

Ampire 360°



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Ampire 360°

ПОЛИГОН КИБЕРБЕЗОПАСНОСТИ



Threat Intelligence

SOC & DFIR

Offensive Security

Киберучения

ИИ и киберзащита

Киберполигон Ampire

📅 14 октября





Устройство сервисов ОС Windows и эксплойты семейства Potato

Василий Кравец

Начальник отдела ИИТ

Перспективный мониторинг



Обо мне

Ampire 360°

CVE-2019-14743

CVE-2019-15316

CVE-2019-17180

CVE-2019-19247

CVE-2019-19248

CVE-2019-20383

CVE-2020-23967

CVE-2021-25261

CVE-2021-25263

CVE-2022-28226

CVE-2022-28225

CVE-2023-5993

CVE-2023-7016



Базовая информация о сервисах

ImagePath – путь к
исполняемому файлу

ObjectName – имя пользователя

Start – способ запуска

Имя	Тип	Значение
 (По умолчанию)	REG_SZ	(значение не присвоено)
 DependOnService	REG_MULTI_SZ	rpcss
 Description	REG_SZ	@%SystemRoot%\system32\msimsg.dll,-32
 DisplayName	REG_SZ	@%SystemRoot%\system32\msimsg.dll,-27
 ErrorControl	REG_DWORD	0x00000001 (1)
 FailureActions	REG_BINARY	84 03 00 00 00 00 00 00 00 00 00 00 03 00 00 00 14 00 00 00 01 00 00
 ImagePath	REG_EXPAND_SZ	%systemroot%\system32\msiexec.exe /V
 ObjectName	REG_SZ	LocalSystem
 RequiredPrivileges	REG_MULTI_SZ	SeTcbPrivilege SeCreatePagefilePrivilege SeLockMemoryPrivilege
 ServiceSidType	REG_DWORD	0x00000001 (1)
 Start	REG_DWORD	0x00000003 (3)
 Type	REG_DWORD	0x00000010 (16)

Пользователи

1. NT AUTHORITY\SYSTEM

2. NT AUTHORITY\LOCAL SERVICE

3. NT AUTHORITY\NETWORK SERVICE

4. Другие варианты

Доступ к сети: **anonymous**

Доступ к сети: **УЗ машины**

Эксплойты семейства Potato

Ampire 

1. Hot Potato
2. Smashed Potato
3. Rotten Potato
4. Lonely Potato
5. Juicy Potato
6. Ghost Potato
7. Sweet Potato
8. Rogue Potato
9. Generic Potato
10. RemotePotato0



**Провокация
аутентификации**



**Привилегия
Selfpersonate**



**Получение прав
NT AUTHORITY\SYSTEM**

Больше информации о сервисах

RequiredPrivileges – список доступных привилегий

Type – флаги запуска (отдельный процесс или совместный)

Parameters\ServiceDll – путь к библиотеке

Имя	Тип	Значение
 (По умолчанию)	REG_SZ	(значение не присвоено)
 DependOnService	REG_MULTI_SZ	RpcSs http fdphost
 Description	REG_SZ	@%systemroot%\system32\fdrespub.dll,-101
 DisplayName	REG_SZ	Публикация ресурсов обнаружения функции
 ErrorControl	REG_DWORD	0x00000001 (1)
 FailureActions	REG_BINARY	80 51 01 00 00 00 00 00 00 00 03 00 00 00 14 00 00 00 01 00 00 00 c0 d4 01 00 01
 Group	REG_SZ	
 ImagePath	REG_EXPAND_SZ	%SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation -p
 ObjectName	REG_SZ	NT AUTHORITY\LocalService
 RequiredPrivileges	REG_MULTI_SZ	SeChangeNotifyPrivilege
 ServiceSidType	REG_DWORD	0x00000001 (1)
 Start	REG_DWORD	0x00000002 (2)
 Type	REG_DWORD	0x00000020 (32)

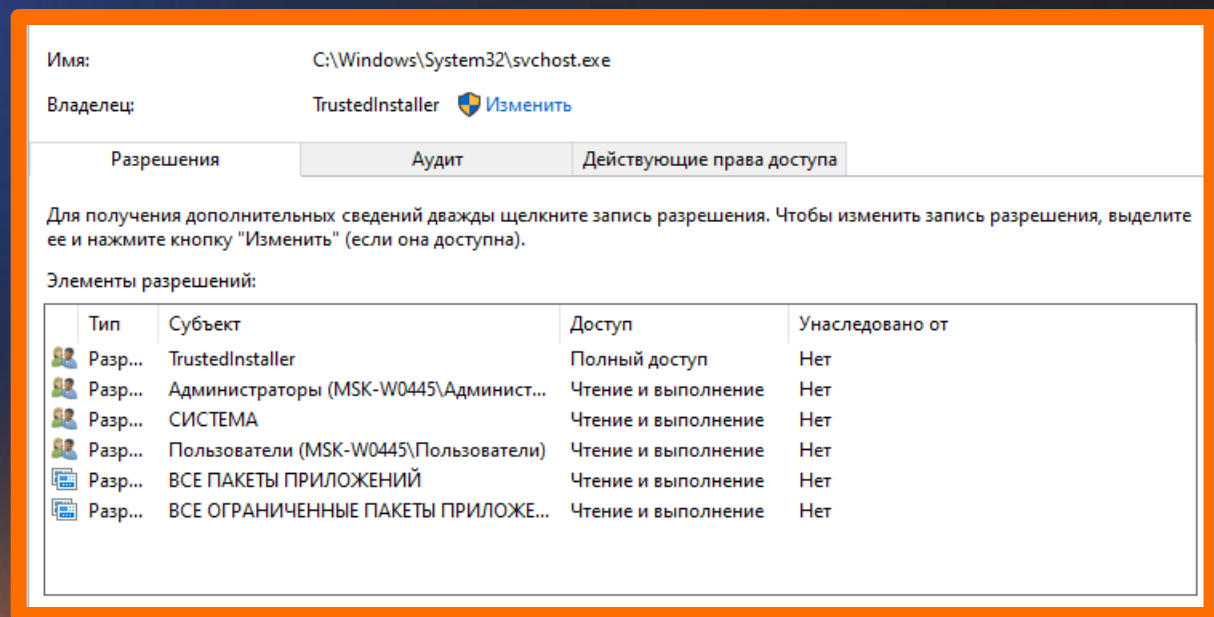
Имя	Тип	Значение
 (По умолчанию)	REG_SZ	(значение не присвоено)
 ServiceDll	REG_EXPAND_SZ	%SystemRoot%\system32\fdrespub.dll
 ServiceDllUnloadOnStop	REG_DWORD	0x00000001 (1)

Схема элементов сервисов

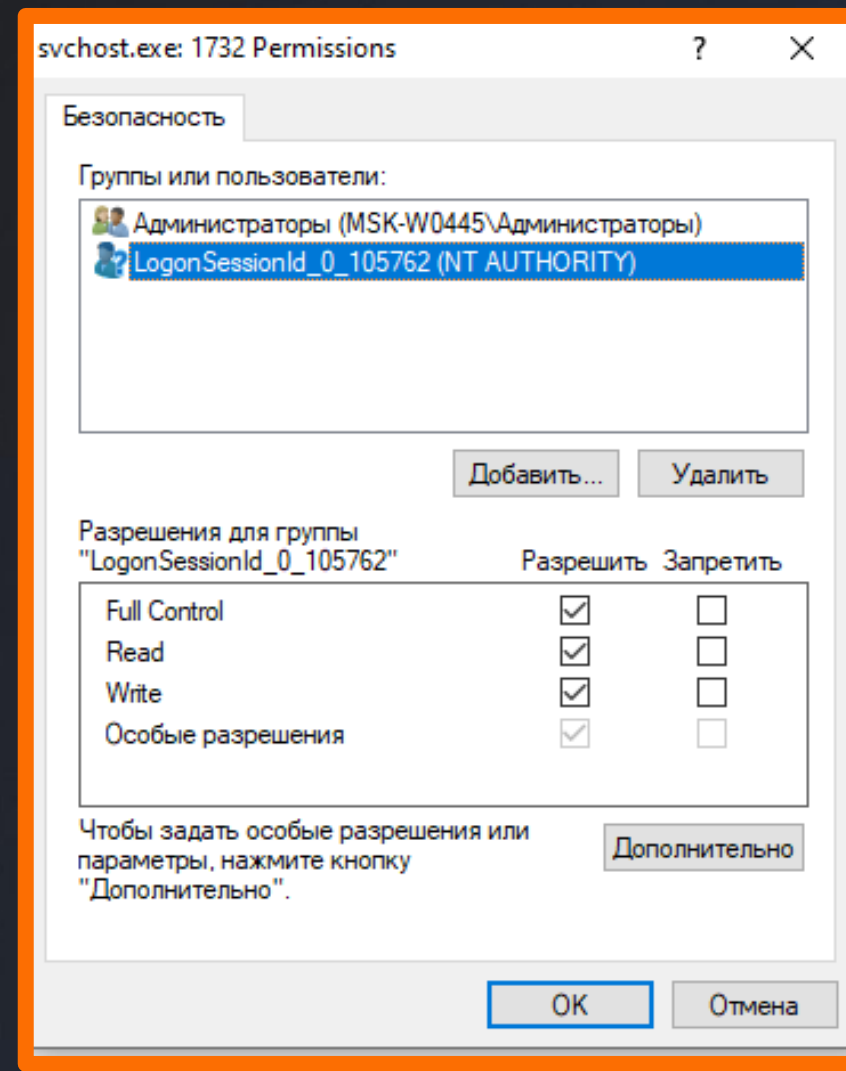


Права на файлы и процессы

Ampire 360°



Права на файл



Права на процесс

В чем заключается существенная разница?

ImagePath – %SystemRoot%\system32\svchost.exe -k
LocalServiceAndNoImpersonation -p

Parameters\ServiceDll – %SystemRoot%\system32\fdrespub.dll

Три неправильных разных способа запуска сервиса



`sc start service`



`net start service`



`services.msc`

Права сервиса

Сервис: Оптимизация доставки (DoSvc)

SDDL:

O:SY

G:SY

D:

(A;;CCLCSW**R**PLORC;;;AU)

(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)

(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)

(A;;**D**CRC;;;S-1-5-80-3055155277-3816794035-
3994065555-2874236192-2193176987)

NT SERVICE\DoSvc

Еще больше информации о сервисах

ServiceSidType – создание SID
для сервиса

Security\Security – бинарный
SDDL для сервиса

(По умолчанию)	REG_SZ	(значение не присвоено)
DelayedAutostart	REG_DWORD	0x00000001 (1)
DependOnService	REG_MULTI_SZ	rpcss
Description	REG_SZ	@%systemroot%\system32\dosvc.dll,-101
DisplayName	REG_SZ	@%systemroot%\system32\dosvc.dll,-100
ErrorControl	REG_DWORD	0x00000001 (1)
FailureActions	REG_BINARY	80 51 01 00 00 00 00 00 00 00 03 00 00 00 14 00 00 00 01 00 00 00 6
ImagePath	REG_EXPAND_SZ	%SystemRoot%\System32\svchost.exe -k NetworkService -p
LaunchProtected	REG_DWORD	0x00000002 (2)
ObjectName	REG_SZ	NT Authority\NetworkService
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\system32\dosvc.dll
ServiceDllUnloadOnStop	REG_DWORD	0x00000001 (1)
ServiceSidType	REG_DWORD	0x00000001 (1)
Start	REG_DWORD	0x00000002 (2)
SvcMemHardLimitInMB	REG_DWORD	0x00000027 (39)
SvcMemMidLimitInMB	REG_DWORD	0x0000001b (27)
SvcMemSoftLimitInMB	REG_DWORD	0x0000000f (15)
Type	REG_DWORD	0x00000020 (32)

Имя	Тип	Значение
(По умолчанию)	REG_SZ	(значение не присвоено)
Security	REG_BINARY	01 00 14 80 a0 00 00 00 ac 00 00 00 14 00 00 00

Значения прав сервиса

Обозначение	Право
RP	Старт сервиса
WP	Остановка сервиса
DC	Изменение конфигурации сервиса
WD	Изменение прав для сервиса
WO	Изменение владельца сервиса

План эксплуатации сервиса DoSvc

1. Правим переменные окружения

2. **Запускаем** сервис DoSvc

```
(A;;CCLCSWRPLORC;;;AU)  
(A;;DCRC;;;NT SERVICE\DoSvc )
```

3. Меняем сами себе конфигурацию

Еще чуть-чуть информации о сервисах

LaunchProtected — усиление
защиты процесса сервиса

ab (По умолчанию)	REG_SZ	(значение не присвоено)
ou DelayedAutostart	REG_DWORD	0x00000001 (1)
ab DependOnService	REG_MULTI_SZ	rpcss
ab Description	REG_SZ	@%systemroot%\system32\dosvc.dll,-101
ab DisplayName	REG_SZ	@%systemroot%\system32\dosvc.dll,-100
ou ErrorControl	REG_DWORD	0x00000001 (1)
ou FailureActions	REG_BINARY	80 51 01 00 00 00 00 00 00 00 00 03 00 00 00 14 00 00 00 01 00 00 00 6
ab ImagePath	REG_EXPAND_SZ	%SystemRoot%\System32\svchost.exe -k NetworkService -p
ou LaunchProtected	REG_DWORD	0x00000002 (2)
ab ObjectName	REG_SZ	NT Authority\NetworkService
ab ServiceDll	REG_EXPAND_SZ	%SystemRoot%\system32\dosvc.dll
ou ServiceDllUnloadOnStop	REG_DWORD	0x00000001 (1)
ou ServiceSidType	REG_DWORD	0x00000001 (1)
ou Start	REG_DWORD	0x00000002 (2)
ou SvcMemHardLimitInMB	REG_DWORD	0x00000027 (39)
ou SvcMemMidLimitInMB	REG_DWORD	0x0000001b (27)
ou SvcMemSoftLimitInMB	REG_DWORD	0x0000000f (15)
ou Type	REG_DWORD	0x00000020 (32)

Права на ветки реестра сервиса

Сервис: Служба времени Windows (W32Time)

SDDL:

O:SY

G:SY

D:PAI

(A;CIIO;GA;;;SY) (A;;KA;;;SY) (A;CIIO;GR;;;LS)
(A;;KR;;;LS) (A;;KR;;;NS) (A;CIIO;GR;;;NS) (A;;KA;;;BA)
(A;CIIO;GA;;;BA) (A;CIIO;GR;;;BU) (A;;KR;;;BU)
(A;;KR;;;NO) (A;CIIO;GR;;;NO)
(A;;CCDCLCSWRPSDRC;;;S-1-5-80-3169285310-278349998-
1452333686-3865143136-4212226833)
(A;CIIO;SDGWGR;;;S-1-5-80-3169285310-278349998-
1452333686-3865143136-4212226833)
NT SERVICE\autotimesvc

Значения прав реестра

Обозначение	Право
DC	Запись значений
LC	Создание подразделов
GW	Полные права на запись
GA	Полные права на все
KW	Полные права на запись
KA	Полные права на все

План эксплуатации сервиса W32Time

1. Правим переменные окружения
2. **Запускаем** сервис autotimesvc
3. Меняем конфигурацию сервиса W32Time
4. Запускаем сервис W32Time

Три правильных разных способа запуска сервиса

Ampire 360°



WinAPI StartService()



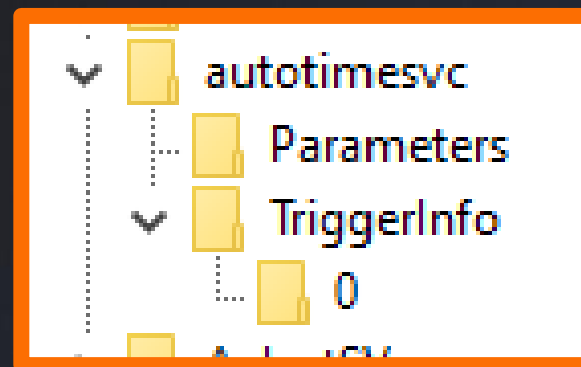
TriggerInfo в реестре



Специальные триггеры

Да сколько ещё этой информации о сервисах?

TriggerInfo\0 — триггеры на
старт и остановку сервиса



TriggerInfo\0\Action — действие

TriggerInfo\0\Type — тип

Имя	Тип	Значение
(По умолчанию)	REG_SZ	(значение не присвоено)
Action	REG_DWORD	0x00000001 (1)
Data0	REG_BINARY	75 d0 be a3 2e 0b 8a 0d
DataType0	REG_DWORD	0x00000001 (1)
GUID	REG_BINARY	16 28 7a 2d 5e 0c fc 45 9c e7 57 0e 5e cd e9 c9
Type	REG_DWORD	0x00000007 (7)

Триггер (код)	Описание
SERVICE_TRIGGER_TYPE_CUSTOM (20)	ETW-событие
SERVICE_TRIGGER_TYPE_DEVICE_INTERFACE_ARRIVAL (1)	Подключение устройства
SERVICE_TRIGGER_TYPE_IP_ADDRESS_AVAILABILITY (2)	Доступность ip-адреса
SERVICE_TRIGGER_TYPE_DOMAIN_JOIN (3)	Подключение к домену
SERVICE_TRIGGER_TYPE_FIREWALL_PORT_EVENT (4)	Открытие порта
SERVICE_TRIGGER_TYPE_GROUP_POLICY (5)	Изменение групповой политики
SERVICE_TRIGGER_TYPE_NETWORK_ENDPOINT (6)	Создание pipe или RPC-сервера

WNF (Windows Notification Facility)

WNF — Windows реализация механизма уведомлений на базе модели издатель-подписчик (pub-sub)

Для autotimesvc в триггере используется WNF_CELL_NITZ_INFO

CC — чтение, DC — запись

D:

(A;;CCDC;;;SY)

(A;;CCDC;;;NT SERVICE\WwanSvc)

(A;;CCDC;;;BA)

(A;;CC;;;AU)

(A;;CC;;;IU)

Полный план эксплуатации сервиса W32Time

1. Правим переменные окружения
2. Запускаем сервис **WwanSvc**
3. Записываем WNF данные (стартует сервис autotimesvc)
4. Меняем конфигурацию сервиса W32Time
5. Запускаем сервис W32Time

Третья попытка: сервис DHCP

Dhcp — HKLM\SYSTEM\ControlSet001\Services\dhcp

Элемент разрешения для "Dhcp"

Субъект: Dhcp Выберите субъект Dhcp — NT SERVICE\Dhcp

Тип: Разрешить

Применяется к: Этот раздел и его подразделы

Дополнительные разрешения:

☐ Полный доступ	☐ Создание связи
☐ Запрос значения	☐ Удаление
☐ Задание значения	☐ Запись DAC
☐ Создание подраздела	☐ Смена владельца
☒ Перечисление подразделов	☒ Чтение разрешений
☒ Уведомление	

☐ Применять эти разрешения к объектам и контейнерам только внутри этого контейнера

Очистить все

Отображение общих разрешений

Последняя часть информации о сервисах

Performance — ветка
с информацией о мониторе
производительности

Performance\Library — путь
к библиотеке для монитора
производительности

Имя	Тип	Значение
 (По умолчанию)	REG_SZ	(значение не присвоено)
 Close	REG_SZ	Close
 Collect	REG_SZ	Collect
 Library	REG_EXPAND_SZ	%systemroot%\system32\msscntrs.dll
 Open	REG_SZ	Open

Угадайте, куда загрузится библиотека?



Сервис



Системный процесс сбора метрик производительности

План эксплуатации сервиса DHCP

1. Правим переменные окружения
2. **Перезапускаем** сервис DHCP
3. Создаем ветку Performance и ключи в ней
4. Запускаем метрику производительности

Доведение идеи до PoC



BYOVL (bring your own vulnerable library)



RPC и ALPC



Завершение процесса

Спасибо за внимание!

Василий Кравец

@xitauw

Vasily.Kravets@amonitoring.ru



Ampire 360°