



kaspersky



Kaspersky Industrial
Cybersecurity
Conference 2021

Сергей Повышев

Старший менеджер-руководитель
направления «Управление
информационной безопасностью», ПАО
«Северсталь», Россия


#KasperskyICS

Чат конференции: <https://kas.pr/kicscon>

Практика киберучений

Делимся опытом

 Повышев Сергей Алексеевич

 Сентябрь 2021. Сочи

Содержание

- Киберучения. С чего начать?
- Теория. Не всё форензика, что блестит.
- Киберполигон. Если вы варите чугун, не учитесь защищать банкоматы.
- Red vs Blue Team:
 - Фишинг. RAT Merlin для обхода средств защиты.
 - Несанкционированное воздействие на АСУ ТП через физическое подключение подрядчика.
 - Маскировка источника Wanna.
- Итоги киберучений.



Киберучения. С чего начать?



Формат:



Требования к исполнителю:
Он не вендор СЗИ, внедренных в Компании



Теория. Не всё форензика, что блестит.



Tactics, Techniques



Хостовая форензика

Incident Response и
Threat Hunting, hardening



Много теории
без закрепления

Teaming



«Сферические
кони в вакууме»

Forensics tools
for network and endpoint



Только endpoint tools:
FTK Imager; Volatility

Согласовывайте не только темы для
обучения, но и их содержание

Теория сразу должна сопровождается
практической демонстрацией





Киберполигон. Если вы варите чугуны, не учитесь защищать банкоматы



Jenkins



django



docker



PostgreSQL

5 команд
2 дня
18 часов

5 сценариев

Защита

Web-приложения

Защита

приложения с микро
сервисной архитектурой

Расследование атаки на производственный
сегмент сети (CTF)

Расследование APT атаки (CTF)

Расследование атаки на веб-сайт (CTF)

01

Роли участников

Назначенные роли в команде не
соблюдались

02

Теоретическая подготовка

Знаний, полученных на первом
этапе было недостаточно. Вопрос
отражения атак не был освещён

03

Применимость

Разобранные кейсы, по
наполнению, маловероятно
встретятся на практике

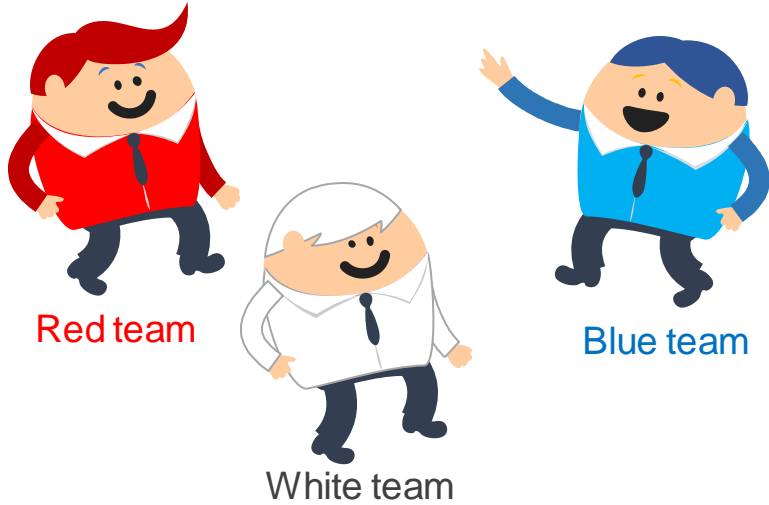
04

Составы команд

Необходимо правильно разделить
команды по уровню навыков и
компетенций участников

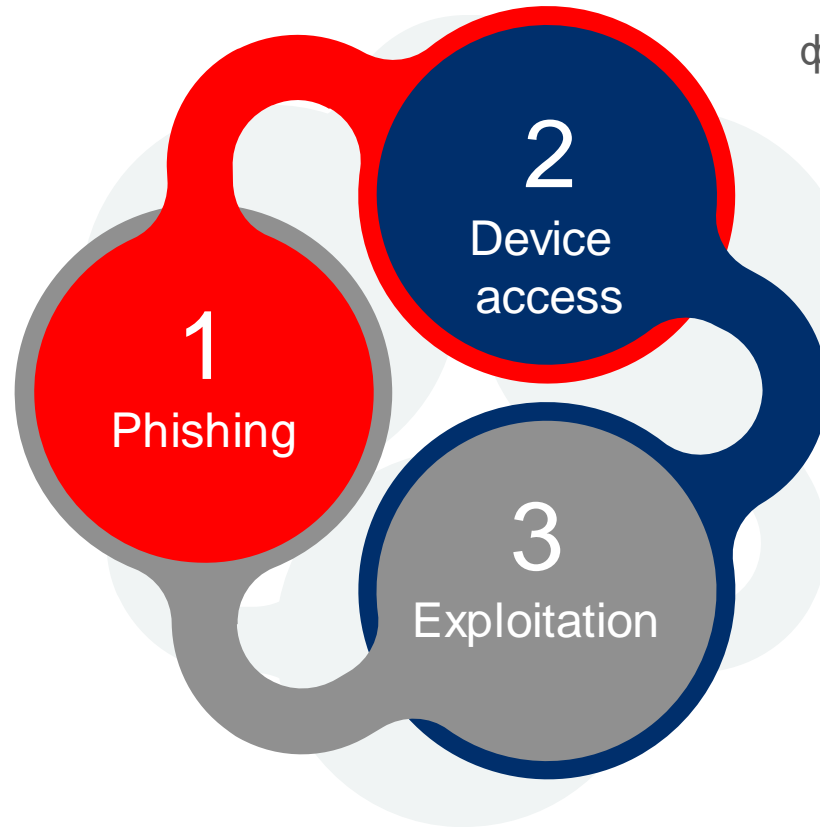


Red vs Blue Team. Три сценария атаки на инфраструктуру.



1 Сценарий 1

Точечная фишинговая рассылка.
Получение контроля над
рабочей станцией.



2 Сценарий 2

Industrial этап. Имитация действий
нерадивого подрядчика,
физически подключенного во
внутреннюю сеть

3 Сценарий 3

Industrial этап. Атака на цепочку
поставок.
Заражённая виртуальная машина
на внешнем накопителе
подрядчика

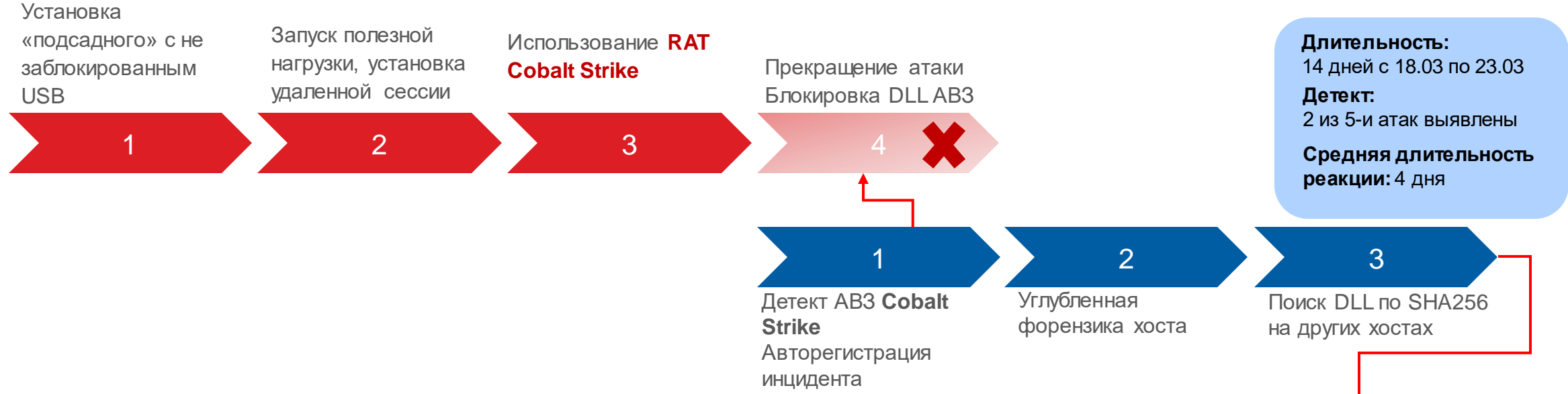


Фишинг. RAT Merlin для обхода средств защиты.

Атака 1

Red

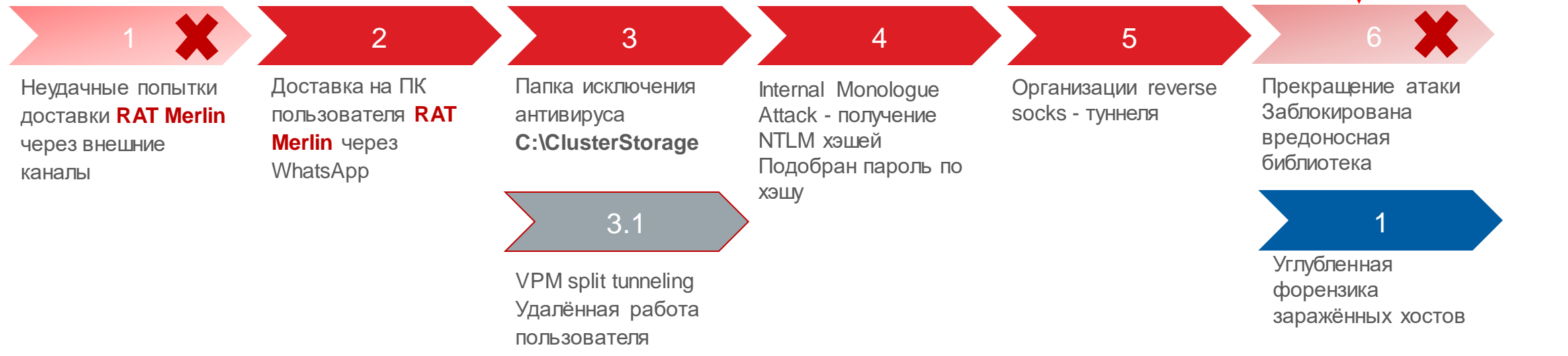
Blue

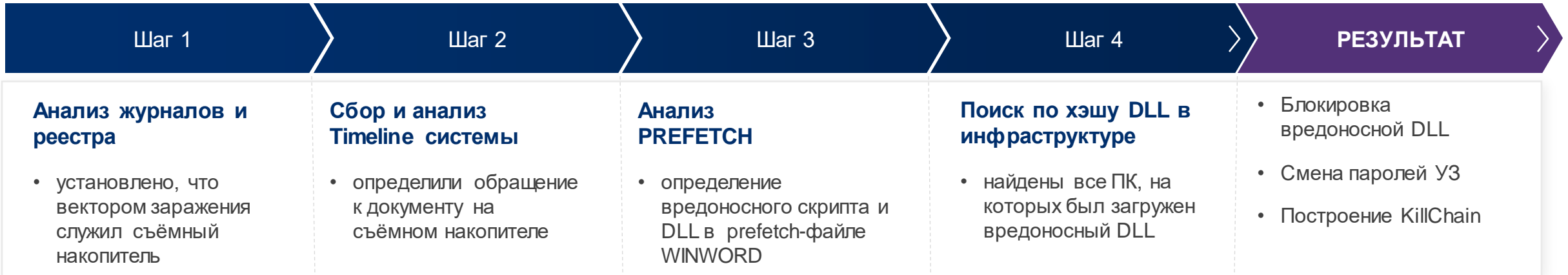


Атака 2

Red

Blue





```
211: \VOLUME{01d71bc651a4a062-3252089b}\WINDOWS\SYSWOW64\SCRRUN.DLL
212: \VOLUME{01d71bc651a4a062-3252089b}\USERS\AP[REDACTED]VA\APPDATA\ROAMING\MICROSOFT\WINDOWS\
213: \VOLUME{01d71bc651a4a062-3252089b}\USERS\AP[REDACTED]VA\APPDATA\LOCAL\TEMP\TELEMETRY.VBS
214: \VOLUME{01d71bc651a4a062-3252089b}\USERS\AP[REDACTED]VA\APPDATA\LOCAL\MICROSOFT\WINDOWS\IN
215: \VOLUME{01d71bc651a4a062-3252089b}\PROGRAM FILES (X86)\COMMON FILES\SYSTEM\ADO\MSADO15.
216: \VOLUME{01d71bc651a4a062-3252089b}\WINDOWS\SYSWOW64\MSDART.DLL
```



Несанкционированное воздействие на АСУ ТП через физическое подключение подрядчика



Изменить область памяти
в ПЛК



Выполнить перезапуск ПЛК
Изменить значение счетчика



На управляющей SCADA заменить главную
маску экрана на вымогательскую надпись

Длительность:
14 дней с 06.04 по 19.04

Детект:
4 из 11-и атак выявлены

**Средняя длительность
реакции: 5 дней**

Сценарий атаки:

- Подключение миниПК с 3G в коммутатор ТСПД
- Сканирование сетевых портов сегмента АСУТП
- Сканирование на наличие уязвимостей ОТ устройств
- Эксплуатация уязвимостей, получение доступа к целевым узлам



Несанкционированное изменение проекта ПЛК №1

Атака 1



Заголовок ↓

Добавлен MAC-адрес 94:c6:91:1e:23:e3 устройству с IP-адресом [REDACTED] 19.100

Обнаружено новое устройство с адресом [REDACTED] 19.100

Получена новая информация об устройстве с адресом [REDACTED] 19.100

Сработало правило из набора network_scan (системный набор правил)

Сработало правило из набора network_scan (системный набор правил)

Добрый день!

В КР обнаружено подключение неавторизованного устройства в сеть АСУ ТП, с дальнейшим сканированием хостов по сигнатуре HackTool.SQLScan.TCP.ServerRequest

src:172.23.19.100

устройство подключено в 19 порт [REDACTED]

Определено - устройство не является собственностью Общества, в процессах АСУ ТП не задействовано.

необходимо заблокировать 19 порт коммутатора [REDACTED]

Несанкционированное изменение проекта ПЛК №2



1

Перехват из NBNS и LLMNR хэша Local USER через **Responder**

2

Сканирование сети с низким и высоким рейтингом

3

Найден ПК, уязвимый к **MS17-010**. Добавлена УЗ для подключения через RDP

4

В папку **C:\ClusterStorage** скопирован и запущен Mimikatz. Получен пароль от локальной УЗ

5

Найдена УЗ **admin** и подобран пароль от нее. Подключение под УЗ к доменному серверу

6

Запуск **Mimikatz**. Получение пароля от доменной УЗ

7

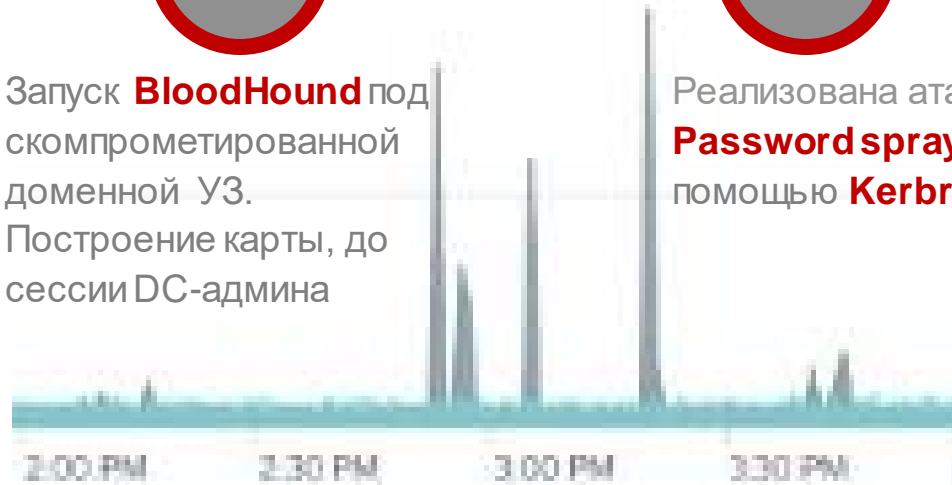
Запуск **BloodHound** под скомпрометированной доменной УЗ. Построение карты, до сессии DC-админа

8

Реализована атака **Password spraying** с помощью **Kerbrute**

9

Реакция **BlueTeam** на сетевые сканирования + 7 дней





Маскировка источника Wanna

01

ЦЕЛЬ

Эксплуатация уязвимости BlueKeep
Соккрытие источника заражения

02

ПОДГОТОВКА

Модифицированный Wanna,
не шифрующий файлы

03

ЛЕГЕНДА

Подрядчик выполнял работы по наладке оборудования.
Единожды использовал в работе виртуальную машину, размещённую на USB-накопителе.
ВМ была заражена вирусом WannaCry.
Сразу после работ ВМ была отключена, а работа продолжена на ОС ноутбука.

Длительность:

5 дней с 04.04 по 10.04

Детект:

Обнаружена

**Средняя длительность
реакции: 1 день**

Маскировка источника Wanna



Обнаружение

- Событие IDS Trojan-Ransom.Wanna.TCP.Sprea
- Регистрация инцидента

Индикаторы

Ip: x.x.16.198
 MAC: x.x.x.x.e3:09
 Статус: не в сети

16.198	ac-e2-d3-e6-2e-b8
16.198	00-0c-29-bd-d3-aa
16.201	e4-bb-6d-4e-fb-bc
16.206	3c-97-0e-04-24-f1

Локализация

- Выезд на место сотрудника ИТ
- Осмотрены ноутбуки подрядчиков, искомые IP и MAC не найдены
- Следов заражения на ноутбуках не найдено.
- Ноутбук не передан **BlueTeam**

Индикаторы

Адрес источника вредоносной активности находился в диапазоне адресов, выданных подрядчику X

В ARP- таблице ACO найдены искомые MAC адреса и локализован конкретный коммутатор

Параметры

Маршрут. устройство: Нет
 Статус: Неразрешенное
 ОС: Windows 7/Server 2008 R2
 Производитель: VMware, Inc.
 Сетевое имя: LOL-win7PC

Расследование

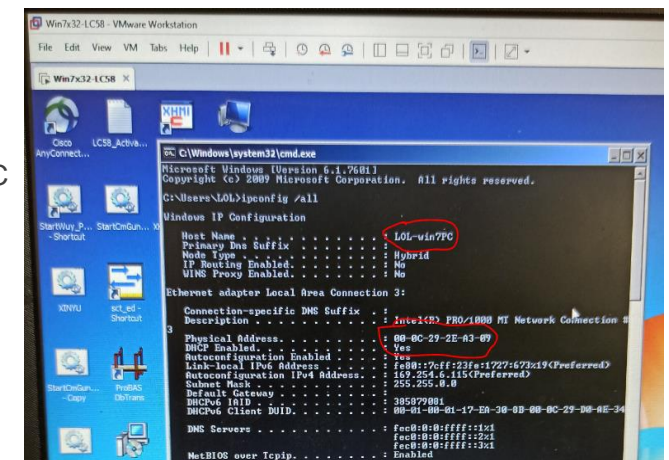


- В именах ноутбука содержатся фрагменты искомого имени LOL-xxx
- Определено что источник заражения - VM
- Санкционированно эксплуатируемых VM в исследуемом сегменте нет.
- Обнаружен Гипервизор VMware
- По логам установлен факт запуска VM с USB
- На столе найден USB с зараженной VM



Индикаторы

Сетевое имя: LOL-win7PC
 Тип ОС: VMware





Итоги киберучений

Мониторинг

- Контролируйте папки исключения антивируса

`C:\ClusterStorage`

- Используйте sysmon для детальных логов.

Предотвращение

- Запускайте Только подписанные скрипты powershell

Ловушки

- Используйте ловушки для хакера, например **Canary Account**, для выявления SharpHound **Event ID 4662**
- Используйте другие HoneyTokens

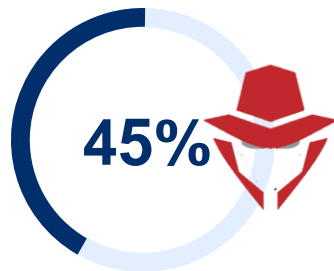
Возможности

- Недостаточное покрытие сенсорами анализа трафика
- Устаревшие IRM и сценарии выявления инцидентов

Бенефиты

- Получили независимую оценку защищенности инфраструктуры
- Вывели навыки в хостовой и сетевой форензике на новый уровень

Не пренебрегайте общением с пользователями

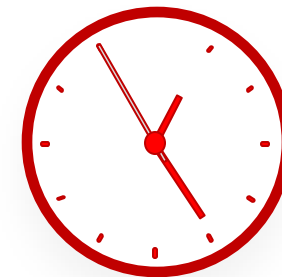


действий RedTeam обнаружено



4 дня

Среднее время реакции



50 дней

Длительность ReadTeaming