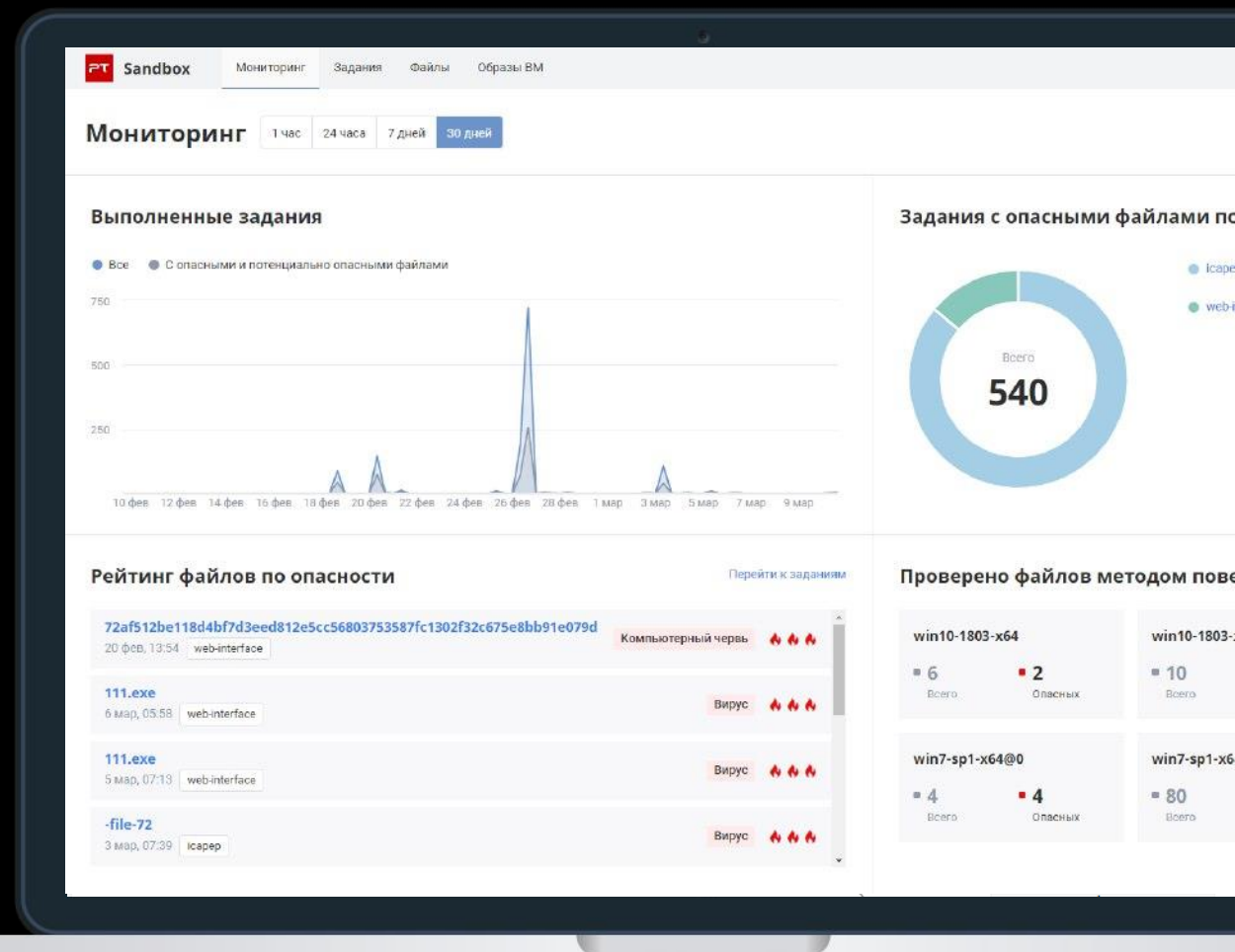
- Коротко о PT Sandbox
- Как работает безагентная песочница
- Техники автозапуска
- Техники выполнения по событию
- Техники внедрения в процессы

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



Как работает безагентная песочница



Positive Technologies — одни из
участников развития проекта DRAKVUF™

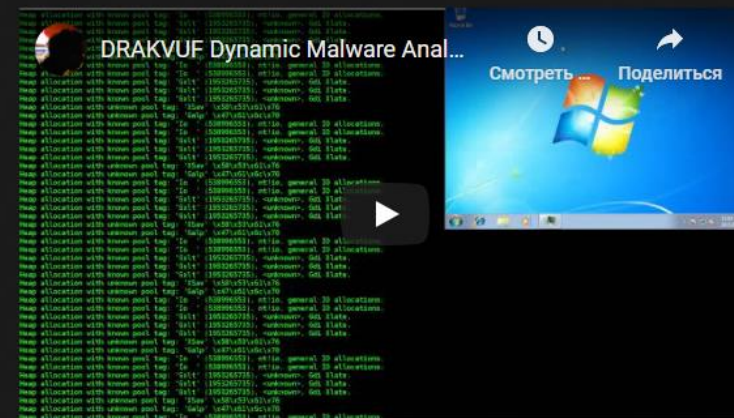
github.com/tklengyel/drakvuf

Malware analysis

DRAKVUF™ provides a perfect platform for stealthy malware analysis as its footprint is nearly undetectable from the malware's perspective. While DRAKVUF has been mainly developed with malware analysis in mind, it is certainly not limited to that task as it can be used to monitor the execution of arbitrary binaries.

Demos

Using DRAKVUF™ to trace Windows internal kernel functions, including heap allocations.



Как работает безагентная песочница

РТ

Гипервизор Xen



Виртуальная
машина №1



Виртуальная
машина №2



Виртуальная
машина №3

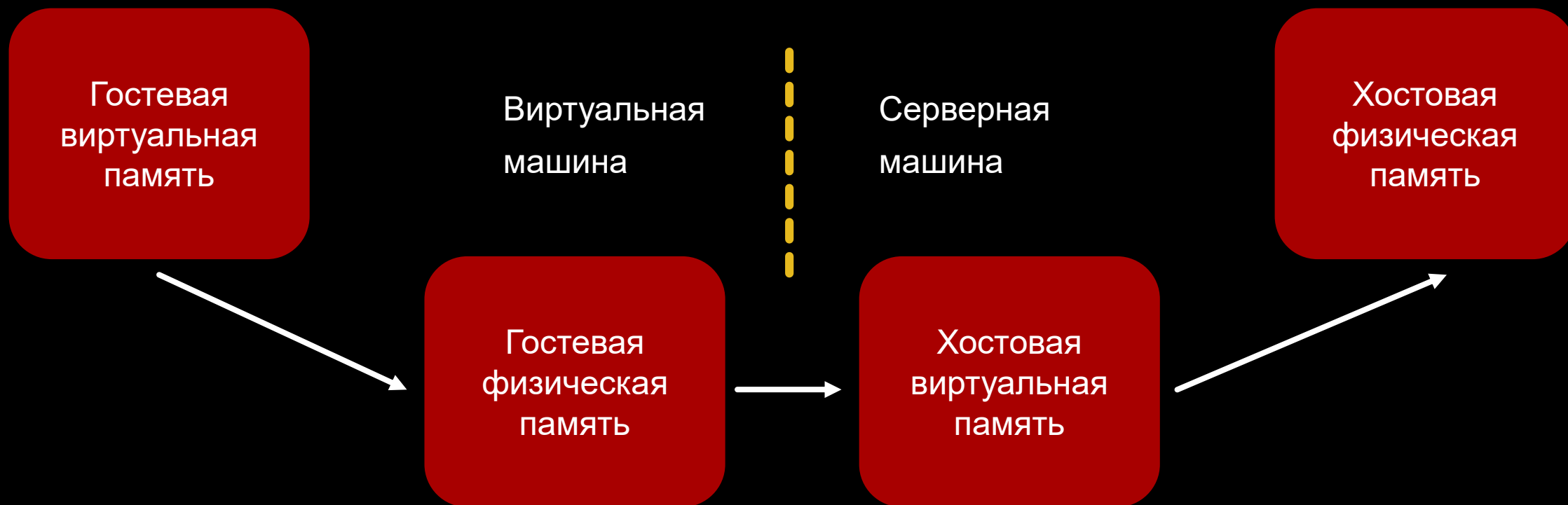


Виртуальная
машина №n

Как работает безагентная песочница

РТ

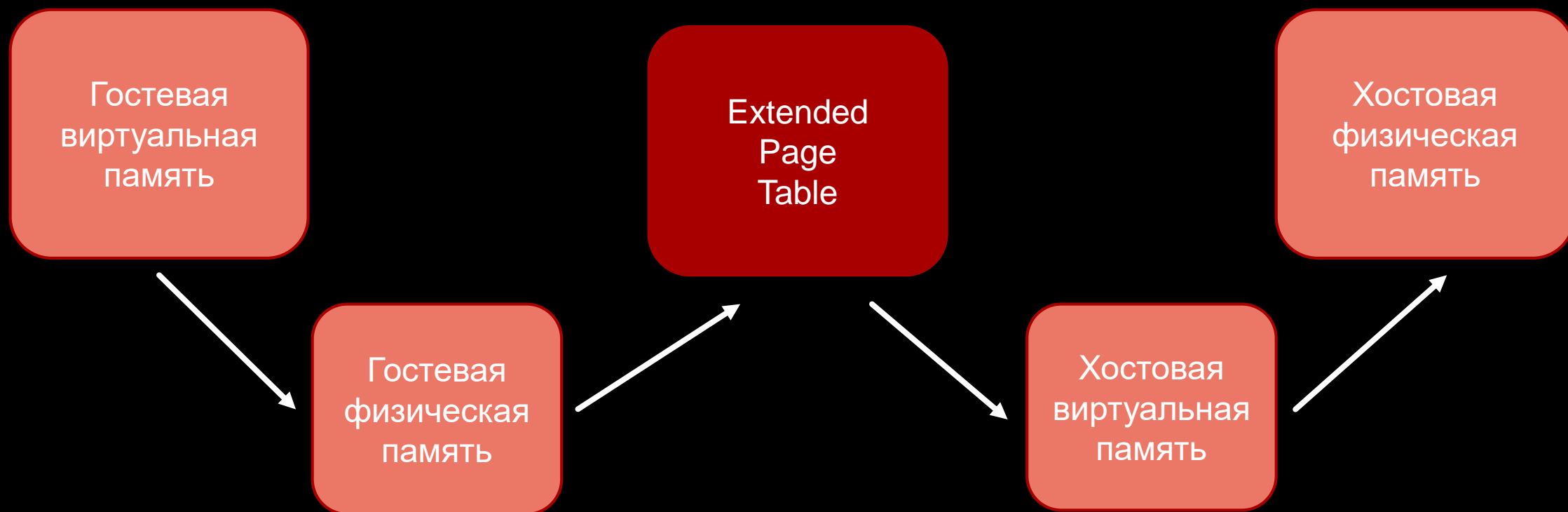
Трансляция адресов



Как работает безагентная песочница

РТ

Технология SLAT




Как работает безагентная песочница



Перехват событий

- Найти в памяти интересующий фрагмент кода или данных
- Изменить права доступа соответствующей страницы памяти (4 Кб)
- Поймать исключение (#PF)
- Обработать событие
- Восстановить права доступа страницы памяти

Техники автозапуска



*HKCU\Software\
Microsoft\Windows\
CurrentVersion\Run*

- Используется в >70% вредоносного ПО
- Наиболее часто встречаемая техника закрепления через реестр Windows

Техники автозапуска



- HKCU\Software\Policies\Microsoft\Windows\System\Scripts* (Script)
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\AppKey* (ShellExecute)
- HKLM\SYSTEM\CurrentControlSet\Control\BootVerificationProgram (ImageName)
- ... saule-spb.ru/library/autorun.html

regmon Time = 1234567890.123456, PID = 1660, PPID = 3636, TID = 920, ProcessName =
"\\Device\\HarddiskVolume2\\Windows\\System32\\malware.exe", Method = **NtSetValueKey**, Key =
"\\REGISTRY\\USER\\S-1-5-21-2110523999-2054815194-2341945532-1001\\ENVIRONMENT", ValueName =
"**UserInitMprLogonScript**", Value = "C:\\TMP\\mim.exe sekurlsa::LogonPasswords > C:\\TMP\\o.txt"

Техники автозапуска



- %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup
- %ProgramData%\Microsoft\Windows\Start Menu\Programs\Startup
- %windir%\Start Menu\Programs\StartUp
- ...

filetracer Time = 1234567890.123456, PID = 3656, PPID = 1252, TID = 1136, ProcessName =
"\\Device\\HarddiskVolume2\\Windows\\System32\\malware.exe", Method = **NtWriteFile**, FileName =
"\\Users\\Victim\\AppData\\Roaming\\Microsoft\\Windows**Start Menu\\Programs\\Startup\\Updater.lnk**",
FileHandle = 0x60

Техники автозапуска

PT

Планировщик задач

Operation TaskMasters:

ptsecurity.com/ru-ru/research/analytics/operation-taskmasters-2019/



Техники автозапуска



Задача: как обнаружить следующий вызов?

```
schtasks.exe /create /sc daily /tn "Malware task" /TR  
"C:\Windows\System32\malware.exe" /ST 12:34
```

Техники автозапуска



1) Создание процесса schtasks.exe

procmon Time = 1234567890.123456, PID = 2000, PPID = 1252, TID = 3592, ProcessName =
"\Device\HarddiskVolume2\Windows\System32\cmd.exe", Method = **NtCreateUserProcess**, Status
= 0x0, NewProcessHandle = 0x5C, NewPid = 3476, NewThreadHandle = 0x60, NewTid = 2364,
CommandLine = "schtasks.exe /create /sc daily /tn \"Malware task\" /TR
\"C:\\Windows\\System32\\malware.exe\" /ST 12:34", ImagePathName =
"C:**Windows\\system32\\schtasks.exe**", CWD = "C:\\Users\\Victim\\Desktop\\"

Техники автозапуска

PT

2) COM интерфейс

Стадия закрепления

Планирование задач с помощью COM интерфейсов

Вебинар «Mlw #41: новый сложный загрузчик АРТ-группировки TA505»: ptsecurity.com/ru-ru/research/webinar/309243/

```
if ( (*(&advapi32_GetUserNameW + v14))(var_lpBuffer, &var_pcbBuffer) )
{
    var_username = var_lpBuffer;
    var_username2 = var_lpBuffer;
}
else
{
    fVirtualFree(var_lpBuffer);
}
if ( !var_username )
    goto LABEL_55;
var_ppFolder->lpVtbl->DeleteTask(var_ppFolder, var_numstr->str, 0);
if ( var_ppv->lpVtbl->NewTask(var_ppv, 0, &var_ppDefinition) )
    goto LABEL_55;
var_ppRegistrationInfo = 0;
if ( !var_ppDefinition->lpVtbl->get_RegistrationInfo(var_ppDefinition, &var_ppRegistrationInfo) )
{
    var_ppRegistrationInfo->lpVtbl->put_Author(var_ppRegistrationInfo, var_username);
    var_ppRegistrationInfo->lpVtbl->Release(var_ppRegistrationInfo);
}
var_ppSettings = 0;
if ( !var_ppDefinition->lpVtbl->get_Settings(var_ppDefinition, &var_ppSettings) )
{
    var_ppSettings->lpVtbl->put_StartWhenAvailable(var_ppSettings, 1);
    var_ppSettings->lpVtbl->put_Hidden(var_ppSettings, 1);
    var_ppSettings->lpVtbl->put_DisallowStartIfOnBatteries(var_ppSettings, 0);
    var_ppSettings->lpVtbl->put_StopIfGoingOnBatteries(var_ppSettings, 0);
    var_PT0S[0] = 'P';
    var_PT0S[1] = 'T';
    var_PT0S[2] = '0';
    var_PT0S[3] = 'S';
}
```

Техники автозапуска



2) COM интерфейс

Событие №1

regmon Time = 1234567890.123456, PID = 3476, PPID = 2000, TID = 2364, ProcessName =
"\\Device\\HarddiskVolume2\\Windows\\System32\\malware.exe", Method = **NtOpenKeyEx**, Key =
"\\REGISTRY\\USER\\S-1-5-21-2110523999-2054815194-2341945532-1001_CLASSES\\CLSID\\{0F87369F-A4E5-
4CFC-BD3E-73E6154572DD}"

Техники автозапуска

PT

2) COM интерфейс

Событие №1

Abusing COM & DCOM objects:

[dl.packetstormsecurity.net/papers/g
eneral/abusing-objects.pdf](http://dl.packetstormsecurity.net/papers/general/abusing-objects.pdf)

HA3C03

Abusing COM & DCOM objects

COM object with CLSID {0F87369F-A4E5-4CFC-BD3E-73E6154572DD}:

This com object implements the Schedule.Service class for operating the Windows Task Scheduler Service. This COM object allows privileged users to schedule a task on a host **(including a remote host)** without using the schtasks.exe binary or the schtasks.exe at command. [2]

```
$TaskName = [Guid]::NewGuid().ToString()
$Instance = [activator]::CreateInstance([type]::GetTypeFromProgID("Schedule.Service"))
$Instance.Connect()
$Folder = $Instance.GetFolder("")
$Task = $Instance.NewTask(0)
$Trigger = $Task.triggers.Create(0)
$Trigger.StartBoundary = Convert-Date -Date ((Get-Date).addSeconds($Delay))
$Trigger.EndBoundary = Convert-Date -Date ((Get-Date).addSeconds($Delay + 120))
$Trigger.ExecutionTimelimit = "PT5M"
```

Техники автозапуска



2) COM интерфейс

События №2 и №3

regmon Time = 1234567890.123456, PID = 816, PPID = 436, TID = 1584, ProcessName =
"\\Device\\HarddiskVolume2\\Windows\\System32\\svchost.exe", Method = **NtSetValueKey**, Key =
"\\REGISTRY\\MACHINE\\SOFTWARE\\MICROSOFT\\WINDOWS NT\\CURRENTVERSION**SCHEDULE\\TASKCACHE\\TASKS\\{0AE30475-**
C7BE-4E6A-BD96-356C6BDA513C}", ValueName = "Path", Value = "\\Malware task"

regmon Time = 1234567890.123456, PID = 816, PPID = 436, TID = 1584, ProcessName =
"\\Device\\HarddiskVolume2\\Windows\\System32\\svchost.exe", Method = **NtSetValueKey**, Key =
"\\REGISTRY\\MACHINE\\SOFTWARE\\MICROSOFT\\WINDOWS NT\\CURRENTVERSION**SCHEDULE\\TASKCACHE\\TREE\\MALWARE**
TASK", ValueName = "Id", Value = "{**0AE30475-C7BE-4E6A-BD96-356C6BDA513C}**"

Техники автозапуска



2) COM интерфейс

Событие №4

filetracer Time = 1234567890.123456, PID = 816, PPID = 436, TID = 1584, ProcessName =
"\Device\HarddiskVolume2\Windows\System32\svchost.exe", Method = **NtWriteFile**, FileName =
"\Windows\System32\Tasks\Malware task", FileHandle = 0x1078

Техники автозапуска



regmon Time = 1234567890.123456, PID = 816, PPID = 436, TID = 1584, **ProcessName** =
"**\Device\HarddiskVolume2\Windows\System32\svchost.exe**", Method = NtSetValueKey, Key =
"\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TASKS\{0AE30475-
C7BE-4E6A-BD96-356C6BDA513C}", ValueName = "Path", Value = "\Malware task"

regmon Time = 1234567890.123456, PID = 816, PPID = 436, TID = 1584, **ProcessName** =
"**\Device\HarddiskVolume2\Windows\System32\svchost.exe**", Method = NtSetValueKey, Key =
"\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TREE\MALWARE
TASK", ValueName = "Id", Value = "{0AE30475-C7BE-4E6A-BD96-356C6BDA513C}"

filetracer Time = 1234567890.123456, PID = 816, PPID = 436, TID = 1584, **ProcessName** =
"**\Device\HarddiskVolume2\Windows\System32\svchost.exe**", Method = NtWriteFile, FileName =
"\Windows\System32\Tasks\Malware task", FileHandle = 0x1078

Техники автозапуска



`schtasks.exe -> TaskScheduler COM`

Техники автозапуска



Вызовы объектов TaskScheduler COM

apimon Time = 1234567890.123456, PID = 3476, PPID = 2000, TID = 2364, ProcessName =
"\\Device\\HarddiskVolume2\\Windows\\System32\\schtasks.exe", Method = **ITaskService::NewTask**, Event = "api_called", CLSID = "**0F87369F-A4E5-4CFC-BD3E-73E6154572DD**", CalledFrom = 0xFF1FB067, ReturnValue = 0x0, Arg0 = 0x447df0, Arg1 = 0x0, Arg2 = 0x4462b0

apimon Time = 1234567890.123456, PID = 3476, PPID = 2000, TID = 2364, ProcessName =
"\\Device\\HarddiskVolume2\\Windows\\System32\\schtasks.exe", Method = **IExecAction::put_Path**, Event = "api_called", CLSID = "0F87369F-A4E5-4CFC-BD3E-73E6154572DD", CalledFrom = 0xFF1FA6A5, ReturnValue = 0x0, Arg0 = 0x446740, Arg1 =
"**C:\\Windows\\System32\\malware.exe**"

apimon Time = 1234567890.123456, PID = 3476, PPID = 2000, TID = 2364, ProcessName =
"\\Device\\HarddiskVolume2\\Windows\\System32\\schtasks.exe", Method = **ITaskFolder::RegisterTaskDefinition**, Event = "api_called", CLSID = "0F87369F-A4E5-4CFC-BD3E-73E6154572DD", CalledFrom = 0xFF1FB566, ReturnValue = 0x0, Arg0 = 0x31ff70, Arg1 = "**Malware task**",
Arg2 = 0x4462b0, Arg3 = 0x2, Arg4 = 0x1dcda0, Arg5 = 0x1dcde0, Arg6 = 0x3, Arg7 = 0x1dcdc0, Arg8 = 0x446a90

Техники автозапуска



А что насчёт at.exe?

Техники автозапуска



Задача: как обнаружить следующий вызов?

```
sc.exe create MalwareService binPath= C:\Windows\malware.exe
```


Техники автозапуска



Задача: как обнаружить следующий вызов?

sc.exe create MalwareService binPath= C:\Windows\malware.exe

DESCRIPTION:

Creates a service entry in the registry and Service Database.

USAGE:

sc <server> create [service name] [binPath=] <option1> <opti

OPTIONS:

NOTE: The option name includes the equal sign.

A space is required between the equal sign and the value.

type= <own|share|interact|kernel|filesys|rec|userown|usershare>
(default = own)

start= <boot|system|auto|demand|disabled|delayed-auto>
(default = demand)

error= <normal|severe|critical|ignore>
(default = normal)

binPath= <BinaryPathName to the .exe file>

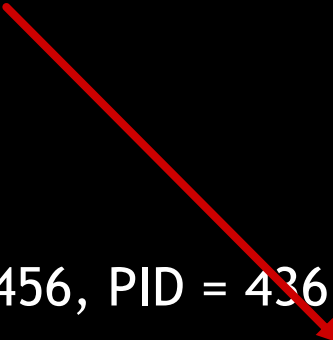
group= <LoadOrderGroup>

tag= <value>

Техники автозапуска



Создание службы



```
regmon Time = 1234567890.123456, PID = 436, PPID = 344, TID = 672, ProcessName =  
"\Device\HarddiskVolume2\Windows\System32\services.exe", Method = NtSetValueKey,  
Key = "\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\SERVICES\MALWARESERVICE",  
ValueName = "ImagePath", Value = "C:\Windows\malware.exe"
```

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  ms_exc_registration.TryLevel = 1;
95  v16 = NdrClientCall4(
96      &off_10001080,
97      dword_10003AAC,
98      hSCManager,
99      v24,
100     v23,
101     dwDesiredAccess,
102     dwServiceType,
103     dwStartType,
104     dwErrorControl,
105     v22,
```


Техники автозапуска

PT

367ABB81-9844-35F1-AD32-98F038001003 - \PIPE\svcctl

docs.microsoft.com/en-us/openspecs/windows_protocols/ms-scmr/4c8b7701-b043-400c-9350-dc29cfaa5e7a

```
.text:10008D78 44 00 00 00      dword_10008D78 dd 44h      ; DATA XREF: .text:off_10001080fo
.text:10008D7C 81              db 81h ; f      ; 367abb81-9844-35f1-ad32-98f038001003
.text:10008D7D BB              db 0BBh ; »
.text:10008D7E 7A              db 7Ah ; z
.text:10008D7F 36              db 36h ; 6
.text:10008D80 44              db 44h ; D
.text:10008D81 98              db 98h
.text:10008D82 F1              db 0F1h ; c
.text:10008D83 35              db 35h ; 5
.text:10008D84 AD              db 0ADh ; -
.text:10008D85 32              db 32h ; 2
.text:10008D86 98              db 98h
.text:10008D87 F0              db 0F0h ; p
.text:10008D88 38              db 38h ; 8
.text:10008D89 00              db 0
.text:10008D8A 10              db 10h
.text:10008D8B 03              db 3
```



Техники автозапуска



Так, что там с at.exe?

Техники автозапуска

at.exe -> NetScheduleJobAdd (schedcli.dll)

```
1 DWORD __stdcall JobAdd()  
2 {  
3     DWORD v0; // esi  
4     char v2; // [esp+0h] [ebp-Ch]  
5  
6     while ( 1 )  
7     {  
8         v0 = NetScheduleJobAdd(GlobalServerName, &GlobalAtInfo, &GlobalJobId);  
9         if ( v0 != 87 || !(byte_406A89 & 0x10) )  
10            break;  
11         byte_406A89 &= 0xEFu;  
12     }  
13     if ( v0 )  
14     {  
15         if ( !MessagePrint(v0, v2) )  
16             _exit(1);  
17     }  
18     else  
19     {  
20         MessagePrint(0x2713u, GlobalJobId);  
21     }  
22     return v0;  
23 }
```

Техники автозапуска

NetScheduleJobAdd (schedcli.dll) -> NdrClientCall4 (RPCRT4.dll)

```
1 DWORD __stdcall NetScheduleJobAdd(LPCWSTR Servername, LPBYTE Buffer, LPDWORD JobId)
2 {
3     signed int v3; // esi
4     unsigned int v4; // eax
5     int v6; // [esp+1Ch] [ebp-1Ch]
6
7     v6 = 0;
8     v3 = _NdrClientCall4(&off_10001008, &word_100013A2, Servername, Buffer, JobId);
9     if ( v3 == 2470 )
10         v6 = 1;
11     if ( v6 )
12         v3 = 50;
13     if ( v3 > 0 )
14         v4 = (unsigned __int16)v3 | 0x80070000;
15     else
16         v4 = v3;
17     TschedSqm::SendApiUsageData(v4);
18     return v3;
19 }
```

Техники автозапуска

PT

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 ; ч  
.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 ; m  
.text:10001496 74                db 74h ; t  
.text:10001497 0B                db 0Bh  
.text:10001498 E8                db 0E8h ; и  
.text:10001499 CE                db 0CEh ; O  
.text:1000149A E9                db 0E9h ; й  
.text:1000149B 8B                db 8Bh ; <
```



Техники автозапуска



apimon Time = 1234567890.123456, PID = 1352, PPID = 3012, TID = 824, ProcessName =
"\\Device\\HarddiskVolume2\\Windows\\System32\\sc.exe", Method = **CreateServiceW**, CalledFrom =
0xFF2B1822, ReturnValue = 0x406600, hSCManager = 0x4065d0, lpServiceName =
"MalwareService", lpDisplayName = "", dwDesiredAccess = 0xf01ff, dwServiceType = 0x10,
dwStartType = 0x3, dwErrorControl = 0x1, lpBinaryPathName = **"C:\\Windows\\malware.exe"**,
lpLoadOrderGroup = "", lpdwTagId = 0x0, lpDependencies = "", lpServiceStartName = "",
lpPassword = ""

rpcmon Time = 1234567890.123456, PID = 1352, PPID = 3012, TID = 824, ProcessName =
"\\Device\\HarddiskVolume2\\Windows\\System32\\sc.exe", Method = **NdrClientCall2**, CalledFrom =
0x7FEFF076609, ReturnValue = 0x0, pStubDescriptor = 0x7feff075790, pFormat = 0x7feff073ac6,
InterfaceId = **"367ABB81-9844-35F1-AD32-98F038001003"**, TransferSyntax = "8A885D04-1CEB-
11C9-9FE8-08002B104860"

Техники выполнения по событию



AppCert DLLs — загрузка библиотек при старте процессов через CreateProcess/WinExec

regmon Time = 1234567890.123456, PID = 920, PPID = 3656, TID = 2516, ProcessName =
"\Device\HarddiskVolume2\Windows\System32\malware.exe", Method = **NtSetValueKey**, Key =
"\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER\APPCERTDLLS",
ValueName = "foobar", Value = "C:\malware.dll"

Техники выполнения по событию



(Load)AppInit DLLs — загрузка библиотек при использовании user32.dll

regmon Time = 1234567890.123456, PID = 2516, PPID = 3636, TID = 3288, ProcessName =
"\Device\HarddiskVolume2\Windows\System32\malware.exe", Method = **NtSetValueKey**, Key =
"\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINDOWS",
ValueName = "**LoadAppInit_DLLs**", Value = "\"C:\malware.dll\""

Техники выполнения по событию



Image File Execution Options — запуск процесса в качестве отладчика

```
regmon Time = 1234567890.123456, PID = 920, PPID = 3656, TID = 2516, ProcessName =  
"\Device\HarddiskVolume2\Windows\System32\malware.exe", Method = NtSetValueKey, Key =  
"\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE  
EXECUTION OPTIONS\notepad.exe", ValueName = "Debugger", Value = "C:\malware.exe /s"
```

Техники выполнения по событию



Shimming — перенаправление вызова символов из таблицы импорта исполняемого файла

filetracer Time = 1234567890.123456, PID = 2256, PPID = 1992, TID = 2784, ProcessName =
"\\Device\\HarddiskVolume2\\Windows\\System32\\malware.exe", Method = **NtWriteFile**, FileName =
"\\Windows\\AppPatch\\Custom\\{55aab41f-5d5c-abdf-4568-baef76587bd7}.sdb", FileHandle = 0x60

regmon Time = 1234567890.123456, PID = 2256, PPID = 1992, TID = 2784, ProcessName =
"\\Device\\HarddiskVolume2\\Windows\\System32\\malware.exe", Method = **NtSetValueKey**, Key =
"\\REGISTRY\\MACHINE\\SOFTWARE\\MICROSOFT**WINDOWS NT\\CURRENTVERSION**
APPCOMPATFLAGS\\CUSTOM\\SERVICES.EXE", ValueName = "{55aab41f-5d5c-abdf-4568-baef76587bd7}.sdb",
Value = "A0 EE E4 0C 27 30 D6 01"

Техники выполнения по событию



Windows hooking — выполнение кода при наступлении системных событий

syscall Time = 1234567890.123456, PID = 3040, PPID = 1324, TID = 1496, ProcessName =
"\\Device\\HarddiskVolume2\\Windows\\System32\\malware.exe", Method =
NtUserSetWindowsHookEx, Module = "win32k", vCPU = 1, CR3 = 0x5C5EB000, Syscall = 140, Mod =
0x74C10000, UnsafeModuleName = "C:\\Users\\Victim\\AppData\\Local\\Temp\\malware.dll", ThreadId
= 0x0, **HookId = 0xD**, HookProc = 0x74C11010, Ansi = 0x0

Техники внедрения в процессы

РТ

Внедрение в процесс



Передача управления

Техники внедрения в процессы



Внедрение в процесс

- NtWriteVirtualMemory (WriteProcessMemory)
- NtMapViewOfSection (MapViewOfSection)
- NtAddAtom + NtQueryInformationAtom (aka Atom Bombing)
- NtUserFindWindowEx/NtUserSetWindowLong (aka Extra Window)

Техники внедрения в процессы



Передача управления

- NtCreateThreadEx (CreateRemoteThread)
- NtQueueApcThread/NtQueueApcThreadEx (QueueUserAPC)
- NtGetContextThread/NtSetContextThread (SetThreadContext)
 - NtQueryInformationThread/NtSetInformationThread
(ThreadInformationClass=0x1D, WoW64)

Техники внедрения в процессы



Doppelganging, NtCreateTransaction

syscall Time = 1234567890.123456, PID = 2296, PPID = 1336, TID = 2620, ProcessName =
"\\Device\\HarddiskVolume2\\Users\\Victim\\Desktop\\malware.exe", Method = **NtCreateTransaction**,
Module = "nt", vCPU = 1, CR3 = 0x5FC38000, Syscall = 168, TransactionHandle = 0x19BED90,
DesiredAccess = 0x1F003F, ObjectAttributes = 0x19BED38, Uow = 0x0, TmHandle = 0x0,
CreateOptions = 0x0, IsolationLevel = 0x0, IsolationFlags = 0x0, Timeout = 0x0, Description = 0x0

Техники внедрения в процессы



Doppelganging, NtRollbackTransaction

syscall Time = 1234567890.123456, PID = 2296, PPID = 1336, TID = 2620, ProcessName =
"\\Device\\HarddiskVolume2\\Users\\Victim\\Desktop\\malware.exe", Method = **NtRollbackTransaction**,
Module = "nt", vCPU = 0, CR3 = 0x5FC38000, Syscall = 327, TransactionHandle = 0x150, Wait = 0x1

Техники внедрения в процессы



Doppelganging, NtCreateProcessEx

syscall Time = 1234567890.123456, PID = 2296, PPID = 1336, TID = 2620, ProcessName =
"\Device\HarddiskVolume2\Users\Victim\Desktop\malware.exe", Method = **NtCreateProcessEx**,
Module = "nt", vCPU = 0, CR3 = 0x5FC38000, Syscall = 74, ProcessHandle = 0x19BEE50,
DesiredAccess = 0x10000000, ObjectAttributes = 0x0, ParentProcess = 0xFFFFFFFFFFFFFFFF, Flags
= 0x4, SectionHandle = 0x15C, DebugPort = 0x0, ExceptionPort = 0x0, JobMemberLevel = 0x0

Техники внедрения в процессы



Doppelganging, NtWriteVirtualMemory

syscall Time = 1234567890.123456, PID = 2296, PPID = 1336, TID = 2620, ProcessName =
"\Device\HarddiskVolume2\Users\Victim\Desktop\malware.exe", Method = **NtWriteVirtualMemory**,
Module = "nt", vCPU = 0, CR3 = 0x5FC38000, Syscall = 55, **ProcessHandle = 0x160**, BaseAddress =
0x5C5060, Buffer = 0x5C5060, BufferSize = 0x1724, NumberOfBytesWritten = 0x19BED78

Техники внедрения в процессы



Doppelganging, NtCreateThreadEx

syscall Time = 1234567890.123456, PID = 2296, PPID = 1336, TID = 2620, ProcessName =
"\\Device\\HarddiskVolume2\\Users\\Victim\\Desktop\\malware.exe", Method = **NtCreateThreadEx**,
Module = "nt", vCPU = 0, CR3 = 0x5FC38000, Syscall = 165, ThreadHandle = 0x19BEE70,
DesiredAccess = 0x10000000, ObjectAttributes = 0x0, ProcessHandle = 0x160, StartRoutine =
0x1000170C0, Argument = 0x0, CreateFlags = 0x1, ZeroBits = 0x0, StackSize = 0x0,
MaximumStackSize = 0x0, AttributeList = 0x0

Техники внедрения в процессы



- NtUserMessageCall (aka Extra Window)
 - Msg=0xf (WM_PAINT)
- NtUserMessageCall (aka ListPlanting)
 - Msg=0x1030 (LVM_SORTITEMS)
 - Msg=0x109f (LVM_INSERTGROUPSORTED)
 - Msg=0x109e (LVM_SORTGROUPS)

Полезные ссылки



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

Кастомизация песочниц:
почему это нужно вам прямо сейчас

habr.com/ru/company/pt/blog/494240/

Детектирование техник обхода песочниц
и виртуализации на примере PT Sandbox

habr.com/ru/company/pt/blog/507912/

Alexey Vishnyakov

avishnyakov@ptsecurity.com

Twitter: @Vishnyak0v